COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT AMENDMENT

Contract Number: UCP-TS-C01-11
Amendment #4

The above referenced contract is amended this 15th day of November, 2016 by GMO GlobalSign Inc, hereinafter called the "Contractor" and the Commonwealth of Virginia, Virginia Polytechnic Institute and State University, hereinafter called "Virginia Tech".

The parties hereby agree to renew the above referenced contract for another one-year period:

All other terms and conditions remain in full force and effect.

The parties agree to execute this Contract Amendment by electronic means, via facsimile/scanned signatures.

By: [Signature]
Contractor Authorized Signature

By: [Signature]
Virginia Tech Authorized Signature

IN WITNESS WHEREOF, the parties have caused this Contract Amendment to be duly executed intending to be bound thereby.

Contractor: GMO GlobalSign Inc

Authorized Signature: [Signature]
Printed Name: John M. Murrey
Title: VP Sales, North America

Virginia Tech

Authorized Signature: [Signature]
Printed Name: Patricia K. Branscome
Title: Director of Information Technology Acquisitions

Invent the Future

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
An equal opportunity, affirmative action institution
COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract Number: UCP-TS-C01-11

This contract is entered into this 27th day of September, 2010 by GMO GlobalSign Inc, hereinafter called "Contractor", and the Commonwealth of Virginia, Virginia Polytechnic Institute and State University called "Virginia Tech".

WITNESSETH that the Contractor and Virginia Tech, in consideration of the mutual covenants, promises, and agreements herein contained, agrees as follows:

SCOPE OF CONTRACT: The Contractor shall provide the Public Key Infrastructure (PKI) Root Key Signing Solution to Virginia Tech as set forth in the Contract Documents.

PERIOD OF CONTRACT: From September 27, 2010 through November 26, 2010, and if accepted in writing by Virginia Tech will continue with a four-year initial term followed by optional one-year renewals.

COMPENSATION AND METHOD OF PAYMENT: The Contractor shall be paid by Virginia Tech in accordance with the Contract Documents.

CONTRACT DOCUMENT: The contract documents shall consist of:

- This signed contract
- Attachment A – Request for Proposal (RFP) 648260 dated March 12, 2010
- Attachment B – RFP 648260 Addendum 1
- Attachment C – Proposal submitted by Contractor dated April 15, 2010
- Attachment D – Terms and Conditions for Trusted Root, for Virginia Tech and Virginia Non-Profit Cooperative Use Only
- Attachment E – Pricing and Registration Form for Trusted Root, for Virginia Non-Profit Cooperative Use Only
- Attachment F – Terms and Conditions for Managed SSL and ePKI, for Virginia Non-Profit Cooperative Use Only
- Attachment G – Pricing and Information for Managed SSL and ePKI, for Virginia Non-Profit Cooperative Use Only
- Attachment H – Summary of Negotiations
- Attachment I – CONFIDENTIAL – Revised Registration Form with Pricing for Virginia Tech Only

All of which contract documents are incorporated herein.

The parties agree to execute this Contract by electronic means, via facsimile/scanned signatures.

By: John Murray
Virginia Tech Authorized Signature

In WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

Contractor: Virginia Tech:

By: John Murray
Name: John D. Krallman
Title: Senior Vice President Sales
Title: Director of IT Acquisitions

invent the Future
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract</td>
<td>1</td>
</tr>
<tr>
<td>Attachment A – Request for Proposal (RFP) 648260 dated March 12, 2010</td>
<td>3</td>
</tr>
<tr>
<td>Attachment B – RFP 648260 Addendum 1</td>
<td>20</td>
</tr>
<tr>
<td>Attachment C – Proposal submitted by Contractor dated April 15, 2010</td>
<td>22</td>
</tr>
<tr>
<td>Attachment D – Terms and Conditions for Trusted Root,</td>
<td>183</td>
</tr>
<tr>
<td>for Virginia Tech and Virginia Non-Profit Cooperative Use Only</td>
<td></td>
</tr>
<tr>
<td>Attachment E – Pricing and Registration Form for Trusted Root,</td>
<td>188</td>
</tr>
<tr>
<td>for Virginia Non-Profit Cooperative Use Only</td>
<td></td>
</tr>
<tr>
<td>Attachment F – Terms and Conditions for Managed SSL and ePKI,</td>
<td>191</td>
</tr>
<tr>
<td>for Virginia Non-Profit Cooperative Use Only</td>
<td></td>
</tr>
<tr>
<td>Attachment G – Pricing and Information for Managed SSL and ePKI,</td>
<td>209</td>
</tr>
<tr>
<td>for Virginia Non-Profit Cooperative Use Only</td>
<td></td>
</tr>
<tr>
<td>Attachment H – Summary of Negotiations</td>
<td>220</td>
</tr>
<tr>
<td>Attachment I – CONFIDENTIAL – Revised Registration Form with Pricing,</td>
<td>222</td>
</tr>
<tr>
<td>for Virginia Tech Only</td>
<td></td>
</tr>
</tbody>
</table>
Attachment A

Request for Proposal (RFP) 648260 dated March 12, 2010

Request for Proposal 648260
Request for Proposal # 648260

for

PKI Root Key Signing Solution

March 12, 2010
RFP 648260
GENERAL INFORMATION FORM

QUESTIONS: All inquiries for information regarding this solicitation should be directed to: Nancy Sterling, Sr. Contract Officer, Phone: (540) 231-9517, e-mail: nancy.sterling@vt.edu.

DUE DATE: Sealed Proposals will be received until **April 16, 2010 at 3:00 PM**. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

ADDRESS: Proposals should be mailed or hand delivered to Virginia Polytechnic Institute and State University (Virginia Tech) at: Virginia Tech, Attn: Nancy Sterling, IT Acquisitions Office (0214), 1700 Pratt Drive, Blacksburg, Virginia 24061

**Reference the Opening Date and Hour, and RFP Number in the lower left corner of the return envelope or package.**

**TYPE OF BUSINESS:** (Please check all applicable classifications). If your classification is certified by the Virginia Department of Minority Business Enterprise, provide your **DMBE certification number:** ______________. For certification assistance, please visit: http://www.dmb.state.va.us/swamcert.html.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

COMPANY INFORMATION/SIGNATURE: In compliance with this Request for Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods and services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

<table>
<thead>
<tr>
<th>FULL LEGAL NAME (PRINT)</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears with your Federal Taxpayer Number)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS NAME/DBA NAME/TA NAME</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(If different than the Full Legal Name)</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BILLING NAME</th>
<th>FEDERAL TAXPAYER NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears on your invoice)</td>
<td>(If different than ID# above)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURCHASE ORDER ADDRESS</th>
<th>PAYMENT ADDRESS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CONTACT NAME/TITLE (PRINT)</th>
<th>SIGNATURE (IN INK)</th>
<th>DATE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>E-MAIL ADDRESS</th>
<th>TELEPHONE NUMBER</th>
<th>TOLL FREE TELEPHONE NUMBER</th>
<th>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</th>
</tr>
</thead>
</table>

04/09
I. PURPOSE:

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals to establish a contract or contracts through competitive negotiations for a Public Key Infrastructure (PKI) Root Key Signing Solution for Virginia Polytechnic Institute and State University (Virginia Tech), an agency of the Commonwealth of Virginia.

In order to realize the benefits of PKI, Virginia Tech has established its own enterprise Certification Authority (CA) with a self-signed root certificate that can be used to issue digital certificates to employees, machines and services. These digital certificates are primarily used for digital signature and encryption of network communications to help provide a secure business environment for the enterprise.

The self-signed root certificate of the Virginia Tech Certification Authority (VTCA) is not automatically trusted by the mainstream browsers, operating systems, email clients and other business applications. As a result, many of these applications typically display warning messages that cause confusion and low confidence by the end user. In order to avoid these warning messages, the university would be forced to implement a root embedding project to ensure that its self-signed root certificate is included as a trusted certificate in all of these mainstream applications. The time and cost associated with such a project is not realistic as it would quickly nullify the benefits for operating an in-house enterprise CA.

A Root Key Signing Solution eliminates the need to directly embed the self-signed root certificate into applications by allowing the in-house CA self-signed root certificate to be chained under a pre-distributed and trusted commercial root certificate. By using a Root Key Signing Solution, certificates issued by the VTCA automatically inherit the trust associated with the root certificate of the key signing vendor and would be transparently accepted by the majority of mainstream PKI enabled applications.

II. CONTRACT PERIOD:

The term of this contract is for one year, or as negotiated. Optional renewals may be negotiated. Please indicate if you have a minimum contract period requirement.

III. BACKGROUND:

Founded in 1872 as a land-grant college named Virginia Agricultural and Mechanical College, Virginia Tech is now a comprehensive, innovative research university with the largest full-time student population in Virginia. Through a combination of its three missions of learning, discovery, and engagement, Virginia Tech continually strives to accomplish the charge of its motto: *Ut Prosim* (That I May Serve).

About Virginia Tech:

- Located in Blacksburg, Virginia
- Nine colleges and graduate school
- 65 bachelor's degree programs
- 145 master's and doctoral degree programs
- 30,000+ full-time students
- 16:1 student-faculty ratio
- Main campus includes more than 125 buildings, 2,600 acres, and an airport
- Computing and communications complex for worldwide information access
- Ranked 46th in university research in the United States
- Has adjacent corporate research center

More information about Virginia Tech can be found at [www.vt.edu](http://www.vt.edu).
About Virginia Tech Certification Authority (VTCA):

In April 2003, Virginia Tech established the Virginia Tech Certification Authority (VTCA) with the goal to provide enhanced enterprise security solutions for the university’s web based business processes. The VTCA is implemented using a hierarchical architecture consisting of a self-signed root CA (RSA-4096 bit key size) and three subordinate CAs (each RSA-4096 bit key size). The subordinate CAs in the hierarchy include the VT Class 1 Server, Middleware and User CAs which issue end entity SSL server, application, and personal digital certificates respectively.

The hierarchical architecture of the VTCA has been designed to help facilitate the implementation of additional subordinate CA’s if a need to accommodate new certificate profiles should arise. The VTCA runs commercial grade open source EJBCA (Enterprise Java Beans Certification Authority – www.ejbca.org) and OpenCA (www.openca.org) application software to support its in-house certificate services. It is administered as a high assurance CA using a hardware based HSM (Hardware Security Module) meeting FIPS 140-2 Level 3 requirements for secure key management. Strong user multi-factor authentication including M of N, hardware token, and biometric authentication techniques have been implemented to ensure a high level of security for ongoing operation of the VTCA.

The registration authority component of the VTCA enforces rigorous validation methods, including face to face enrollment for personal certificates and department head approval for SSL server/application certificates. To ensure the VTCA meets university requirements, a Policy Management Authority (PMA) has been formed to approve policies/standards for operation and administration of the PKI. More information about the VTCA including Certificate Policy (CP) and Certification Practice Statement (CPS) documents can be found at www.pki.vt.edu.

VTCA Hierarchical Architecture

VTCA Specifications

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Hierarchical Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Software</td>
<td>EJBCA 3.8.0 and OpenCA 0.925</td>
</tr>
<tr>
<td>Keys</td>
<td>RSA 4096 bit</td>
</tr>
<tr>
<td>Online/Offline</td>
<td>Root CA: Offline (EJBCA)</td>
</tr>
<tr>
<td></td>
<td>Class 1 Server CA: Online (EJBCA)</td>
</tr>
<tr>
<td></td>
<td>Middleware CA: Online (EJBCA)</td>
</tr>
<tr>
<td></td>
<td>User CA: Online (OpenCA)</td>
</tr>
<tr>
<td>Virginia Tech CA Certificates Download Page</td>
<td><a href="http://www.pki.vt.edu/developer/rootca.html">http://www.pki.vt.edu/developer/rootca.html</a></td>
</tr>
<tr>
<td>Server OS</td>
<td>RedHat AS 5.3</td>
</tr>
<tr>
<td>Server Hardware</td>
<td>Class 1 Server and Middleware CAs: 1 primary Dell 1850; 1 secondary failover Dell 1850</td>
</tr>
<tr>
<td></td>
<td>User CA: 1 primary Dell 1950; 1 secondary failover Dell 1950</td>
</tr>
<tr>
<td>HSMs</td>
<td>1 primary and 1 secondary SafeNet LunaSA HSMs as backup</td>
</tr>
<tr>
<td>HSM Authentication Controls</td>
<td>Root CA requires multi-factor authentication using 3 of 6 tokens in conjunction with token/PIN authentication</td>
</tr>
<tr>
<td></td>
<td>Subordinate CAs requires token/PIN and partition password</td>
</tr>
</tbody>
</table>
Physical Access Controls | Biometric and card access security for building entry; biometric and card access security for room entry where servers are located; servers are shelved in a key locked rack accessible only by authorized personnel
Certificate Policy (CP) and Certification Practices Statement (CPS) | Available at www.pki.vt.edu
Virginia Tech CA Certificates Download Page | http://www.pki.vt.edu/developer/rootca.html
Sha1Thumbprints | Root CA: af6feb42fa2fe4a26e9f7fb5b5ff3abc13c60d81
               Class 1 Server CA: e46fb958b785cbbdb93b6865bf8a9837ab0b7d027
               Middleware CA: 6d66434d7c26e6b00482ec3a73226f6835a7e1ba
               User CA: ac01d04e230893bcba450ca15582c3a8840b7b7
Certificate Singing Request (CSR) Format | Base64 encoded PKCS#10

In recent years, the VTCA has played an increasingly significant role by providing several important security functions including:
- Strong digital identity credentials for authentication
- Strong encryption to provide secure data communications
- Digital signatures which support non-repudiation of online transactions
- Document integrity using digital signatures

The following table provides a summary of the number of active digital certificates used/estimated at Virginia Tech during a three year period spanning 2008 – 2010.

### Active Digital Certificate Usage at Virginia Tech

<table>
<thead>
<tr>
<th>Certificate Profile</th>
<th>2008 01/08-12/08</th>
<th>2009 01/09-10/09</th>
<th>2010 (Estimated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTCA SSL Server Certs</td>
<td>253</td>
<td>320</td>
<td>405</td>
</tr>
<tr>
<td>VTCA Middleware Certs</td>
<td>56</td>
<td>68</td>
<td>83</td>
</tr>
<tr>
<td>VTCA Personal Certs</td>
<td>549</td>
<td>623</td>
<td>706</td>
</tr>
<tr>
<td>SSL Server Certs Purchased from a Commercial Vendor</td>
<td>163</td>
<td>196</td>
<td>236</td>
</tr>
</tbody>
</table>

The lack of global recognition/trust of the VTCA self-signed root certificate has in many cases prevented subscribers from using VTCA issued SSL certificates for securing their outward facing web based applications. Further, when e-mail is digitally signed with a VTCA personal digital certificate and sent to a recipient outside the Virginia Tech domain, the Virginia Tech sender's certificate is not trusted. When a certificate is not trusted, the error message or complaint received by the relying party from their browser can result in mistrust of the server or the source.

To remedy this situation, subscribers typically purchase globally trusted certificates from a commercial certificate vendor when securing their public facing applications. By taking advantage of a **Root Key Signing Solution**, Virginia Tech will be able to retain complete control over the lifecycle management for the certificates it issues and at the same time realize the inherent security, confidence and recognition benefits from being chained to a globally trusted Root.

More information about the VTCA can be found at [www.pki.vt.edu](http://www.pki.vt.edu).

### IV. CONTRACT PARTICIPATION:

**CONTRACT PARTICIPATION:** Under the authority of the Code of Virginia 2.2-4304. Cooperative Procurement, it is the intent of this solicitation and resulting contract(s) to allow for cooperative procurement. Accordingly, any public body, public or private health or educational institutions or lead-issuing institution’s affiliated corporations may access any resulting contract if authorized by the contractor.
Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) will be extended to the public bodies indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify the lead-issuing institution in writing of any such institutions accessing the contract. No modification of this contract or execution of a separate contract is required to participate. The Contractor will provide semi-annual usage reports for all entities accessing the Contract. Participating entities shall place their own orders directly with the Contractor(s) and shall fully and independently administer their use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the lead-issuing institution. The lead-issuing institution shall not be held liable for any costs or damages incurred by any other participating public body as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that the lead-issuing institution is not responsible for the acts or omissions of any entity and will not be considered in default of the contract no matter the circumstances.

Use of this contract(s) does not preclude any participating entity from using other contracts or competitive processes as the need may be.

V. EVA BUSINESS-TO-GOVERNMENT ELECTRONIC PROCUREMENT SYSTEM:

The eVA Internet electronic procurement solution streamlines and automates government purchasing activities within the Commonwealth of Virginia. Virginia Tech, and other state agencies and institutions, have been directed by the Governor to maximize the use of this system in the procurement of goods and services. We are, therefore, requesting that your firm register as a trading partner within the eVA system.

There are registration fees and transaction fees involved with the use of eVA. These fees must be considered in the provision of quotes, bids and price proposals offered to Virginia Tech. Failure to register within the eVA system may result in the quote, bid or proposal from your firm being rejected and the award made to another vendor who is registered in the eVA system.

Registration in the eVA system is accomplished on-line. Your firm must provide the necessary information. Please visit the eVA website portal at www.eva.state.va.us and complete the Ariba Commerce Services Network registration. This process needs to be completed before Virginia Tech can issue your firm a Purchase Order or contract. If your company conducts business from multiple geographic locations, please register these locations in your initial registration.

For registration and technical assistance, reference the eVA website at: eVAcustomercare@dgs.virginia.gov, or call 866-289-7367.

VI. STATEMENT OF NEEDS:

Root Key Signing Specifications

To meet minimum requirements, the proposed solution shall fulfill the following items A thru D. Specifically state in the proposal if, and how, the proposed solution fulfills these minimum requirements. All references should include the letter beside the relevant line item.

A. CP/CPS of the Root Key Signing CA shall be provided to Virginia Tech for review.
B. Root Key Signing vendor shall provide an evaluation period of at least 30 days to Virginia Tech to allow time for testing and integration of the root key signing solution in the VTCA pre-production test environment.
C. The key signed CA certificate issued to Virginia Tech shall contain the following attributes:
   - Subject: Subject entry will be specified by Virginia Tech in the CSR submitted to the root key signing vendor
   - Public Key: RSA (4096)
   - Signature Algorithm: sha1RSA
   - Basic Constraints: Subject Type=CA, Path Length=None
   - Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing
D. The Trusted Root will provide application support for Internet Explorer 7+, Mozilla Firefox 2+, Safari 3+, Microsoft Entourage (OS/X), Mac Mail 3+, Adobe Certified Document Services (CDS)/Adobe 8+, and Java 5+.
In addition, the critical areas below are categorized by evaluation criteria. Proposals should address all these critical areas fully and make reference to the number beside the relevant line item. Ideally for clarity, the proposal would be structured following the same outline as below. These categories will be used in the assessment and selection of a final solution; please address these questions completely in submitting proposals.

1. **Integration with the VTCA and Functional Features**
   1.1. What applications contain the trusted root? (Browsers, Handsets, Email Clients, Application Suites like Adobe)
   1.2. What are the validity period options for the certificate issued to us? How easily is the certificate issued to us renewed?
   1.3. What is the key size of the trusted root?
   1.4. What is the signature algorithm used by the trusted root?
   1.5. Describe the process for submitting a request for a Root Key Signing.
   1.6. In the future, the VTCA may expand its certificate offerings to include object signing certificates. What is the impact of adding additional types of end entity certificate profiles?
   1.7. Is there any impact if Virginia Tech, in the future, decides to implement additional subordinate CA's that would chain back to the trusted root?
   1.8. What is the publication schedule of the certificate revocation list (CRL) for the trusted root? How will the CRL be made available to Virginia Tech? What is the URL of the trusted root CRL?

2. **Implementation and Support**
   2.1. When does the trusted root expire? What happens when it does?
   2.2. What is the Subject Entry of your trusted root certificate?
   2.3. Does the vendor support a PKCS #10 formatted CSR? What are the requirements for submitting a CSR?
   2.4. Can your company provide Virginia Tech with a pre-production key signed certificate for testing purposes? Can you allow Virginia Tech a minimum 30 day test and evaluation period?
   2.5. What are the options for contacting the vendor with support issues?
   2.6. Does the vendor require an audit of the VTCA?
   2.7. Can the company refer us to any universities that are using their root key signing service?
   2.8. List any special requirements for implementing a root key signing solution.
   2.9. How will the expiration date of the contract between Virginia Tech and the vendor impact the certificates that were issued prior to the contract end date? Is there a cutoff date for issuing certificates before the contract expiration date? If so, how does it affect the validity period of certificates issued prior to this date?
   2.10. The Virginia Tech Root CA is implemented using RSA 4096 bits keys. Does a RSA 4096 bit key size create any implementation issues for your solution?
   2.11. Describe how the addition of a subordinate CA within the VTCA hierarchy will impact the implementation. For example, Virginia Tech may in the future decide to implement a new subordinate CA to issue end entity certificates using an object signing certificate profile.
   2.12. Describe how the removal of a subordinate CA within the VTCA hierarchy will impact the implementation. For example, Virginia Tech may decide in the future to discontinue using the subordinate VTCA SSL server to issue end entity SSL certificates.

3. **Company Background and Financial Stability**
   3.1. How long has the company been in business?
   3.2. What is the location for ownership and operation of the Offeror, parent company, and affiliate company?
   3.3. What other services besides root key signing does the company offer?
   3.4. What certifications does the company have? Does this include WebTrust for CA's?
   3.5. Describe any liability and insurance coverage provided.

4. **Price**
   4.1. Does your company offer discounts to educational institutions like Virginia Tech?
   4.2. The VTCA issues some certificates that do not require a globally trusted root - these certificates (Middleware) are for internal use only. Can pricing accommodate this situation so that we are only paying for Certificates used by public facing applications?
   4.3. How are license fee costs for end entity certificates issued under the root key chain calculated? Is there a charge for certificates that are active (certificate has not expired) but have been revoked? Does the cost vary based on the type of certificate being issued such as personal, SSL server, or object signing?
   4.4. What is the price and what is included in any one time setup fees, annual support fees, and renewal of the
root key signed certificate, and any other expenses for the proposed solution? Which items are essential for a functioning system, and which are optional add-ons?

4.5. Describe how your solution will impact users of certificates that were issued by the VTCA prior to the implementation of your solution.

4.6. Describe what impact the issuance of wildcard end entity certificates will have on your solution. Does this impact pricing?

4.7. Is there a minimum number of end entity certificates that must be issued?

5. SWaM - Small, Women-owned and Minority-owned Business Utilization

5.1. If your business cannot be classified as Small, Women-owned, or Minority-owned, describe your plan for utilizing SWaM businesses if awarded a contract.

5.2. Describe your ability to provide statistical reporting on actual SWaM subcontracting when requested.

5.3. If your firm or any business that you plan to subcontract with can be classified as SWaM, but has not been certified by the Virginia Department of Minority Business Enterprise (DMBE), acknowledge the expectation that the certification process will be initiated no later than the time of the award, and the final DMBE certification decision and certification number provided.

VII. PROPOSAL PREPARATION AND SUBMISSION:

A. General Requirements

1. RFP Response:

In order to be considered for selection, Offerors must submit a complete response to this RFP. The proposal shall be submitted in both print and electronic media as follows: One (1) printed signed original, five (5) printed copies, and one (1) electronic media copy in a generally used format(s) on CD, DVD, or Flash Drive media, with delivery to:

Nancy Sterling
Virginia Tech
IT Acquisitions
1700 Pratt Drive
Blacksburg, VA 24060-6361

Phone: 540-231-9517

Reference the Opening Date and Hour, and RFP Number in the lower left hand corner of the return envelope or package.

No other distribution of the proposals shall be made by the Offeror.

By submitting a bid/proposal and by signing any subsequent contract, the VENDOR WARRANTS AND AGREES that the prices, terms, warranties, and benefits specified in its bid/proposal are comparable to or better than the equivalent prices, terms, warranties, and benefits being offered to the vendor’s commercial or government customer.

The sole point of contact for questions or clarification regarding this RFP process or content shall be the Individual named below. Email is the preferred method of communication.

Nancy Sterling
Email: nancy.sterling@vt.edu
Phone: 540-231-9517

Any ADDENDA to this RFP and a summary of questions and answers that provide new information shall be posted to the department website, www.ita.vt.edu; click Computer Purchasing, then the solicitation of interest.
2. Proposal Preparation:
   a. Proposals shall be SIGNED by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested may result in Virginia Tech requiring prompt submission of missing information and/or giving a lowered evaluation of the proposal. Virginia Tech may reject proposals, which are substantially incomplete or lack key information, at its discretion. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.
   
   b. Proposals should be prepared simply and economically providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be on completeness and clarity of content.
   
   c. Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, sub letter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and sub letter should be repeated at the top of the next page. The proposal should contain a table of contents that cross references the RFP requirements. Information which the Offeror desires to present that does not fall within any of the requirements of the RFP, such as any license or service agreement, should be inserted at an appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.
   
   d. Each copy of the proposal should be bound in a single volume where practical. All documentation submitted with the proposal should be bound in that single volume. No special binding is required; any means to keep each proposal separate and complete is adequate.
   
   e. Ownership and Disclosure:
   Ownership of all data, material and documentation originated and prepared for Virginia Tech pursuant to the RFP shall belong exclusively to Virginia Tech and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act (see required action below).

   However, to prevent disclosure the Offeror must invoke the protections of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data or other materials is submitted. The written request must specifically identify the data or other materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret material submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable and may result in rejection of the proposal.

3. Pricing:
   By submitting a bid/proposal and by signing any subsequent contract, the vendor warrants and agrees that the prices, terms, warranties, and benefits specified in its bid/proposal are comparable to or better than the equivalent prices, terms, warranties, and benefits being offered to any of the vendor’s educational, government, or commercial customers.

   The vendor’s bid/proposal prices are fixed for the original term of the contract. Escalation/de-escalation may be requested at renewal and shall comply with Most Favorable Pricing and comply with Virginia Tech Terms and Conditions.

4. Oral Presentations:
   Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to Virginia Tech. This will provide an opportunity for the Offeror to clarify or elaborate on the proposal but will in no way change the original proposal. Virginia Tech will schedule the time and location of these
presentations; however, oral presentations are an option of Virginia Tech and may not be conducted. Therefore, proposals should be complete.

5. Questions and Answers: Questions should be emailed to Nancy Sterling at nancy.sterling@vt.edu. Questions will be accepted through four (4) business days before response due date. Questions and subsequent answers will be posted as addenda on the ITA department Website, www.ita.vt.edu; click Computer Purchasing, then the solicitation of interest.

B. Specific Requirements:

Proposals should be as thorough and detailed as possible so that Virginia Tech may properly evaluate your capabilities to provide the required goods and services. Offerors are required to submit the following information/items as a complete proposal:

1. The return of the General Information Form and addenda, if any, signed and filled out as required.

2. The return of the completed Virginia Tech Security Questionnaire for Technology-based Procurements (Attachment B)

3. Response to the requirements detailed in Section VI - Statement of Needs

4. Small, Women-owned and Minority-owned Business (SWaM) Utilization:
   If your business cannot be classified as Small, Women-owned, or Minority-owned, describe your plan for utilizing SWaM businesses if awarded a contract. Describe your ability to provide statistical reporting on actual SWaM subcontracting when requested. If your firm or any business that you plan to subcontract with can be classified as SWaM, but has not been certified by the Virginia Department of Minority Business Enterprise (DMBE), it is expected that the certification process will be initiated no later than the time of the award, and the final DMBE certification decision and certification number provided.

VIII. SELECTION CRITERIA AND AWARD

A. Selection Criteria:

Proposals will be evaluated by Virginia Tech using the following:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Maximum Point Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with the VTCA and Functional Features</td>
<td>25</td>
</tr>
<tr>
<td>Implementation and Support</td>
<td>20</td>
</tr>
<tr>
<td>Company Background and Financial Stability</td>
<td>15</td>
</tr>
<tr>
<td>Price</td>
<td>30</td>
</tr>
<tr>
<td>SWaM Utilization (small, women-owned, and minority owned)</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

B. Award:

Selection shall be made of two or more Offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the evaluation factors included in the Request for Proposal, including price, if so stated in the Request for Proposal. Negotiations shall be conducted with the Offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each Offeror so selected, Virginia Tech shall select the Offeror who, in its opinion, has made the best proposal, and shall award the contract to that Offeror. Virginia Tech may cancel this Request for Proposal or reject proposals at any time prior to an award, and is not required to furnish a statement of the reason why a particular proposal was not deemed to be the most advantageous. (Section 2.2-4359(D.), Code of Virginia.) Should Virginia Tech determine in writing and in its sole discretion that only one Offeror is fully qualified, or that one Offeror is clearly more highly qualified than the others under consideration, a contract may be negotiated and awarded to that Offeror. The award document will be a contract incorporating by reference all the requirements, terms and conditions of this solicitation and the Contractor's proposal as negotiated. See Attachment C for sample contract form.

Virginia Tech reserves the right to award more than one contract as a result of this solicitation.
IX. **ONLINE ACCESS TO SOLICITATION DOCUMENTS AND ADDENDA**

To view documents on Virginia Tech’s IT Acquisitions website, go to http://www.ita.vt.edu/. On the left side of first screen, click on the underlined heading “Computer Purchasing”. From this page click on any Solicitation to view details.

To view documents on eVA, Virginia’s e-procurement solution, go to http://www.eva.state.va.us/. On the first screen in the middle box, click on the underlined sub-heading “Solicitation & Awards”. From this page click on any Solicitation to view details. Search and sort as desired.

Please contact Nancy Sterling if you have any questions, nancy.sterling@vt.edu, 540-231-9517.

X. **CONTRACT ADMINISTRATION**

A. Nancy Sterling, Senior Contract Officer, IT Acquisitions, at Virginia Tech, or her designee, shall be identified as the Contract Administrator and shall use all powers under the contract to enforce its faithful performance.

B. The Contract Administrator, or her designee, shall not have authority to approve changes in the services which alter the concept or which call for an extension of time for this contract. Any modifications made must be authorized by the Virginia Tech ITA office through a written, signed amendment to the contract.

XI. **TERMS AND CONDITIONS:**

This solicitation and any resulting contract/purchase order shall be governed by the attached terms and conditions.

XII. **ATTACHMENTS:**

Attachment A - Terms and Conditions
Attachment B - Virginia Tech Security Questionnaire for Technology-based Procurements (submit with proposal)
Attachment C - Standard Contract Form
Special Terms and Conditions

1. **AUDIT**: The Contractor hereby agrees to retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. Virginia Tech, its authorized agents, and/or the State auditors shall have full access and the right to examine any of said materials during said period.

2. **AVAILABILITY OF FUNDS**: It is understood and agreed between the parties herein that Virginia Tech shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

3. **CANCELLATION OF CONTRACT**: Virginia Tech reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the Contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

4. **CONTRACT DOCUMENTS**: The contract entered into by the parties shall consist of the Request for Proposal including all modifications thereof, the proposal submitted by the Contractor, the written results of negotiations, the Commonwealth Standard Contract Form, all of which shall be referred to collectively as the Contract Documents. A separate contract will be executed by each agency, institution or public body wishing to use any contract resulting from this solicitation.

5. **INDEPENDENT CONTRACTOR**: The contractor shall not be an employee of Virginia Tech, but shall be an independent contractor. Nothing in this agreement shall be construed as authority for the contractor to make commitments which shall bind Virginia Tech, or to otherwise act on behalf of Virginia Tech, except as Virginia Tech may expressly authorize in writing.

6. **INSURANCE**: By signing and submitting a proposal under this solicitation, the Offeror certifies that if awarded the contract, it will have the following insurance coverages at the time the work commences. Additionally, it will maintain these during the entire term of the contract and that all insurance coverages will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission. During the period of the contract, Virginia Tech reserves the right to require the Contractor to furnish certificates of insurance for the coverage required.

**INSURANCE COVERAGES AND LIMITS REQUIRED**:

- **A. Worker's Compensation - Statutory requirements and benefits.**
- **B. Employers Liability - $100,000.00**
- **C. General Liability - $500,000.00 combined single limit. Virginia Tech and the Commonwealth of Virginia shall be named as an additional insured with respect to goods/services being procured. This coverage is to include Premises/Operations Liability, Products and Completed Operations Coverage, Independent Contractor's Liability, Owner's and Contractor's Protective Liability and Personal Injury Liability.**
- **D. Automobile Liability - $500,000.00**
- **E. Professional Liability to include errors and omissions- $500,000.00/occurrence.**

The contractor agrees to be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from the payment of all sums of money by reason of any claim against them arising out of any and all occurrences resulting in bodily or mental injury or property damage that may happen to occur in connection with and during the performance of the contract, including but not limited to claims under the Worker's Compensation Act. The contractor agrees that it will, at all times, after the completion of the work, be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from all liabilities resulting from bodily or mental injury or property damage directly or indirectly arising out of the performance or nonperformance of the contract.

7. **MINORITY BUSINESS, WOMEN-OWNED BUSINESSES SUBCONTRACTING AND REPORTING**: Where it is practicable for any portion of the awarded contract to be subcontracted to other suppliers, the contractor is encouraged to offer such business to minority and/or women-owned businesses. Names of firms may be available from the buyer and/or from the Division of Purchases and Supply. When such business has been subcontracted to these firms and upon
completion of the contract, the contractor agrees to furnish the purchasing office the following information: name of firm, phone number, total dollar amount subcontracted and type of product/service provided.

8. **NOTICES:** Any notices to be given by either party to the other pursuant to any contract resulting from this solicitation shall be in writing, hand delivered or mailed to the address of the respective party at the following address

   If to Contractor:
   Address Shown On Proposal Cover Page
   Attention: Name of Person Signing Proposal

   If to Virginia Tech:
   Virginia Polytechnic Institute and State University
   Attn: Nancy Sterling, Sr. Contract Officer
   IT Acquisitions
   1700 Pratt Dr.
   Blacksburg, VA 24061

9. **PROPOSAL ACCEPTANCE PERIOD:** Any proposal received in response to this solicitation shall be valid for 120 days. At the end of the 120 days the proposal may be withdrawn at the written request of the Offeror. If the proposal is not withdrawn at that time it remains in effect until an award is made or the solicitation is cancelled.

10. **PRIME CONTRACTOR RESPONSIBILITIES:** The Contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime Contractor. The Contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

11. **PROPOSAL PRICES:** Proposal shall be in the form of a firm unit price for each item or service during the contract period.

12. **QUANTITIES:** Quantities set forth in this solicitation are estimates only, and the Contractor shall supply at proposal prices actual quantities as ordered, regardless of whether such total quantities are more or less than those shown.

13. **RENEWAL OF CONTRACT:** This contract may be renewed by Virginia Tech upon written agreement of both parties for up to five successive one year periods only under the terms and conditions of the original contract except as stated in A and B below. Price increases may be negotiated only at the time of renewal. Written notice of Virginia Tech's intention to renew shall be given (approximately 90 days) prior to the expiration date of each contract period.

   A. If Virginia Tech elects to exercise the option to renew the contract for an additional one-year period, the contract price(s) for the additional year shall not exceed the contract prices of the original contract increased/decreased by no more than the percentage increase/ decrease of the other services category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

   B. If during any subsequent renewal period Virginia Tech elects to exercise the option to renew the contract, the contract price(s) for the subsequent renewal period shall not exceed the contract price(s) of the previous renewal period increased/decreased by more than the percentage increase/decrease of the other services category of the CPI-W section for the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

14. **COMMUNICATIONS:** Communications regarding this Request for Proposals (RFP) shall be formal from the date of issue for this RFP, until either a Contractor has been selected or the Information Technology Acquisitions Office rejects all proposals. Formal communications will be directed to the Information Technology Acquisitions Office. Informal communications, including but not limited to request for information, comments or speculations regarding this RFP to any University employee other than an Information Technology Acquisitions Office representative may result in the offending Offeror’s proposal being rejected.

15. **CERTIFICATION TESTING AND ACCEPTANCE:** The system specified in the contract shall be considered ready for production testing upon receipt of documentation from the Contractor that a successful system audit or diagnostic test was performed at the site demonstrating that the system meets the minimum design/performance capabilities stipulated by the contract. The system shall be deemed ready for production certification testing on the day following receipt of this documentation. Virginia Tech shall provide written confirmation of its acceptance following successful completion of the production certification test. System (software and/or hardware) payment will be authorized after the successful completion and certification test(s).

16. **SEVERAL LIABILITY:** Virginia Tech will be severally liable to the extent of its purchases made against any contract resulting from this solicitation. Colleges and Universities Cooperative Group (CUCPG) will be severally liable to the extent of its purchases made against any contract resulting from this solicitation. Applicable departments, institutions, agencies, Public Bodies of the Commonwealth of Virginia and private colleges or universities in the Commonwealth of Virginia will be severally liable to the extent of their purchases made against any contract(s) resulting from this solicitation.
If purchased, Virginia Tech reserves the right to conduct an IT security assessment on the product(s), system(s) and/or service(s) once delivered to validate the answers to the questions below. If evaluation copies or instances are available for testing, they should be provided to the IT Security Office when requested.

In the space following each question, please provide a Yes, No or a “no answer” (N/A), and add any appropriate comments. If the answer is No or N/A, please provide comments indicating how this question/concern is addressed elsewhere or why it is not applicable.

1. Does your product(s), system(s) and or service(s) protect against the SANS Top 20 security vulnerabilities http://www.sans.org/top20?

2. Does your product(s), system(s) and or service(s) protect against the OWASP http://www.owasp.org/index.php/OWASP_Top_Ten_Project?

3. What specific encryption algorithms are employed for your product(s), system(s) and/or service(s)?

4. Is all sensitive data (i.e. Social Security Numbers, Credit Card Numbers, Health Information, etc) encrypted in transit and at rest? If not, please explain? (NOTE: Please see the Sensitive Information page at http://www.security.vt.edu/sensitiveinfo.html for specifics).

5. Is login information such as user name and password encrypted during transmission from the client to the server? NOTE: Base-64 encoding is not acceptable.

6. Are operating systems (e.g. Windows or Linux), programming and scripting languages (e.g. Java or PHP), web servers (e.g. Apache or IIS), database servers (e.g. Oracle or MySQL), application servers, etc. always promptly patched and current with security updates? If not, please explain.

7. Is all access, including administrative accounts, controlled and logged (i.e. firewalls, file system permissions, ACLs, database table permissions, packet logs, etc.)? If not, please explain.
8. Does your product(s), system(s) and/or service(s) prevent the use of shared credentials or accounts including administrative accounts?

9. Describe how your product(s), system(s) and/or service(s) authenticates and authorizes users?

10. Does your product(s) and/or system(s) facilitate compliance with Federal and State laws, such as FERPA, HIPPA and PCI?

11. Does your company alert customers to vulnerabilities and security issues in a timely fashion? If so, please describe your process.

For hosted services, in addition to questions above

1. Are intrusion detection technologies and firewalls utilized on the hosted system(s)?

2. Describe how your facility is physically secured?

3. Does your network or facility undergo vulnerability scanning and penetration testing?

4. Do your employees hold Information Technology Security certifications and/or secure coding certifications? If so, please describe them.
ATTACHMENT C

Standard Contract form for reference only
Offerors do not need to fill in this form

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract Number: _______________________

This contract entered into this ___ day of ___________ 20___, by ______________________ ___________, hereinafter called the "Contractor" and Commonwealth of Virginia, Virginia Polytechnic Institute and State University, hereinafter called "Virginia Tech".

WITNESSETH that the Contractor and Virginia Tech, in consideration of the mutual covenants, promises and agreements herein contained, agrees as follows:

SCOPE OF CONTRACT: The Contractor shall provide the _____________ to Virginia Tech as set forth in the Contract Documents.

PERIOD OF CONTRACT: From _______________ through ________________ plus ______________ renewal options.

COMPENSATION AND METHOD OF PAYMENT: The Contractor shall be paid by Virginia Tech in accordance with the contract documents.

CONTRACT DOCUMENT: The contract documents shall consist of:
This signed Contract
Attachment A – Request for Proposal Number __________ dated _________
Attachment B – Proposal Submitted by the Contractor dated _________
Together with all written attachments, negotiations, and modifications thereof all of which Contract Documents are incorporated herein.

The parties agree to execute this Contract by electronic means, via facsimile/scanned signatures.

By: __________________________________________ By: ___________________________________________
Contractor Authorized Signature     Virginia Tech Authorized Signature

In WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

Contractor:  Virginia Tech
By: __________________________________________ By: ________________________________
Title: ______________________________________   Title: ________________________________
<table>
<thead>
<tr>
<th>QUESTION</th>
<th>ANSWER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Is the solution required to have un-restricted path length checking (Basic Constraints, Path Length=None)</td>
<td>1) We do not consider the absence of the “Basic Constraints, Path Length=None” requirement critical if the vendor is able to support the hierarchical structure of the VTCA, which would include the vendor Root certificate, the VTCA Key Signed certificate, the VTCA subordinate CA certificates, and end entity certificates resulting in a path length of 4.</td>
</tr>
<tr>
<td>2) Is the solution required to have application support for Adobe Certified Document services</td>
<td>2) We do not consider the absence of application support for Adobe Certificate Document Services critical since the user can configure Adobe to trust the Windows CA certificate store.</td>
</tr>
</tbody>
</table>
Attachment C
Proposal submitted by Contractor dated April 15, 2010
Request for Proposal 648260
GlobalSign, Inc. Response
Virginia Tech Request for Proposal # 648260
PKI Root Key Signing Solution
Released: March 12th, 2010

Prepared by:

John Murray
Senior Vice President Enterprise Sales, Americas
john.murray@globalsign.com

Roy Hugenberger
Senior Account Executive
roy.hugenberger@globalsign.com

GlobalSign, Inc. (eVA Vendor# VS0000032346)
Two International Drive
Suite 105
Portsmouth, New Hampshire 03801-6810
877-SSL-Global
www.globalsign.com
Virginia Tech Request for RFP #648260

Table of Contents

Root Key Signing Specifications and Key Questions ................................................................. 3

VI. Statement of Needs ............................................................................................................ 3

Root Key Specifications ........................................................................................................... 3-5

1. Integration with the VTCA and functional features ......................................................... 6-10

2. Implementation and Support ......................................................................................... 11-14

3. Company Background and Financial Stability .............................................................. 15-18

4. Price ................................................................................................................................. 19-20

5. SWaM Business Utilization ......................................................................................... 21

Security Questionnaire, Attachment B .................................................................................. 22-24

Additional Items/Information Enclosed

1. One (1) bound copy of GlobalSign Certification Practice Statement v. 6.6

2. One (1) bound copy of GlobalSign Certificate Policy v. 3.4
1. Root Key Signing Specification and Related Questions

VI. STATEMENT OF NEEDS:

Root Key Signing Specifications
To meet minimum requirements, the proposed solution shall fulfill the following items A thru D. Specifically state in the proposal if, and how, the proposed solution fulfills these minimum requirements. All references should include the letter beside the relevant line item.

A. CP/CPS of the Root Key Signing CA shall be provided to Virginia Tech for review.

Copies of our current and last version of Certificate Policy (CP) and Certification Practice Statement (CPS) are available in our online legal repository, www.globalsign.com/repository.

One printed copy enclosed of each enclosed herein.

B. Root Key Signing vendor shall provide an evaluation period of at least 30 days to Virginia Tech to allow time for testing and integration of the root key signing solution in the VTCA pre-production test environment.

GlobalSign will request a “test” PKCS #10 (CSR) two to six weeks prior to final signing ceremony as part of the normal Trusted Root implementation process. The signed test certificate will be provided back to Virginia Tech for their internal testing. The test certificate is issued under a test root and allows full technical and integration testing to be performed.

C. The key signed CA certificate issued to Virginia Tech shall contain the following attributes:

• Subject: **Subject entry will be specified by Virginia Tech in the CSR submitted to the root key signing vendor**

This is acceptable but Common Name must contain the following elements:

CN = <Customer name CA>

OU = <Name CA>

O = <Customer Name>

C = <Country Code>

The current VTCA Root Certificate does not contain CN and OU fields: this makes it impossible for relying parties to identify the CA at a glance. Example in Firefox:
GlobalSign will perform independent organizational and requester vetting prior to issuing the signed CA certificate.

- **Public Key:** **RSA (4096)**
  
  Fully Supported

- **Signature Algorithm:** **sha1RSA**
  
  Fully Supported

- **Basic Constraints:** **Subject Type=CA, Path Length=None**
  
  Because of WebTrust for CA requirements and industry standards, we cannot accept Path Length = none for external SubCA’s. Path Length constrains also protects Virginia Tech against – possible accidental – unauthorized CA signing.

  As per RFP 648260 Addendum 01 Questions and Answers, a basic constraint of Path Length = 1 in VTCA Virginia Tech Root. GlobalSign fully supports the proposed VTCA hierarchy including the Class 1 Server CA, Middleware CA and User CA level.

- **Key Usage:** **Certificate Signing, Off-line CRL Signing, CRL Signing**
  
  Fully supported.

The issued CA to Virginia Tech will also include the following elements:

- CRL Distribution Point: **URI:http://crl.globalsign.net/RootSignPartners.crl**
Policy: 1.3.6.1.4.1.4146.1.60

CPS:

Explicit Text: http://www.globalsign.com/repository/

Please note that Virginia Tech can specify additional certificate policies in addition to this one.

Optionally, but recommended by GlobalSign, we can add Authority Information Access which allows automatically location of issuing CA:

CA Issuers: URI: http://secure.globalsign.net/cacert/RootSignPartners-R1.crt

D. The Trusted Root will provide application support for Internet Explorer 7+, Mozilla Firefox 2+, Safari 3+, Microsoft Entourage (OS/X), Mac Mail 3+, Adobe Certified Document Services (CDS)/Adobe 8+, and Java 5+.

We are compliant in all respects with above with the exception of Adobe CDS. Please note, Adobe does not rely on the standard MS-Windows trust store and has its own proprietary trust hierarchy. Additionally to RFP 648260 Addendum 01 Questions and Answers, GlobalSign is a participant in the Adobe Certified Document Services (CDS) program. We have a separate solution specifically geared to the Adobe CDS and currently there is “no” single signing solution that any vendor can provide that will give you the combined Adobe specific and the broader MS-Windows based trust.
1. Integration with the VTCA and Functional Features

1.1. What applications contain the trusted root? (Browsers, Handsets, Email Clients, Application Suites like Adobe)

GlobalSign Root CA Ubiquity/Support Platforms & Application Information

The GlobalSign Root Certificate is present in every popular machine, device, application and platform that utilizes the trust of Public Key Infrastructure (PKI) e.g. SSL/TLS, S/MIME, Code Signing and Document Signing.

In 1998, GlobalSign had the foresight to create a strong Root Certificate by using 2048 bit RSA keys. This makes the GlobalSign Root Certificate the most widely distributed Certification Authority to already meet the NIST (National Institute of Standards & Technology) recommendation that from 2011 onwards all cryptographic keys should be 2048 bit in strength. Anything less than 2048 bit will most likely be deemed insecure, which has prompted the CA/Browser Forum to insist that all Extended Validation SSL Certificates are to be 2048 bit from the 1st January 2009 in anticipation. GlobalSign can offer 2048 bit strength across our entire Digital Certificate portfolio.

GlobalSign is also one of the few Certification Authorities that can offer SGC (Server Gated Cryptography). This enables SSL Certificates to force web servers to create a strong 128 bit encrypted connection with older, weak 40 bit encryption browsers. To customers, the added strength of a 2048 bit root and the inclusion of SGC strong encryption is transparent – and to you, you are safe in the knowledge that the strongest encryption available is always being used to secure your communications.

Extended Validation Browsers
- Microsoft Internet Explorer 7+ (Vista)
- Microsoft Internet Explorer 7+ ( XP)*
- Opera 9.5+
- Firefox 3+
- Google Chrome 0.3.154.9 +
- Apple Safari 3.2 +
- Apple iPhone 3.0 +

Web Browsers (SSL/TLS enabled)
- Microsoft Internet Explorer (IE) 5.01+
- Mozilla Firefox 1.0+
- Opera 6.1+
- Apple Safari 1.0+
- Google Chrome
- AOL 5+
- Netscape Communicator 4.51+
- Red Hat Linux Konqueror (KDE)
• Microsoft WebTV
• Camino
• Konqueror (KDE) 2.0.0 +

**Email Clients (S/MIME)**
• Microsoft Outlook 99+
• Microsoft Entourage (OS/X)
• Mozilla Thunderbird 1.0+
• Qualcomm Eudora 6.2+
• Lotus Notes (6+)
• Netscape Communicator 4.51+
• Mulberry Mail
• Apple Mail
• Mail.app
• Windows Mail
• The Bat

**Major Operating Systems**
• Microsoft Windows XP, Vista and 7
  (all versions inc 32/64 bit)
• Apple MAC OS 9.0+ (circa 2002),
  includes 10.5.X and 10.6.X
• All Major Linux Distributions
  (Debian, Ubuntu etc)

**Default API Support within Hosting Control Panels**
• WHMCS
• Ubersmith

**Mobile OSs, Micro Browsers, Handsets & Game Consoles**
• Apple iPhone, iPod Safari
• Microsoft Windows Mobile 5/6
• Microsoft Windows CE 4.0
• Microsoft Internet Explorer Pocket PC 2003
• Microsoft Internet Explorer Smartphone 2003
• RIM Blackberry 4.3.0
• NTT / DoCoMo
• SoftBank Mobile
• KDDI
• Brew
• PalmOS 5.x
• Netfront 3.0+
• Opera 4.10+
• Openwave mobile browser 6.20+
• Major Operators inc. Vodafone, Orange, AT&T
• Major Handset providers SonyEricsson, Nokia, Alcatel & Palm (S40/S60/S80/OSSO) based
  Handsets from 2002
• Sony PlayStation Portable
• Sony PlayStation 3
• Nintendo Wii

Application Suites
• Microsoft Authenticode & Visual Basic for
  Applications (VBA)
• Adobe AIR
• Sun Java JRE (1.4.2 Update 16+, 5.0 Update 13+, 6 Update 3+)
• Mozilla Suite v0.9.8+
• SeaMonkey
• OpenSSL.org’s OpenSSL v0.9.5+
• Google Checkout

Document Security Platform
• Adobe Certified Document Services (CDS) for
  Adobe PDF
• Microsoft Office (Word, Excel, Powerpoint, Access, InfoPath)

1.2. What are the validity period options for the certificate issued to us? How easily is the certificate issued to us renewed?

The validity period of the signed root CA provided to Virginia Tech is seven (7) to ten (10) years in length. Renewal of SubCA’s after five / six years is recommended. Depending on industry standards at the time (around hash standards and key-sizes), a new Virginia Tech Root CA can at that time also be signed.

1.3. What is the key size of the trusted root?

The GlobalSign Root CA (Offline Root) and RootSign Partner’s CA (Issuing Intermediate CA) are 2,048 Bit (RSA).

1.4. What is the signature algorithm used by the trusted root?

The GlobalSign Root CA (Offline Root) and RootSign Partner’s CA (Issuing Intermediate CA) uses SHA-1 for the signature algorithm.
1.5. Describe the process for submitting a request for a Root Key Signing.

<table>
<thead>
<tr>
<th>TrustedRoot Project Overview</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GlobalSign</strong></td>
<td><strong>Virginia Tech</strong></td>
</tr>
<tr>
<td>Provide Trusted Root Enrollment form</td>
<td></td>
</tr>
<tr>
<td>Provide technical support to the Customer during the enrollment process.</td>
<td>Complete and return at least two weeks prior to certificate generation.</td>
</tr>
<tr>
<td>Review and approve Enrollment Form.</td>
<td>Generate test certificate PKCS #10</td>
</tr>
<tr>
<td>Review and approve requested evaluation certificate contents.</td>
<td></td>
</tr>
<tr>
<td>Sign PKCS #10 certificate with GlobalSign Root CA Test hierarchy</td>
<td></td>
</tr>
<tr>
<td>Return Test certificate.</td>
<td>Import and evaluate test certificate into CA.</td>
</tr>
<tr>
<td>Schedule date for certificate signing ceremony.</td>
<td></td>
</tr>
<tr>
<td>Validate PKSC#10 checksum through out of bound telephone or fax.</td>
<td></td>
</tr>
<tr>
<td>Generate CA Certificate signed by GlobalSign Trusted Root Partner CA</td>
<td></td>
</tr>
<tr>
<td>Return CA Certificate</td>
<td>Validate CA certificate checksum through out of band method typically telephone or fax</td>
</tr>
<tr>
<td>Provide technical support to the Customer during the certificate issuance process</td>
<td>Validate certificate by: Generating lower level certificate and verifying CA chain.</td>
</tr>
</tbody>
</table>

**Notification of Change or Compromise**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify GlobalSign of any changes or updates by authorized Customer contact(s).</td>
<td>Create a record of and report to GlobalSign all actual or suspected compromises of the Private</td>
</tr>
</tbody>
</table>
Key associated with the CA as soon as the suspected compromise is detected.

<table>
<thead>
<tr>
<th>Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain records of data related to the TrustedRoot ceremony of customer, including security and audit data, physical access data to Customer-related material located in the GlobalSign hosting facility and Certificates.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safeguard the security of the Private Key cryptographically related to the Public Key contained in the CA Certificate in accordance with industry practices for similar material.</td>
</tr>
</tbody>
</table>

1.6. In the future, the VTCA may expand its certificate offerings to include object signing certificates. What is the impact of adding additional types of end entity certificate profiles?

Code Signing certificates are not allowed per the terms and conditions of our Trusted Root solution due to WebTrust audit restrictions and embedment requirements by suppliers. GlobalSign can provide coupon codes for obtaining a typically desired quantity code signing certificates via our online system at no charge as part of an agreement.

1.7. Is there any impact if Virginia Tech, in the future, decides to implement additional subordinate CA's that would chain back to the trusted root?

We require disclosure of additional subCA’s and their profiles created by Virginia Tech, but if these are in line with the submitted CA hierarchy and PKI infrastructure there would be no impact.

1.8 What is the publication schedule of the certificate revocation list (CRL) for the trusted root? How will the CRL be made available to Virginia Tech? What is the URL of the trusted root CRL?

The URL is [http://crl.globalsign.net/RootSignPartners.crl](http://crl.globalsign.net/RootSignPartners.crl). We require that the Virginia Tech CA have this URL in the CDP field. The CRL is published with a lifetime of 7 months, but gets refreshed at least every six months.
2. Implementation and Support

2.1. When does the trusted root expire? What happens when it does?

The GlobalSign Root CA expires in 2028. We do not issue SubCA’s under this root which expires after 2028.

GlobalSign has a continuing root embedment program, submitting new Roots at least 5 year in advance of production use to ensure continued root embedment for our customers.

2.2. What is the Subject Entry of your trusted root certificate?
Screen Shot of GlobalSign Root CA (2028), RSA 2,048 Bit
2.3. Does the vendor support a PKCS #10 formatted CSR? What are the requirements for submitting a CSR?

GlobalSign fully supports and requires the PKCS #10 formatted CSR for CA signing events.

Requirements for submission of a CSR are as follows:

- Received and accepted registration form.
- Received and accepted PKI infrastructure document: this includes sections on how Virginia Tech implemented logical, physical and network security controls. It should also describe the proposed CA hierarchy and the type and model + serial numbers of HSM’s used.
- Successful completion and technical testing of the Test CA.
- Completed vetting of the Common Name of the Virginia Tech CA by GlobalSign.
- Verification if the required GlobalSign CDP and policy OID’s are present and if the agreed basic constraints are used.
- Cross-certificate signing is not allowed.

GlobalSign reviewed the (exemplary) policies of VTCA on [www.pki.vt.edu](http://www.pki.vt.edu) and found no obvious show-stoppers for the above requirements.

2.4. Can your company provide Virginia Tech with a pre-production key signed certificate for testing purposes? Can you allow Virginia Tech a minimum 30 day test and evaluation period?

Part of our standard process for implementation of Trusted Root CA signing is to execute a test signing with the customer from the GlobalSign Root CAT (CA Test) infrastructure to ensure that the production signing will go smoothly. This is a test CA is specifically designed for pre-production testing. A minimum 30 day test and evaluation period is no problem and recommended.

2.5. What are the options for contacting the vendor with support issues?

GlobalSign has a project team that is specifically trained to work with customers on the implementation of Trusted Root and to provide ongoing support of all GlobalSign related functions and responsibilities. A project management contact from our client service group will be assigned to be a point of contact for all pre and post signing related queries. Staff is generally available from 8 AM to 7 PM EST, Monday through Friday.

2.6. Does the vendor require an audit of the VTCA?

Per our Trusted Root Terms and Conditions (Section 10 Below), GlobalSign requires Virginia Tech to self report annual information related to the quantities of certificates issues from their CA environment and its compliance with the published CPS and GlobalSign requirements in point 2.8.
“Customer shall keep reasonable records relating to any of Customer’s responsibilities and obligations under this Agreement. Within thirty (30) calendar days following each anniversary date of this Agreement, Customer agrees to certify to Supplier in writing (i) the total number of certificates issued under or from the Trusted Root CA, and (ii) its compliance with the terms and conditions of this Agreement.

During the Agreement and for a period of one (1) calendar year thereafter, Supplier may, upon reasonable notice and during normal business hours, periodically audit Customer’s compliance with the Agreement.”

2.7. Can the company refer us to any universities that are using their root key signing service?

GlobalSign can provide university references upon request and subsequent approval by our customer to speak with Virginia Tech regarding their experience with our Trusted Root solution and implementation process.

2.8. List any special requirements for implementing a root key signing solution.

1. Written Documentation regarding physical and logical security relevant to Virginia Tech’s CA infrastructure.
2. Provide GlobalSign a CPS (Certificate Practice Statement) with ninety (90) days of production key ceremony
3. Maintain key material in cryptographic hardware meeting the FIPS 140-2 Level 3 standard.
4. Use of SubCA’s constraints to Virginia Tech employees, students and business partners. No commercial reselling allowed.
5. Cross-certificate signing not allowed.
6. Virginia Tech CA follows GlobalSign X509 requirements outlined in Statement of Needs, section B

2.9. How will the expiration date of the contract between Virginia Tech and the vendor impact the certificates that were issued prior to the contract end date? Is there a cutoff date for issuing certificates before the contract expiration date? If so, how does it affect the validity period of certificates issued prior to this date?

Any TrustedRoot contract is at least three years in length. GlobalSign will revoke the Virginia Tech CA two years after expiration of the contract subject to Virginia Tech upholding the annual security and audit requirements outlined in 2.6.
2.10. The Virginia Tech Root CA is implemented using RSA 4096 bits keys. Does a RSA 4096 bit key size create any implementation issues for your solution?

No it does not. Older applications might have interoperability problems with a RSA 4096 bit root, but this occurs less and less and is unlikely to be a problem for Virginia Tech as they would have surfaced in the current implementation.

2.11. Describe how the addition of a subordinate CA within the VTCA hierarchy will impact the implementation. For example, Virginia Tech may in the future decide to implement a new subordinate CA to issue end entity certificates using an object signing certificate profile.

Additional subordinate CA’s can be added to the VTCA hierarchy, as per section 1.7. Object Signing profile is however not allowed because of reasons outside GlobalSign’s reach (webtrust for CA and vendor embedment requirements). As per point 1.6, we do include object sign certificates free of charge in the TrustedRoot service.

2.12. Describe how the removal of a subordinate CA within the VTCA hierarchy will impact the implementation. For example, Virginia Tech may decide in the future to discontinue using the subordinate VTCA SSL server to issue end entity SSL certificates.

Removal of subordinate CA’s within VTCA hierarchy does not impact the implementation as long as the CA’s are properly revoked and disclosed to GlobalSign.
3. Company Background and Financial Stability

3.1. How long has the company been in business?

GlobalSign has been in business since 1996 and is one of the oldest Certificate Authorities (CA) in the industry.

GlobalSign was established over 14 years ago as one of the world’s first public Certification Authorities and SSL providers. With an initial focus in Europe, GlobalSign soon expanded its operations to serve a worldwide customer base. Throughout its years, a number of prestigious companies have invested in GlobalSign: Belgian Chamber of Commerce, Ubizen, ING Bank and Vodafone - helping sculpt the global organization and industry leading technology

GlobalSign customers and partners benefit from today.

In October 2006, GlobalSign was acquired by the GMO Internet Inc (TSE: 9449) group of companies from CyberTrust and welcomed on board a brand new Management Team comprising of some of the most experienced and respected talent in the Digital Certificate market - with senior staff responsible for establishing and operating a number of wide reaching Certification Authority services.

Additionally, GlobalSign, Inc. has been registered in the eVA program since 2008. Our vendor number is VS0000032346.

3.2. What is the location for ownership and operation of the Offeror, parent company, and
affiliate company?

GlobalSign Inc. is the operating entity that supports the “Americas” market for the GlobalSign Group. The America’s headquarters is located in Portsmouth, New Hampshire. GlobalSign has worldwide offices in the United Kingdom, Belgium, Tokyo (Global HQ), and Shanghai. GlobalSign became part of GMO Internet Group in 2006 which is a publicly traded company on Tokyo Stock Exchange (TSE 9449).

Company Statistics
Issued over 1.4 million Digital Certificates / digital IDs to people, web sites and machines
140,000 SSL Certificates – fastest growing SSL Provider worldwide in August 2008
Over 20 million Digital Certificates rely on the public trust of the GlobalSign root CA certificates

3.3. What other services besides root key signing does the company offer?

GlobalSign is highly focused on delivering highly secure, best of breed PKI (Public Key Infrastructure) based solutions. In addition to our Trusted Root, CA signing solution, we provide a variety of managed services that deliver a full range of X. 509 based certificate solutions. They include the full range of certificate types including SSL (Secure Socket Layer) certificates, Code Signing Certificates, Client Certificates as well as specific signing...
credentials for the Adobe Acrobat environment.

**Core Solutions**

*Server & Network Security* – lifecycle management for multiple enterprise level SSL / TLS Certificates  
*Authentication & Access Control* – VPN lifecycle management for enterprise or personal Digital IDs  
*Secure Email* – S/MIME lifecycle management for enterprise or personal Digital IDs  
*Document Security & Compliancy* – Adobe PDF and Microsoft Office document signing and certification  
*Developer* – code signing services, trusted root signing services and root CA certificate embedding  
*Web Hosting Security* – SSL reselling services designed around hosting billing and deployment requirements

**Core Products**

*SSL Certificates* – SSL / TLS encryption and identity assurance for web sites  
*EV SSL Certificates* – extended validation SSL encryption and identity assurance for next generation browsers  
*Adobe CDS* – hardware Digital IDs / PCI server cards to digitally sign and certify PDF documents using Adobe’s Certified Document Services platform  
*Microsoft Office Digital IDs* – digital signatures for MS Office documents  
*S/MIME Digital IDs* – managed digital signatures & encryption for email  
*Code Signing Certificates* – signing services to protect code signed for Microsoft Authenticode, VB Macros, Adobe AIR, Java, Apple, Mozilla Objects  
*Trusted Root* – CA root signing for enterprise / Gov. CAs / Microsoft Certificate Services

3.4. What certifications does the company have? Does this include WebTrust for CA's?

GlobalSign has part of the WebTrust for CA program and maintained this highly important industry specific certification since 2002. We maintain both the WebTrust for CA certification for all certificates as well as the newer WebTrust for EV certification standard for Extended Validation SSL certificates.

We also are a founding member of the CAB (CA Browser) Forum, the Anti-Phishing Working Group, and a member of the Adobe CDS (Certified Document Service) Program.
3.5. Describe any liability and insurance coverage provided.

From Section 9 of Trusted Root Terms and Conditions, Limitation of Liability.

“SUPPLIER’S AGGREGATE LIABILITY TO CUSTOMER FOR ALL DAMAGES AND IN RESPECT OF ANY AND ALL CAUSES OF ACTION AND CLAIM AT ANY TIME OR TIMES, INCLUDING, WITHOUT LIMITATION, ANY BREACH OF WARRANTY, SHALL NOT EXCEED THE AMOUNT EQUAL TO THE LESSER OF (I) THE FEES ACTUALLY PAID BY CUSTOMER HEREUNDER DURING THE PRECEDING TWELVE (12) MONTHS, OR (II) THE EQUIVALENT OF TWO-HUNDRED AND FIFTY THOUSAND U.S. DOLLAR ($250,000).”
4.1. Does your company offer discounts to educational institutions like Virginia Tech?

GlobalSign has special pricing for all types of educational institutions including K-12 and higher education institutions like Virginia Tech.

4.2. The VTCA issues some certificates that do not require a globally trusted root - these certificates (Middleware) are for internal use only. Can pricing accommodate this situation so that we are only paying for Certificates used by public facing applications?

Our pricing model takes into account all certificates issues from the globally trusted CA infrastructure signed by GlobalSign. If the certificates issued are chained to the root signed by GlobalSign, they would need to be covered by the license provided to Virginia Tech. However, we have provided very aggressive licensing pricing that gives Virginia Tech the flexibility to issue all necessary certificates at very reasonable cost structure.

4.3. How are license fee costs for end entity certificates issued under the root key chain calculated? Is there a charge for certificates that are active (certificate has not expired) but have been revoked? Does the cost vary based on the type of certificate being issued such as personal, SSL server, or object signing?

Trusted Root customers can issue either SSL or Client certificates. There are different price implications for each type of certificate issued.

License fees are calculated based on the number of “active” SSL certificates deployed (excluding cancelled and revoked certificates). Personal or Client Certificates are calculated based on the number of active “users” issued certificates. A “user” could have multiple certificates for different uses (i.e. one for client authentication, one for S/MIME) and it would only count as one (1) user towards the client certificate portion of the license.

4.4. What is the price and what is included in any one time setup fees, annual support fees, and
renewal of the root key signed certificate, and any other expenses for the proposed solution? Which items are essential for a functioning system, and which are optional add-ons?

One Time Setup Fee for Initial Key Ceremony, $9,300.00
Cost per Active SSL Certificate (Internal, Middleware, Public Facing) $28.00
Cost per Active Client/Personal Certificate User, $5.00
CA Renewal Key Ceremony, $6,500.00

**Estimated First Year Cost (Based on VT 2010 estimates).**

Initial Key Ceremony, $9,300.00
SSL Certificates (Internal, External, Middleware) 724 active @ $28.00 each=$20,272.00
Client/Personal Certificates, 706 active users @ $5.00 each=$3,530.00

**Total Cost Year One (License and One Time), $33,102.00**
Year Two License Cost (assumes 25% YOY cert growth), $29,753.00

4.5. Describe how your solution will impact users of certificates that were issued by the VTCA prior to the implementation of your solution.

Existing users of non-trusted VTCA would not be impacted by the new CA hierarchy other than if they wanted the benefit of “trusted” personal certificates. They would need to obtain a new certificate from the new trusted CA. If they were using their VTCA certificate to encrypt email (S/MIME) they would need to maintain the related key pair on their system to read the previously encrypted emails.

4.6. Describe what impact the issuance of wildcard end entity certificates will have on your solution. Does this impact pricing?

GlobalSign permits the issuance of any valid type of SSL certificate including “wildcards” and certificates using SAN’s (Subject Alternative Names) as part of this agreement. A wildcard or SAN certificate would count as just one (1) active certificate against the SSL portion of license.

4.7. Is there a minimum number of end entity certificates that must be issued?

License pricing is based on an estimated number of certificates issued in each category (i.e. SSL, Client). The customer would pay GlobalSign annually for the projected number of certificates to be issued for the following term at the contract anniversary date. GlobalSign allows up a 10% variance over the stated quantities agreed to by GlobalSign and Virginia Tech. GlobalSign does not provide a rebate if Virginia Tech does not issue up to the stated quantities in the license agreement. However, if Virginia Tech projections should change drastically in either direction, we can make amendments to the agreement as necessary or adjust the license accordingly during the annual contract renewal process.
5. SWaM - Small, Women-owned and Minority-owned Business Utilization

5.1. If your business cannot be classified as Small, Women-owned, or Minority-owned, describe your plan for utilizing SWaM businesses if awarded a contract.

Due to the sensitive nature of GlobalSign’s technology and business practices does not allow us to utilize third party contractors of this nature to assist with our business execution.

5.2. Describe your ability to provide statistical reporting on actual SWaM subcontracting when requested.

Not applicable.

5.3. If your firm or any business that you plan to subcontract with can be classified as SWaM, but has not been certified by the Virginia Department of Minority Business Enterprise (DMBE), acknowledge the expectation that the certification process will be initiated no later than the time of the award, and the final DMBE certification decision and certification number provided.

Not applicable.
2. Security Questionnaire, Attachment B

If purchased, Virginia Tech reserves the right to conduct an IT security assessment on the product(s), system(s) and/or service(s) once delivered to validate the answers to the questions below. If evaluation copies or instances are available for testing, they should be provided to the IT Security Office when requested. In the space following each question, please provide a Yes, No or a “no answer” (N/A), and add any appropriate comments. If the answer is No or N/A, please provide comments indicating how this question/concern is addressed elsewhere or why it is not applicable.

General Comment by GlobalSign

The proposed TrustedRoot service, in response to Virginia Tech RFP# 648260, provides a supplementary service namely Root Key Signing, to the existing Enterprise Certification Authority implemented and operated by Virginia Tech. As such it does not provide a solution on itself, and has no online component.

1. Does your product(s), system(s) and or service(s) protect against the SANS Top 20 security vulnerabilities http://www.sans.org/top20?

Not Applicable. TrustedRoot service enhances the following security vulnerabilities already addressed by Virginia Tech CA. These include Encryption and authentication of internet facing websites, proper authentication and digital signatures for users and relying parties.

2. Does your product(s), system(s) and or service(s) protect against the OWASP http://www.owasp.org/index.php/OWASP_Top_Ten_Project?

Not Applicable. TrustedRoot service enhances the following security vulnerabilities already addressed by Virginia Tech CA. These include A3 Broken authentication and Session Management, A6 Security Misconfiguration, A7 Failure to restrict URL access, A9 insecure cryptographic storage and A10 Insufficient Transport Layer Protection.

3. What specific encryption algorithms are employed for your product(s), system(s) and/or service(s)?

TrustedRoot employs RSA asymmetric key management with SHA/1 hashes. Its use complements the Virginia Tech CA which enables the use of SSL/TLS (with AES, 3DES), S/Mime, IPSEC among others.
4. Is all sensitive data (i.e. Social Security Numbers, Credit Card Numbers, Health Information, etc) encrypted in transit and at rest? If not, please explain? (NOTE: Please see the Sensitive Information page at http://www.security.vt.edu/sensitiveinfo.html for specifics).

Not applicable. TrustedRoot has no online component.

5. Is login information such as user name and password encrypted during transmission from the client to the server? NOTE: Base-64 encoding is not acceptable.

Not applicable. TrustedRoot has no online component.

6. Are operating systems (e.g. Windows or Linux), programming and scripting languages (e.g. Java or PHP), web servers (e.g. Apache or IIS), database servers (e.g. Oracle or MySQL), application servers, etc. always promptly patched and current with security updates? If not, please explain.

Not applicable. TrustedRoot is implemented on the existing Virginia Tech CA. This infrastructure, as per policy published on http://www.pki.vt.edu/, is properly patched at all times.

7. Is all access, including administrative accounts, controlled and logged (i.e. firewalls, file system permissions, ACLs, database table permissions, packet logs, etc.)? If not, please explain.

Not applicable.

8. Does your product(s), system(s) and/or service(s) prevent the use of shared credentials or accounts including administrative accounts?

Not applicable.

9. Describe how your product(s), system(s) and/or service(s) authenticates and authorizes users?

Not applicable. During implementation, GlobalSign will properly vet the requester of the SubCA, and Virginia Tech as an organization through outside sources.

10. Does your product(s) and/or system(s) facilitate compliance with Federal and State laws, such as FERPA, HIPPA and PCI?

Not applicable.
11. Does your company alert customers to vulnerabilities and security issues in a timely fashion? If so, please describe your process.

GlobalSign alerts our TrustedRoot customers on new security standards and requirements and follow up on implementation. We base ourselves on industry reports by NIST, our own research and input from our Auditors and vendors in which GlobalSign’s root is present.

For hosted services, in addition to questions above

All below questions not applicable to Trusted Root as it is not a hosted service.

1. Are intrusion detection technologies and firewalls utilized on the hosted system(s)?
2. Describe how your facility is physically secured?
3. Does your network or facility undergo vulnerability scanning and penetration testing?
4. Do your employees hold Information Technology Security certifications and/or secure coding certifications? If so, please describe them.
GlobalSign CA
Certificate Policy

Date: May 12th 2009
Version: v.3.4
# Table of Contents

**DOCUMENT HISTORY** ........................................................................................................................... 1  
**ACKNOWLEDGMENTS** ............................................................................................................................ 2  

## 2. INTRODUCTION

2.1 OVERVIEW .................................................................................................................................. 4  
2.2 DOCUMENT NAME AND IDENTIFICATION ............................................................................... 6  
2.3 PKI PARTICIPANTS ......................................................................................................................... 6  
2.4 CERTIFICATE USE .......................................................................................................................... 10  
2.5 POLICY ADMINISTRATION ....................................................................................................... 11  
2.6 DEFINITIONS AND ACRONYMS .................................................................................................. 12  

## 3. PUBLICATION AND REPOSITORY RESPONSIBILITIES ............................................................ 13  
3.1 ACCESS CONTROL ON REPOSITORIES .................................................................................. 13  

## 4. IDENTIFICATION AND AUTHENTICATION ........................................................................... 14  
4.1 NAMING ..................................................................................................................................... 14  
4.2 INITIAL IDENTITY VALIDATION ................................................................................................. 14  
4.3 SUBSCRIBER REGISTRATION PROCESS ................................................................................... 14  
4.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS ............................ 16  

## 5. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .................................................. 17  
5.1 CERTIFICATE APPLICATION FOR A ROOT CERTIFICATE ...................................................... 17  
5.2 CERTIFICATE APPLICATION PROCESSING ............................................................................... 17  
5.3 CERTIFICATE ISSUANCE ............................................................................................................. 17  
5.4 CERTIFICATE GENERATION ...................................................................................................... 17  
5.5 CERTIFICATE ACCEPTANCE ...................................................................................................... 18  
5.6 KEY PAIR AND CERTIFICATE USAGE ....................................................................................... 18  
5.7 CERTIFICATE RENEWAL ........................................................................................................... 19  
5.8 CERTIFICATE REVOCAION ......................................................................................................... 19  
5.9 CERTIFICATE STATUS SERVICES ............................................................................................. 20  
5.10 END OF SUBSCRIPTION............................................................................................................. 20  

## 6. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS ............................................... 21  
6.1 PHYSICAL SECURITY CONTROLS ............................................................................................. 21  
6.2 PROCEDURAL CONTROLS ......................................................................................................... 21  
6.3 PERSONNEL SECURITY CONTROLS .......................................................................................... 22  
6.4 AUDIT LOGGING PROCEDURES ............................................................................................... 22  
6.5 RECORDS ARCHIVAL ................................................................................................................... 23  
6.6 COMPROMISE AND DISASTER RECOVERY .............................................................................. 24  
6.7 CA OR RA TERMINATION .......................................................................................................... 24  

## 7. TECHNICAL SECURITY CONTROLS .................................................................................... 25  
7.1 KEY PAIR GENERATION AND INSTALLATION .......................................................................... 25  
7.2 KEY PAIR RE-GENERATION AND RE-INSTALLATION ............................................................... 25  
7.3 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS ........ 27  
7.4 OTHER ASPECTS OF KEY PAIR MANAGEMENT ...................................................................... 27  
7.5 ACTIVATION DATA ..................................................................................................................... 27  
7.6 COMPUTER SECURITY CONTROLS ............................................................................................ 27  
7.7 LIFE CYCLE SECURITY CONTROLS .......................................................................................... 27  
7.8 NETWORK SECURITY CONTROLS .............................................................................................. 28  

## 8. CERTIFICATE AND CRL PROFILES ............................................................................... 29
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Certificate Profile</td>
</tr>
<tr>
<td>8.2</td>
<td>CRL Profile</td>
</tr>
<tr>
<td>8.3</td>
<td>OCSP Profile</td>
</tr>
<tr>
<td>8.4</td>
<td>Time Stamping Profile for Time Stamping Services</td>
</tr>
<tr>
<td>9.</td>
<td>Compliance Audit and Other Assessment</td>
</tr>
<tr>
<td>10.</td>
<td>Other Business and Legal Matters</td>
</tr>
<tr>
<td>10.1</td>
<td>Fees</td>
</tr>
<tr>
<td>10.2</td>
<td>Financial Responsibility</td>
</tr>
<tr>
<td>10.3</td>
<td>Confidentiality of Business Information</td>
</tr>
<tr>
<td>10.4</td>
<td>Privacy of Personal Information</td>
</tr>
<tr>
<td>10.5</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>10.6</td>
<td>Representations and Warranties</td>
</tr>
<tr>
<td>10.7</td>
<td>Disclaimers of Warranties</td>
</tr>
<tr>
<td>10.8</td>
<td>Limitations of Liability</td>
</tr>
<tr>
<td>10.9</td>
<td>Indemnities</td>
</tr>
<tr>
<td>10.10</td>
<td>Term and Termination</td>
</tr>
<tr>
<td>10.11</td>
<td>Individual Notices and Communications with Participants</td>
</tr>
<tr>
<td>10.12</td>
<td>Amendments</td>
</tr>
<tr>
<td>10.13</td>
<td>Dispute Resolution Procedures</td>
</tr>
<tr>
<td>10.14</td>
<td>Governing Law</td>
</tr>
<tr>
<td>10.15</td>
<td>Compliance with Applicable Law</td>
</tr>
<tr>
<td>10.16</td>
<td>Miscellaneous Provisions</td>
</tr>
<tr>
<td>11.</td>
<td>List of Definitions</td>
</tr>
<tr>
<td>12.</td>
<td>List of Acronyms</td>
</tr>
</tbody>
</table>


Document History

Distribution List

<table>
<thead>
<tr>
<th>Version</th>
<th>Company</th>
<th>Name + Title</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2.0</td>
<td>30.06.05</td>
<td>Andreas Mitrakas</td>
<td>Second version</td>
</tr>
<tr>
<td>V2.1</td>
<td>26.1.07</td>
<td>Johan Sys</td>
<td>Distributed to Policy Board</td>
</tr>
<tr>
<td>V2.2</td>
<td>19.6.07</td>
<td>Johan Sys</td>
<td>Distributed to Policy Board</td>
</tr>
<tr>
<td>V2.3</td>
<td>14.11.07</td>
<td>Steve Roylance</td>
<td>Distributed to Policy Board</td>
</tr>
<tr>
<td>V3.0</td>
<td>17.12.07</td>
<td>Steve Roylance</td>
<td>Distributed to Policy Board</td>
</tr>
<tr>
<td>V3.1</td>
<td>18.04.08</td>
<td>Steve Roylance</td>
<td>Distributed to Policy Board</td>
</tr>
<tr>
<td>V3.2</td>
<td>05.12.08</td>
<td>Steve Roylance</td>
<td>Distributed to Policy Board</td>
</tr>
<tr>
<td>V3.3</td>
<td>11.02.09</td>
<td>Steve Roylance</td>
<td>Distributed to Policy Board</td>
</tr>
<tr>
<td>V3.4</td>
<td>12.05.09</td>
<td>Steve Roylance</td>
<td>Distributed to Policy Board</td>
</tr>
</tbody>
</table>

Document Change Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Author</th>
<th>Status + Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3.0</td>
<td>17.12.07</td>
<td>Steve Roylance</td>
<td>Administrative update</td>
</tr>
<tr>
<td>V2.3</td>
<td>14.11.07</td>
<td>Steve Roylance</td>
<td>Administrative update</td>
</tr>
<tr>
<td>V 2.2</td>
<td>19.6.07</td>
<td>Johan Sys</td>
<td>Small administrative update</td>
</tr>
<tr>
<td>V 2.1</td>
<td>26.1.07</td>
<td>Johan Sys</td>
<td>Added GlobalSign Root CA R2</td>
</tr>
<tr>
<td>V2.0</td>
<td>30.06.05</td>
<td>Andreas Mitrakas</td>
<td>Second version</td>
</tr>
<tr>
<td>1.1.1</td>
<td>05.09.05</td>
<td>Jean-Paul Declerck</td>
<td>Final version</td>
</tr>
<tr>
<td>V3.0</td>
<td>17.12.07</td>
<td>Steve Roylance</td>
<td>Final Version</td>
</tr>
<tr>
<td>V3.1</td>
<td>20.05.08</td>
<td>Steve Roylance</td>
<td>Modification of RootSign to TrustedRoot</td>
</tr>
<tr>
<td>V3.2</td>
<td>16.12.08</td>
<td>Steve Roylance</td>
<td>Registered GlobalSign Logo and removal of suspension.</td>
</tr>
<tr>
<td>V3.3</td>
<td>11.02.09</td>
<td>Steve Roylance</td>
<td>Support for TrustedRoot TPM</td>
</tr>
<tr>
<td>V3.4</td>
<td>15.05.09</td>
<td>Steve Roylance</td>
<td>Administrative update</td>
</tr>
</tbody>
</table>
Acknowledgments

This GlobalSign CA CP endorses in whole or in part the following industry standards:

- RFC 3039: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 862: Qualified certificate profile.
- ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only).
- The ISO 1-7799 standard on security and infrastructure


This CP has been submitted for assessment of compliance with the requirements of the above-mentioned standards. This CP is assessed according to the requirements of the following schemes:

- AICPA/CICA, WebTrust Program for Certification Authorities.
- AICPA/CICA, WebTrust For Certification Authorities – Extended Validation Audit Criteria.

This CP intends to become compliant with the requirements of the above-mentioned scheme. The dates of compliance will be announced on the web site of GlobalSign.
2. Introduction

This Certificate Policy (CP) of the GlobalSign Certification Authority (hereinafter, GlobalSign CA) applies to the services of the GlobalSign CA that are associated with the issuance of and management of digital certificates issued under the Top Roots managed by GlobalSign. Top Root certificates can be used to manage certificate hierarchies of certification authorities as well as of end entity certificates. This CP can be found on the GlobalSign CA repository at http://www.globalsign.com/repository. This CP may be updated from time to time.

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements". This CP is a certificate policy in broad sense and meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format (RFC 3647 obsoletes RFC 2527). An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and certificate management. While certain section titles are included in this policy according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the certificate management services of the GlobalSign CA. These sections have been omitted. Where necessary additional information is presented as subsections added to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability of the GlobalSign CA with other third party CAs and provides relying parties with advance notice on the practices and procedures of the GlobalSign CA. Additional assertions on standards used in this CP can be found under section “Acknowledgements”.

This CP addresses the technical, procedural personnel policies and practices of the CA in certain services and during the complete life cycle of off line certificate solutions that are issued by the GlobalSign CA.

Request for information on the compliance of the GlobalSign CA with accreditation schemes as well as any other inquiry associated with this CP can be addressed to:

GlobalSign NV
attn. Legal Practices,
Ubicenter,
Philippsite 5
B-3001 Leuven,
Belgium.
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

The GlobalSign CA operates within the scope of activities of GlobalSign NV/SA. This CP addresses the requirements of the CA that issues top level certificates. Top-level certificates are also known as root certificates or anchor certificates. The GSCA also issues other certificate types at varying levels of its hierarchy. More information can be obtained from http://www.globalsign.com/repository.

This CP applies in all cases of offline solutions that are associated with the CA chaining services that GlobalSign makes available. This CP also applies in cases related with the validation of the certificate path for certificates that are issued at lower levels in it's the GlobalSign hierarchy like for example end entity certificates.

This CP is final and binding between GlobalSign NV/SA, a company under public law, with registered office at Ubicenter, Philippsite 5, B-3001 Leuven, VAT Registration Number BE
0459.134.256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (Hereinafter referred to as “GlobalSign”)

and

the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the GlobalSign CA.

For subscribers this CP becomes effective and binding by accepting a subscriber agreement. For subscribers seeking CA chaining services this CP becomes effective by executing a CA chaining agreement with GlobalSign for any of the roots that GlobalSign owns or manages under license. For relying parties this CP becomes binding by merely addressing a certificate related request on a GlobalSign certificate to a GlobalSign directory. The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CP.

2.1 Overview

This CP applies to the specific domain of the GlobalSign CA that address the management of top level or root certificates issued under GlobalSign’s own procedures. The purpose of this CP is to present the GlobalSign practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of top root certificates according to GlobalSign’s own procedures as they are audited in the framework of formal accreditations that it currently pursues. This CP applies to the above-stated domain to the exclusion of any other. This CP aims at facilitating the GlobalSign CA in delivering certification services through discreet CA issuing Client end entity certificates. This certificate type is known as GlobalSign TrustedRoot or TrustedRoot TPM.

This CP sets out the objectives to identify the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of top-level root certificates of GlobalSign. This CP describes the policy requirements to issue, manage and use GlobalSign top-root certificates of GlobalSign. As a top root CA, GlobalSign manages a hierarchy of certificates according to publicised practices to be found under http://www.globalsign.com/repository.

A CP states “what is to be adhered to” and, therefore, set out an operational rule framework for the broad range of GlobalSign products and services. Such level is generally defined by the entity wishing to ensure a level of trust by managing the life cycle of digital certificates. The GlobalSign CP addresses the requirements of the entire application domain of GlobalSign certificates focusing on top root certificates and not just the end entity area.

A GlobalSign Certificate Practice Statement complements this CP and states, “how the Certification Authority adheres to the Certificate Policy”. The Certificate Practice Statement provides the end user with a summary of the processes, procedures and overall prevailing conditions that the Certification Authority will use in creating and maintaining digital certificates it manages. GlobalSign maintains a Certification Practice Statements for general types of entity certificates.

In addition to the CP and Certificate Practice Statement, GlobalSign maintains a range of adjacent documented polices which include but are not limited to addressing such issues as:

- The GlobalSign Limited Warranty Policy that addresses issues on insurance.
- The GlobalSign Data Protection Policy on the protection of personal data
- Business continuity
- Security policy
- Personnel policies
- Key management policies
- Registration procedures
- etc.

A subscriber or relying party of a GlobalSign CA certificate must refer to the GlobalSign CP in order to establish trust on a certificate issued by the GlobalSign Root CA as well as for notices
with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire certificate chain of the GlobalSign certificate hierarchy, including the Top Root CA and operational roots, which can be established on the basis of the assertions of this CP.

All applicable GlobalSign policies have been subjected to continuous audit and scrutiny of authorised third parties. Additional information can be made available upon request.

The exact name of the GlobalSign CA certificates that makes use of this CP is

- GlobalSign Root CA*
- GlobalSign Root CA - R2*
- GlobalSign Root CA - R3*

TrustedRoot** are the GlobalSign services which allow third-party CAs to chain to one of the GlobalSign CA certificates.

- GlobalSign Trusted Platform Module Root CA*

TrustedRoot TPM** is the GlobalSign services which allows third-party CAs to chain to one of the GlobalSign Trusted Platform Module Root CA certificates.

* They are called collectively the GlobalSign CA Root
** They are called collectively TrustedRoot

Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants or sign data electronically. By means of a digital certificate, GlobalSign provides confirmation of the relationship between a named entity (subscriber) and its public key. For the purposes of this CP an end entity is a subscribing third party Certification Authority that seeks to enter the GlobalSign hierarchy. The purpose of entering the GlobalSign hierarchy enhances trust in the hierarchy as well as greater functionality within third party applications such as browsers etc. GlobalSign seeks to maintain a position of leadership with regard to inclusion of its top root in third party application. This endeavour does not undermine, however, the ability of GlobalSign to revise its approach and seek alternative strategies in the future. It is at the discretion of and a duty of the end entity that is a third party CA to assess the value of the GlobalSign services at any point in time and act accordingly.

The process to obtain a digital certificate includes the identification, naming, authentication and registration of the client as well as aspects of certificate management such as the issuance, revocation and expiration of the digital certificate. By means of this procedure to issue digital certificates, GlobalSign provides adequate and positive confirmation about the identity of the user of a certificate and a positive link to the public key that such entity uses. An entity on this instance might include an end use, another certification authority, as it might be required under the circumstances. GlobalSign makes available general-purpose digital certificates that can be used for non-repudiation and authentication. The use of these certificates can be further limited to a specific business or contractual context or transaction level according a warranty policy or other limitations imposed by the applications that certificates are used in.

This CP is maintained by the GlobalSign CA, which is the issuing authority of certificates in the GlobalSign Public Key Infrastructure. In a certificate management environment based on Public Key Infrastructure (PKI), an Issuing Authority is the entity that manages a Trust hierarchy from which all end user certificates inherit Trust.

This CP governs the issuance of GlobalSign TrustedRoot during the application period of the GlobalSign CA Roots. An application period is for example, the time during which a certain CA may issue GlobalSign CA certificates. The application period is indicated in the certificate issued to the GlobalSign TrustedRoot by a hierarchically superior CA within the GlobalSign hierarchy.

This CP is made available on-line in the Repository of the issuing CA under http://www.globalsign.com/repository

The GlobalSign CA accepts comments regarding this CP addressed to the address mentioned above in the Introduction of this document.
2.1.1 GlobalSign TrustedRoot

This CP addresses the requirements for GlobalSign TrustedRoot to be used to appropriately authorized Certification authorities that seek to enter the certificate hierarchy of GlobalSign. Entering the GlobalSign hierarchy is carried out through a CA chaining program that GlobalSign makes available to interested parties. TrustedRoot certificates:

- Are issued by GlobalSign to a third party CA that meets the contractual and policy requirements of GlobalSign TrustedRoot services with regard to operational practices and technical implementation.
- Are issued to CAs only.

2.1.2 Certificate usages

Certain limitations apply to the use of GlobalSign TrustedRoot and TrustedRoot certificates which typically allow for authentication of the third party CA within an application environment in order to facilitate relying parties in establishing the identity of the CA.

Any other use of GlobalSign TrustedRoot and TrustedRoot certificates is forbidden.

2.2 Document Name and Identification

The identifiers under control of GlobalSign which refer to this document are.

1.3.6.1.4.1.4146.1.1 Extended Validation Certificates Policy
1.3.6.1.4.1.4146.1.10 Domain Validation Certificates Policy
1.3.6.1.4.1.4146.1.20 Organization Validation Certificates Policy
1.3.6.1.4.1.4146.1.30 Time Stamping Certificates Policy
1.3.6.1.4.1.4146.1.40 Client Certificates Policy
1.3.6.1.4.1.4146.1.50 Code Signing Certificates Policy
1.3.6.1.4.1.4146.1.60 CA Chaining Policy
1.3.6.1.4.1.4146.1.80 Retail Industry Electronic Data Interchange Client Certificate Policy
1.3.6.1.4.1.4146.1.81 Retail Industry Electronic Data Interchange Server Certificate Policy
1.3.6.1.4.1.4146.1.90 TrustedRoot TPM Policy
1.3.6.1.4.1.4146.1.95 Online Certificate Status Protocol Policy

2.3 PKI participants

2.3.1 GlobalSign Certification Authority

A Certification Authority is an organisation that issues digital certificates that are used in the public domain or within a business or transactions context. GlobalSign is a Certification Authority. Sometimes, a certification authority is also described by the term issuing authority.

GlobalSign is also responsible to draft the policy prevailing in issuing a certain type or class of digital certificate. GlobalSign is also a Policy Authority while this Certificate Policy is a policy for the issuance of GlobalSign TrustedRoot certificates.

To provide notice or knowledge to relying parties functions associated with the revoked certificates requires appropriate publication in a certificate revocation list. GlobalSign operates such a list.

A subject of GlobalSign CA chaining services is a third party CA that successfully contracts with GlobalSign on the delivery of root services. Root certificates are issued for the purpose of authenticating the trust anchor of a hierarchy as well as the certification path prior to relying on a digital certificate issued by a lower hierarchically CA. Any other uses of root certificates are restricted.

Root certificates can be used for any public purposes. As “public”, this CP considers any use that takes place among CAs that is not restricted to uses governed by voluntary agreements under
private law among participants. Closed user groups are also permitted to leverage on the GlobalSign hierarchy.

The GlobalSign CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates. The GlobalSign CA is a Policy Authority with regard to issuing GlobalSign CA certificates. The GlobalSign CA has ultimate control over the lifecycle and management of the GlobalSign CA Root and any subsequent root belonging to its hierarchy.

The GlobalSign CA ensures the availability of all services pertaining to the management of certificates under the GlobalSign CA Root, including without limitation the issuing, revocation, status verification of a certificate including GlobalSign TrustedRoot, as they may become available or required in specific applications. The GlobalSign CA also manages a registration system for all certificate types issued under the GlobalSign CA Root or TrustedRoot.

Appropriate publication is necessary to ensure that relying parties obtain notice or knowledge of functions associated with the revoked certificates. Publication is manifested by including a revoked certificate in a certificate revocation list that is published in an online directory. Issues certificates also appear on directories of issued certificates. The GlobalSign CA operates such directories.

The domain of responsibility of the GlobalSign CA’s comprises of the overall management of the certificate lifecycle including the following actions:

- Issuance
- Revocation
- Renewal
- Status validation
- Directory service

Some of the tasks attributed to the certificate lifecycle are delegated to selected GlobalSign RAs that operate on the basis of a service agreement with GlobalSign as explained below under 1.3.2.

2.3.1.1 GlobalSign outsource agent

GlobalSign relies on outsource agents to operate a secure facility and deliver CA services including the issuance, revocation, renewal and status validation of GlobalSign CA certificates. The GlobalSign outsource agent operates a service to GlobalSign on the basis of a service agreement.

2.3.1.2 Roles of GlobalSign

GlobalSign operates under two discreet roles. Firstly, as a Trust Service Provider to deliver Trust Services to a user community, directly or through an agent. An agent in this case includes third party entities, called Registration Authorities (RAs) that operate under agreement with and within the conditions laid out by GlobalSign.

Secondly GlobalSign operates an international network of Trusted Third Parties (TTP’s) sharing the GlobalSign procedures and using suitable brand name to issue high quality and highly trusted digital certificates to public and private entities. Such partners include GlobalSign accredited Certification Authorities and RAs that operate under an agreement with GlobalSign. This role is typically limited to the issuance of certificates to other certification authorities, which seek to inherit trust that is usually vested in the GlobalSign top root and brand name.

The main activities of GlobalSign are to:

- Manage an international network of RAs, establishing the brand name of GlobalSign as a universal Trusted Third Party leveraging on in PKI technology.
- Manage the life cycle of digital certificates issued to end user entities as well as to other certification authorities and administrators within the GlobalSign domain.
The GlobalSign public certification services aim at supporting secure electronic commerce and on-line business services to address the business and personal requirements of the users of electronic signatures.

2.3.1.3 GlobalSign root and hierarchy

GlobalSign makes available to subscribers a dedicated root hierarchy to ensure the integrity of the end user certificate and the uniqueness of the resources that it makes available. The GlobalSign CA Root belongs to the broader domain of the GlobalSign trust network that includes roots that have been set up to fulfil specific purposes such as the issuance of end user certificates at levels defined by GlobalSign etc. as well as other participating CAs that take advantage from GlobalSign's root, which is embedded in applications. This GlobalSign Certificate Policy addresses the Root level of the GlobalSign hierarchy and provides guidance with regard to the general conditions of the GlobalSign services.

The GlobalSign CA Root has been used to certify each of the private keys of the subsequent third party CA roots. By validating the certificate of such a CA, trust vested in GlobalSign can also be extended to the certified third party CA root.

2.3.2 GlobalSign Registration Authorities

The GlobalSign CA reaches its subscribers through a designated Registration Authorities. An RA requests the issuance and revocation of a certificate under this CP.

An RA submits the necessary data for the generation and revocation of the certificates to the CA.

A GlobalSign RA interacts with the subscriber to deliver public certificate management services to the end-user. A GlobalSign RA:

- Accepts, evaluates, approves or rejects the registration of certificate applications.
- Registers subscribers to GlobalSign CA certification services.
- Attends all stages of the identification of subscribers as assigned by the GlobalSign CA according to the type of certificates they issue.
- Uses official, notarised or otherwise authorised documents to evaluate a subscriber application.
- Following approval of an application, notifying the GlobalSign CA to issue a certificate.
- Initiates the process to revoke a certificate and request a certificate revocation from the GlobalSign CA.

The GlobalSign RA acts locally on approval and authorisation by the GlobalSign CA. The GlobalSign RA acts in accordance with the approved practices and procedures of the GlobalSign CA including this CP and documented GlobalSign RA procedures.

Sometimes to grant a specific certificate type, GlobalSign RAs might rely on certificates issued by third party certification authorities or other third party databases and sources of information. Relying Parties are hereby prompted to seek specific information by referring to the appropriate certificate policies prevailing in managing specific certificate types issued under the GlobalSign Root.

If successful, the evaluation is followed by the issuance of the certificate to the applicant organisation.

Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of GlobalSign RAs.
2.3.3 Subscribers

Subscribers of GlobalSign TrustedRoot are third party CAs that seek to be issued with certificates within a hierarchy managed by GlobalSign. Subscribers of GlobalSign services are also natural persons or legal persons that successfully apply for a CA certificate. Subscribers use electronic signature services within the domain of the GlobalSign. Subscribers are parties that:

- Set the framework of providing certification services with the GlobalSign CA to the benefit of the subject mentioned in a certificate.
- Have ultimate authority over the private key corresponding to the public key that is listed in a subject certificate.

Legal persons must be duly represented by an authorised agent (e.g. an authorised Director).

Legal persons which are natural persons, are conditionally accepted as subscribers for CA chaining services. The relationship of these persons with the CA to be chained to has to be duly explained and justification must be provided to GlobalSign. If representation of a third party is desired, GlobalSign recommends alternative credentials might be required (e.g. attribute or role certificates), which, however, can be arranged on a case-by-case basis.

Subscribers typically hold a valid identification document, such as an identity card, passport or equivalent, which is used as credential in order to issue electronic certificates. Additional identification of the applying organisation is also needed.

2.3.4 Subjects

Subjects of GlobalSign TrustedRoot are third party CAs that seek to be issued with certificates within a hierarchy managed by GlobalSign

Subjects of GlobalSign CA certificates services may be natural persons themselves or they may be associated with a subscriber through a contractual obligation on the subscriber. Subjects use electronic signature services under authorisation of and within the domain that is designated by the subscriber (if applicable). Subjects are parties that:

- Apply for a certificate.
- Are identified in a certificate.
- Hold the private key corresponding to the public key that is listed in a subscriber certificate.

A subject enrolls with the GlobalSign RA or a Service Provider that requires it to use a certificate within the designated service. A subject nominates a named Certificate Applicant also called a Subscriber, to apply for a certificate. A certificate applicant can be any natural person acting on behalf of the subject.

Subjects of GlobalSign CA root certificates are the same as the applying organisation, which is the third party CA that requests GlobalSign for CA chaining services.

2.3.5 Certificate Applicants

A Certificate Applicant is a party wishing to become a subscriber of a certificate. A certificate Applicant is a party designated by the subject to act on the subject's behalf in:

- Applying for a certificate.
- Agreeing with and accepting the CA's subscriber agreement.

The applicant may be:

- The same as the subject itself, where this is a named individual.
- An individual employed by the subject.
- An individual employed by a contractor, or sub-contractor acting upon explicit authorisation.
2.3.6 Relying Parties

Relying parties are natural persons or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate. For example, the GlobalSign operators that receive signed requests from GlobalSign CA subjects are relying parties of the GlobalSign certificates.

To verify the validity of a digital certificate, relying parties must always refer to CA revocation information, currently a Certificate Revocation List (CRL). Validation takes place prior to relying on information featured in a certificate. Alternatively, relying parties may refer to an automated response by using the OCSP protocol where available. Relying parties meet specific obligations as described in this CP.

2.4 Certificate use

Certain limitations apply to the use of GlobalSign CA certificates.

2.4.1 Appropriate certificate usage

Root certificates issued under the GlobalSign CA can be used to issue digital certificates for public domain transactions that require:

- Authentication
- Assurance about the identity of a remote device

Additional uses are specifically designated once they become available to end entities. Unauthorised use of GlobalSign CA certificates may result in an annulment of warranties offered by the GlobalSign CA to subscribers and relying parties.

2.4.2 Prohibited certificate usage

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not permitted.

2.4.3 Certificate extensions

GlobalSign root certificate extensions are defined by the X.509 v.3 standard other standards as well as any other formats including those used by Microsoft and Netscape.

GlobalSign uses certain constraints and extensions for its public PKI services as per the definition of the International Standards Organisation (ISO). Such constraints and extensions may limit the role and position of a CA or subscriber certificate so that such subscribers can be identified under varying roles.

As key usage extension limits the technical purposes for which a public key listed in a certificate may be used. GlobalSign's own certificates may contain a key usage extension that limits the functionality of a key to only signing certificates, certificate revocation lists, and other data.

A certificate policy extension limits the usage of a certificate to the requirements of a business or a legal context. GlobalSign pro-actively supports and participates in the proliferation of industry, government or other certificate policies for its public certificates as it sees appropriate.

2.4.4 Critical Extensions

GlobalSign uses certain critical extensions in the certificates it issues such as:

- A basic constraint in the key usage to show whether a certificate is meant for a CA or not.
- To show the intended usage of the key.
- To show the number of levels in the hierarchy under a CA certificate.
2.5 Policy Administration

The GlobalSign CA is a top root authority (also known as trust anchor) that manages certificates services within its own domain. The GlobalSign CA might also interact with or seek recognition by third party certification authorities.

The Policy Managing Authority of the GlobalSign CA manages this CP. The GlobalSign CA registers, observes the maintenance, and interprets this CP. The GlobalSign CA makes available the operational conditions prevailing in the life-cycle management of certificates issued under the GlobalSign CA root. The operational conditions for each root are publicised in this CP.

2.5.1 Scope

In an effort to invoke credibility and Trust in the publicised GlobalSign CP and to better correspond to accreditation and legal requirements, GlobalSign may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CP and/or CP.

2.5.2 GlobalSign Policy Management Authority

New versions and publicized updates of GlobalSign policies are approved by the GlobalSign Policy Management Authority. The GlobalSign Policy Management Authority in its present organisational structure comprises members as indicated below:

- At least one member of the management of GlobalSign.
- At least two authorised agents directly involved in the drafting and development of GlobalSign practices and policies.

The Management member chairs the GlobalSign Policy Management Authority ex officio.

All members of the GlobalSign Policy Management Authority have one vote. There are no other voting rights reserved for any other party. In case of lock vote the vote of the Chair of the GlobalSign Policy Management Authority counts double.

2.5.3 Acceptance of Updated Versions of the CP

Upon approval of a CP update by the GlobalSign Policy Management Authority that CP is published in the GlobalSign online Repository at [http://www.globalsign.com/repository](http://www.globalsign.com/repository).

GlobalSign publishes a notice of such updates on its public web site at [http://www.globalsign.com](http://www.globalsign.com). The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CP is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the GlobalSign CP.

Subscribers that are affected by changes may file comments with the policy administration organization within 15 days from notice. Only subscribers and the supervisory authority may submit objections to policy changes. Relying parties that are not subscribers do not have the right to submit objections and any such submissions will be regarded as never received.

GlobalSign publishes on its web site at least the two latest versions of its CP.

2.5.3.1 Changes with notification

Updated versions of this CP are notified to auditor as necessary.
2.5.4 Version management and denoting changes

Changes are denoted through new version numbers for the CP. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

2.6 Definitions and acronyms

A list of definitions can be found at the end of this CP.
3. Publication and Repository Responsibilities

GlobalSign publishes information about the digital certificates that it issues in an online publicly accessible repository. GlobalSign reserves its right to publish certificate status information on third party repositories.

GlobalSign retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain policies including this CP. GlobalSign reserves its right to make available and publish information on its policies by any appropriate means within the GlobalSign repository.

All parties who are associated with the issuance, use or management of GlobalSign certificates are hereby notified that GlobalSign may publish submitted information on publicly accessible directories in association with the provision of electronic certificate status information.

GlobalSign refrains from making publicly available certain elements of documents including security controls, procedures, internal security policies etc. However these elements are disclosed in audits associated with formal accreditation schemes that GlobalSign adheres to.

3.1 Access control on repositories

While GlobalSign strives to keep access to its public repository and access to its policy is (e.g. CP, CPS etc.) free of charge, it might charge for services such as the publication of status information on third party databases, private directories, etc.
4. Identification and Authentication

GlobalSign maintains documented practices and procedures to authenticate the identity and/or other attributes of an end-user certificate applicant to a GlobalSign CA or GlobalSign RA prior to issuing a certificate.

GlobalSign uses approved procedures and criteria to accept applications from entities seeking to become GlobalSign CAs, RAs, or other entities operating in or interoperating with GlobalSign’s infrastructure including entities seeking CA chaining services.

GlobalSign authenticates the requests of parties wishing the revocation of certificates under this policy.

GlobalSign maintains appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

4.1 Naming

To identify a subscriber GlobalSign follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names RFC-822 names and X.400 names.

When applying for a TrustedRoot certificate, the applicant’s name must be meaningful unless explicitly permitted in the relevant product description and the GlobalSign CPS. GlobalSign issues certificates to applicants submitting a documented application containing a verifiable name.

GlobalSign does not accept trademarks, logos or otherwise copyrighted graphic or text material for inclusion in its certificates.

4.2 Initial Identity Validation

The identification of the applicant for GlobalSign services including CA chaining services is carried out according to a documented procedure that is implemented by the GlobalSign RAs.

The subscriber identified in the subject field must prove possession of the private key corresponding to the public key being registered with GlobalSign. Such a relationship can be proved by, for example, a digital signature in the certificate request message.

GlobalSign accepts other CAs wishing to enter its own network and operate under its own hierarchy. Following an initial assessment and the signing of a specific agreement with GlobalSign the applicant CA has to provide GlobalSign with certain identification documents including an authorisation letter, articles of association. GlobalSign retains its right to consult third party databases that identify organisations in this regard.

CA chaining services do not require the physical appearance of the customer as long as an agreement between the applicant organisation and GlobalSign has been executed.

4.3 Subscriber registration process

GlobalSign ensures that:
- Subscribers are properly identified and authenticated
- Subscriber certificate requests are complete, accurate and duly authorized.

In particular:
- GlobalSign provides notice to the applicant through its web site at http://www.globalsign.com and the dedicated policy framework published on its repository at http://www.globalsign.com/repository.
Before entering any contractual relationship with the subscriber, GlobalSign makes available a CA chaining agreement, which the applicant must approve prior to placing a request with GlobalSign.

GlobalSign’s policy framework is limited under data protection and consumer protection laws and warranty, as explained in this GlobalSign CP as well as GlobalSign’s Limited Warranty framework.

GlobalSign maintains documented contractual relationships with all third party registration authorities or outsourced agents it uses to deliver certificates.

4.3.1 Documents used for subscriber registration

GlobalSign or an authorized GlobalSign RA verifies by appropriate means and on the basis of a documented procedure, the identity and, if applicable, all specific attributes thereof of applicants of a certificate. In addition to the above, to identify organizations GlobalSign typically obtains certified copies of by-laws, and possibly additional identification elements such as proof of VAT registration etc.

4.3.2 Data needed for subscriber registration

For CA chaining services, evidence requires might include:

- Full name (including surname and given names) of the subscriber.
- Date and place of birth, a nationally recognized identity number, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.

4.3.3 Pseudonyms

Pseudonyms are not permitted for GlobalSign TrustedRoot certificates.

4.3.4 Records for subscriber registration

GlobalSign records all information used to verify the subscriber identity, including any reference number on the documentation used for verification, and any limitations on the validity thereof.

GlobalSign maintains records of the executed CA chaining contract and any material or documents that support the application which also might include but is not limited to:

- CA chaining agreement as approved of and executed by the applicant.
- Consent to the keeping of a record by GlobalSign of information used in registration and any subsequent certificate status change and passing of this information to third parties under the same conditions as required by this CP in the case of the CA terminating its services.
- A statement to the effect that information held in the certificate is correct and accurate.
- Full name of the subscriber.
- Proof of organization context.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.

The records identified above shall be kept for a period of no less than five (5) years following the expiration of a certificate as mandated by business documentation legislation. A GlobalSign RA maintains such records.
4.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests of TrustedRoot certificates, GlobalSign requires a written and undersigned statement of the subscriber requesting the revocation.
5. Certificate Life-Cycle Operational Requirements

All entities within the GlobalSign domain including third party CAs, RAs and subscribers or other participants, have a continuous duty to inform the GlobalSign CA of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or gets revoked.

The GlobalSign CA issues, revokes certificates following an authenticated and duly signed request issued by a GlobalSign RA.

To carry out its tasks, GlobalSign relies on third party agents. GlobalSign, however, assumes responsibility and accountability towards all entities in its domain as well as relying parties, for acts or omissions of all third party agents it may use to deliver services associated with CA operations within the GlobalSign CA.

Certificate Application

5.1 Certificate Application for a root certificate

The application process for a root certificate requires the execution of a CA chaining agreement with GlobalSign. Subsequently the applicant sends to GlobalSign through secure dispatch the required registration data as well as the public key to be included in a root certificate. The GlobalSign RA validates the identity of the applicant on the basis of credentials presented prior to requesting the issuance of a root certificate by the GlobalSign CA.

5.2 Certificate Application Processing

For all certificate types, a GlobalSign RA acts upon a certificate application to validate an applicant’s identity. Subsequently, an RA either approves or rejects a certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

The RA uses documented procedures and adopts its own practices.

5.3 Certificate Issuance

Further to validation and approval of a certificate application, the GlobalSign RA sends a certificate issuance request to the GlobalSign CA.

Requests from the RA are granted approval provided that they are validly made and they contain valid subscriber data, formatted according the GlobalSign CA specifications.

Issued certificates are delivered to the subject.

5.4 Certificate generation

With reference to the issuance and renewal of certificates GlobalSign represents towards all parties that certificates are issued securely according to the conditions set below:

- The procedure to issue a certificate including a root certificate is securely linked to the associated registration and certificate renewal, including the provision of any subscriber generated public key.
- GlobalSign ensures the uniqueness of the distinguished name assigned to the subscriber within its own domain.
- The confidentiality and integrity of registration data is ensured at all times through appropriate means.
- The authentication of RA registrars is ensured through appropriate credentials.
Certificate requests and generation are also supported by robust and tested procedures.
If external registration service providers are used, registration data is exchanged with authenticated registration service providers.
GlobalSign accepts independent audits of its services and practices.

5.5 Certificate Acceptance

An issued GlobalSign CA certificate is deemed accepted by the subscriber when the RA confirms the acceptance of a certificate the CA issues.

Objection to accepting an issued certificate must explicitly be notified to the GlobalSign CA within 5 working days from delivery. Thereafter the root certificate is deemed accepted.

The GlobalSign CA publishes issued certificates.

5.6 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

5.6.1 Subscriber

The obligations of the subscriber include the following ones:

5.6.1.1 Subscriber duties

The duties of subscribers include the following:
1. Accepting all applicable terms and conditions in the CP of GlobalSign published in the GlobalSign Repository.
2. Notifying the GlobalSign CA or a GlobalSign RA of any changes in the information submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a GlobalSign CA certificate when it becomes invalid.
4. Using a GlobalSign CA certificate, as it may be reasonable under the circumstances.
5. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
6. Using secure devices and products that provide appropriate protection to their keys and which were approved prior by GlobalSign.
7. For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
8. Refraining from submitting to GlobalSign or any GlobalSign directory any material that contains statements that violate any law or the rights of any party.
9. Request the revocation of a CA certificate in case of an occurrence that materially affects the integrity of a GlobalSign CA certificate.
10. Refraining from tampering with a certificate.
11. Only using certificates for legal and authorised purposes in accordance with the CP and the CA chaining agreement.

The Subscriber has all above stated duties towards the CA at all times. When the subscriber applies on behalf of a different named Subject certain duties can be mitigated to the Subject, which in return shall have to inform the Subscriber of any eventualities affecting the life cycle of a certificate. In such case of mitigation, duties 2, 3, 4, 5, 6, 8, 9 10, 11 above apply to the Subject and not to the Subscriber.

5.6.1.2 Certificate Life-Cycle Operational Requirements

Subscribers have a continuous duty to inform directly a GlobalSign RA of any and all changes in the information featured in a CA certificate during the validity period of such CA certificate or of
any other fact that materially affects the validity of a certificate. This duty can be exercised either directly by the subscriber or through an agent.

5.6.1.3 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign CA Repositories and web site to assess and rely on information featured therein.

5.6.2 Relying party

The duties of a relying party are as follows:

5.6.2.1 Relying party duties

A party relying on a certificate will:

- Receive notice of the GlobalSign CA and associated conditions for relying parties.
- Validate a GlobalSign CA certificate by using certificate status information (e.g. a CRL or OCSP) published by GlobalSign, in accordance with the certificate path validation procedure, and validate at least those certificate attributes that materially affect the relying party's own signature policy if available.
- Trust a GlobalSign CA certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a GlobalSign certificate only as it may be reasonable under the circumstances.
- Trust a CA certificate only if it has not been revoked.
- Validate at least those certificate attributes that materially affect the relying party's own signature policy or practices.

5.6.2.2 GlobalSign CA Repository and Web site Conditions

Parties, including subscribers and relying parties, accessing the GlobalSign CA Repository and web site agree with the provisions of this CP and any other conditions of use that the GlobalSign CA may make available. Parties demonstrate acceptance of the conditions of usage of the CP by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. Using GlobalSign CA Repositories results is:

- Obtaining information as a result of the search for a CA certificate.
- Verifying the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Obtaining information published on the GlobalSign CA web site.

5.7 Certificate Renewal

Renewal of GlobalSign CA certificates is not supported.

5.8 Certificate Revocation

The identification of the subscriber who applies for a revocation is carried out according to an internal procedure.

Subject to prior agreement with GlobalSign any GlobalSign RA may carry out the identification and authentication of holders seeking to revoke a certificate.

Revocation requests can also be placed directly to the GlobalSign RA at: GlobalSign, Philippsite 5, 3001, Leuven, Belgium or ra@globalsign.com or through the telephone numbers provided in the introduction of this CP or via the revocation form in the GlobalSign Legal repository. www.globalsign.com/repository
Upon request from an RA, the GlobalSign CA revokes the CA certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate's subject.
- The certificate's subject or their appointed subscriber has breached a material obligation under this CP or the CA chaining agreement.
- The performance of a person's obligations under this CP is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate's subject.

The GlobalSign RA requests the revocation of a certificate promptly upon verifying the identity of the requesting party and confirming that it has not been issued in accordance with the procedures required by this CP. Verification of the identity can be done through information elements featured in the identification data that the subscriber has submitted to the GlobalSign RA. Upon request by a GlobalSign RA, the GlobalSign CA takes prompt action to revoke the certificate.

**5.9 Certificate Status Services**

The GlobalSign CA makes available certificate status checking services including CRLs, OCSP where applicable, and appropriate Web interfaces.

**5.10 End of Subscription**

Subscriber subscription ends when a CA certificate is revoked, expired or the service is terminated.
6. Management, Operational, And Physical Controls

This section describes non-technical security controls used by GlobalSign CA to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

6.1 Physical Security Controls

The GlobalSign CA implements physical controls on its own leased or rented premises. GlobalSign requires physical controls by service providers that it uses to deliver its services.

The GlobalSign CA infrastructure is logically separated from other certificate management infrastructure, used for other purposes.

The GlobalSign CA secure premises are located in an area appropriate for high-security operations.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

The GlobalSign CA implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The GlobalSign CA implements a partial off-site backup.

The sites of the GlobalSign CA host the infrastructure to provide the GlobalSign CA services. The GlobalSign CA sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list, which is subject to audit.

6.2 Procedural Controls

The GlobalSign CA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The GlobalSign CA takes measures regarding confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

GlobalSign may exercise vetting of personnel in trusted positions.

GlobalSign pursues the accountability of all actors for actions performed.

The GlobalSign CA implements dual control for critical CA functions.
6.3 Personnel Security Controls

6.3.1 Qualifications, Experience, Clearances
The GlobalSign CA carries out checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Background checks include:
- Misrepresentations by the candidate.
- Any other as it might be deemed necessary.

6.3.2 Training Requirements and Procedures
The GlobalSign CA makes available training for their personnel to carry out CA and RA functions.

6.3.3 Retraining Period and Retraining Procedures
Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

6.3.4 Sanctions against Personnel
GlobalSign CA sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

6.3.5 Controls of independent contractors
Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as GlobalSign CA personnel.

6.3.6 Documentation for initial training and retraining
The GlobalSign CA, and RAs make available documentation to personnel, during initial training, retraining, or otherwise.

6.4 Audit Logging Procedures
Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment. GlobalSign CA implements the following controls:

GlobalSign CA audit records events that include but are not limited to
- Issuance of a certificate
- Revocation of a certificate
- Published CRLs

Audit trail records contain:
- The identification of the operation
- The data and time of the operation
- The identification of the certificate, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation.

Documents that are required for audits include:
- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

GlobalSign CA ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.
Log files and audit trails are archived for inspection by the authorized personnel of GlobalSign CA, the RA and designated auditors. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up.

Auditing events are not given log notice.

6.5 Records Archival

GlobalSign CA keeps internal records of the following items:

- CA certificates for a period of a maximum of 10 years after the expiration of the certificate.
- Audit trails on the issuance of CA certificates for a period of 5 years after issuance of a certificate.
- Audit trail of the revocation of a CA certificate for a period of 5 years after revocation of a certificate.
- CRLs for a minimum of 5 year after expiration or revocation of a CA certificate.
- Support documents on the issuance of CA certificates for a period of 5 years after expiration of a certificate.

GlobalSign CA keeps archives in a retrievable format.

6.5.1 Types of records

GlobalSign CA retains in a trustworthy manner records of GlobalSign CA digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

6.5.2 Retention period

GlobalSign CA retains in a trustworthy manner records of CA certificates for a maximum of 10 years following expiration or revocation.

6.5.3 Protection of archive

Conditions for the protection of archives include:

Only the records administrator (member of staff assigned with the records retention duty) may view the archive:

- Protection against modification of archive, such as storing the data on a write once medium.
- Protection against deletion of archive.
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

6.5.4 Procedures to obtain and verify archive information

To obtain and verify archive information GlobalSign CA maintains records under clear hierarchical control and a definite job description.

GlobalSign CA retains records in electronic or in paper-based format. The GlobalSign CA may require RAs, subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic, in paper-based format or any other format that GlobalSign CA may see fit.

GlobalSign CA may revise record retention terms as it might be required in order to comply with accreditation requirements.
6.6 Compromise and Disaster Recovery

In a separate internal document, GlobalSign CA documents applicable incident, compromise reporting and handling procedures. GlobalSign CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

GlobalSign CA establishes the necessary measures to ensure recovery of the service in case of a disaster, corrupted servers, software or data.

6.7 CA or RA Termination

Before terminating its CA activities, the GlobalSign CA will take steps to transfer to a designated organisation the following information at the GlobalSign CA’s own costs:

- All information, data, documents, repositories, archives and audit trails pertaining to GlobalSign CA.
7. Technical Security Controls

This section sets out the security measures taken by GlobalSign CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares).

7.1 Key Pair Generation and Installation

GlobalSign CA protects its private key(s) in accordance with this CP. For specific types of certificates GlobalSign CA uses private signing keys only for signing CRLs, and OCSP responses in accordance with the designated use of each of these keys.

GlobalSign CA will refrain from using its private keys used within GlobalSign CA in any way outside the scope of GlobalSign CA.

7.1.1 GlobalSign CA Private Key Generation Process

The GlobalSign CA uses a trustworthy process for the generation of its root private key according to a documented procedure. The GlobalSign CA distributes the secret shares of its private key(s).

7.1.1.1 GlobalSign CA Private Key Usage

The private keys of the GlobalSign CA are used to sign GlobalSign CA issued certificates, GlobalSign CA certification revocation lists and OCSP responses. Other usages are restricted.

7.1.1.2 GlobalSign CA Private Key Type

For the CA Root key it uses, the GlobalSign CA makes use of the RSA algorithm with a key length of 2048 bits and a validity period of at least 14 years.

For the operational CA keys it uses the GlobalSign CA makes use of the RSA algorithm with a key length of 2048 bits and a validity period of up to 14 years.

7.1.2 GlobalSign CA Key Generation

The GlobalSign CA securely generates and protects its own private keys, using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of them. The GlobalSign CA implements and documents key generation procedures, in line with this CP.

The key generation is carried out using an algorithm recognized as being fit for the purposes of issuing certificates. GlobalSign uses RSA SHA-1 and RSA SHA-256.

The selected key length and algorithm for CA signing key is recognized as being fit for the purposes of issuing certificates as issued by the CA.

7.2 Key Pair re-generation and re-installation

The GlobalSign CA decommissions and destroys keys used in the past as well as the active tamper-resistant devices and all backup or escrowed copies of its private keys.

7.2.1 GlobalSign CA Key Generation Devices

The generation of the private keys of the GlobalSign CA occurs within a secure cryptographic device.
7.2.1.1 GlobalSign CA Key Generation Controls

The generation of the private key of the GlobalSign CA requires the control of more than one appropriately authorised member of staff serving in trustworthy positions. This action entails dual control.

7.2.2 GlobalSign CA Private Key Storage

The GlobalSign CA uses a secure cryptographic device to store its private keys meeting the appropriate requirements of ISO.

When outside the signature-creation device the GlobalSign private signing key for a certificate is encrypted at all times.

7.2.2.1 GlobalSign CA Key Storage Controls

The storage of the private key of the GlobalSign CA requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

7.2.2.2 GlobalSign CA Key Back Up

The GlobalSign CA’s private keys are backed up, stored and recovered by multiple and appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

7.2.2.3 Secret Sharing

The GlobalSign CA secret shares use multiple authorised holders, to safeguard and improve the trustworthiness of private keys and provide for key recovery. The GlobalSign CA stores its own private keys in several tamper-resistant devices. This action entails dual control.

7.2.2.4 Acceptance of Secret Shares

Before secret shareholders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody.

A secret shareholder receives the secret share within a physical medium, such as a GlobalSign CA approved hardware cryptographic module. The GlobalSign CA keeps written records of secret share distribution.

7.2.3 GlobalSign CA Public Key Distribution

Public key distribution of GlobalSign’s own public key takes place according to GlobalSign’s own practices as well as additional conditions required by Law in Belgium.

The GlobalSign CA documents its own private key distribution and has the ability to alter the distribution of tokens in case token custodians need to be replaced in their role of token custodians.

7.2.4 GlobalSign CA Private Key Destruction

GlobalSign CA private keys are destroyed by at least two trusted operatives present at the end of their lifetime in order to guarantee that they cannot ever be retrieved and used again.

Key destruction process is documented and associated records are archived.
7.3 Private Key Protection and Cryptographic Module Engineering Controls

The GlobalSign CA uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements, which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted.

Hardware and software mechanisms that protect CA private keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting.

GlobalSign CA custodians are assigned with the task to activate and deactivate the private key. The key is then active for a defined time period.

The GlobalSign CA private keys can be destroyed at the end of their lifetimes.

7.4 Other Aspects of Key Pair Management

The GlobalSign CA archives its own public keys. The GlobalSign CA issues subscriber certificates with usage periods as indicated on such certificates.

7.4.1 Computing resources, software, and/or data are corrupted

The GlobalSign CA establishes the necessary measures to ensure full recovery of the service in case of a disaster, corrupted servers, software or data.

If resources or services are not retained under the control of the GlobalSign CA, the CA ensures that any agreement with the resource owner or services provider is compliant with the requirements for disaster recovery.

7.4.2 CA public key revocation

If a GlobalSign CA public key is revoked the GlobalSign CA will immediately:

- Notify all CAs with which it is cross-certified.

7.4.3 CA private key is compromised

If the private key of the GlobalSign CA is compromised, the corresponding certificate will immediately be revoked. Additional measures will be taken including the revocation of all end user certificates.

7.5 Activation Data

The GlobalSign CA securely stores and archives activation data associated with its own private key and operations.

7.6 Computer Security Controls

The GlobalSign CA implements computer security controls.

7.7 Life Cycle Security Controls

The GlobalSign CA performs periodic development controls and security management controls.
7.8 Network Security Controls

The GlobalSign CA maintains a high-level network of systems security including firewalls. Network intrusions are detected. In specific:

- The GlobalSign CA encrypts connections to the RA, using dedicated administrative certificates.
- The GlobalSign CA website provides certificate based Secure Socket Layer connections and anti-virus protection.
- The GlobalSign CA network is protected by a managed firewall and intrusion detection system.
- Accessing GlobalSign CA databases from outside the CAs network is prohibited.
- Internet sessions for request and delivery of information are encrypted.
8. Certificate and CRL Profiles

This section specifies the certificate format, CRL and OCSP and Timestamping formats.

8.1 Certificate Profile


<table>
<thead>
<tr>
<th>Field</th>
<th>Value or Value constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Unique value per Issuer DN</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Object identifier of the algorithm used to sign the certificate – sha1RSA - in accordance with RFC 3279.</td>
</tr>
<tr>
<td>Issuer DN</td>
<td>GlobalSign together with the appropriate intermediate issuing CA appended to the description.</td>
</tr>
<tr>
<td>Valid From</td>
<td>Universal Coordinate Time base Synchronized to the Royal Observatory of Belgium. Encoded in accordance with RFC 5280.</td>
</tr>
<tr>
<td>Valid To</td>
<td>Universal Coordinate Time base Synchronized to the Royal Observatory of Belgium. Encoded in accordance with RFC 5280.</td>
</tr>
<tr>
<td>Subject DN</td>
<td>In accordance with 3.1</td>
</tr>
<tr>
<td>Subject Public Key</td>
<td>Encoded in accordance with RFC 5280</td>
</tr>
<tr>
<td>Signature</td>
<td>Generated and encoded in accordance with RFC 5280</td>
</tr>
</tbody>
</table>

8.1.1 Authority Key Identifier

GlobalSign generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA’s subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

8.1.2 Authority Information Access

GlobalSign generally populates the Authority Information Access extension of X.509 Version 3 end user Subscriber Certificates and if appropriate Intermediate CA Certificates with the URL of the location where a Relying Party can obtain the issuing CA certificate. The criticality field of this extension is set to FALSE.

8.1.3 CRL Distribution Points

Most GlobalSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate’s status. The criticality field of this extension is set to FALSE.
8.1.4 Subject Key Identifier

Where GlobalSign populates X.509 Version 3 certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

8.1.5 Subject Alternative Name

Where GlobalSign populates X.509 Version 3 certificates with a subjectAlternativeName extension, the subjectAlternativeName is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

8.2 CRL Profile

Most GlobalSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate’s status. The criticality field of this extension is set to FALSE.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value or Value constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V2 in accordance with RFC 5280.</td>
</tr>
<tr>
<td>Issuer DN</td>
<td>The Entity who has signed and issued the CRL</td>
</tr>
<tr>
<td>Effective date</td>
<td>Issue date of the CRL. CRLs are effective upon issuance.</td>
</tr>
<tr>
<td>Next update</td>
<td>Date by which the next CRL will be issued.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Object identifier of the algorithm used to sign the certificate – sha1RSA - in accordance with RFC 3279.</td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>160-bit SHA-1 hash of the public key of the CA issuing the Certificate</td>
</tr>
<tr>
<td>CRL Number</td>
<td>A monotonically increasing sequence number in accordance with RFC 5280</td>
</tr>
<tr>
<td>This update</td>
<td>Issuance</td>
</tr>
<tr>
<td>Next Update</td>
<td>Date of Issuance + 3 hours</td>
</tr>
</tbody>
</table>

8.3 OCSP Profile

The GlobalSign CA maintains a record of the OCSP profile it might use in an independent technical document. This will be made available at the discretion of the GlobalSign CA, on request from parties explaining their interest.

8.4 Time Stamping Profile for Time Stamping Services

The GlobalSign CA maintains a record of the Time Stamping profile it might use in an independent technical document. This will be made available at the discretion of the GlobalSign CA, on request from parties explaining their interest.
9. Compliance Audit and Other Assessment

The GlobalSign CA accepts under condition the auditing of practices and procedures it does not publicly disclose. The GlobalSign CA gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content the GlobalSign CA accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CP and accreditation schemes it publicly claims compliance with.

9.1 Compliance Audit and Other Assessment

Information on GlobalSign’s conformance with the requirements of any accreditation scheme can be sought by the organization of such accreditation scheme directly.

GlobalSign has successfully been audited and currently meets the requirements of the accreditation scheme known as WebTrust for CAs. GlobalSign seeks to maintain its accreditation.

GlobalSign accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CP. GlobalSign accepts this auditing of its own practices and procedures that it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by a party to which GlobalSign owes duty.

The CA evaluates the results of such audits before further implementing them.

9.1.1 Audit process conditions

To carry out the audits, there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with GlobalSign nor having any conflicting interests thereof.

An audit is carried out in areas that include but are not limited to the following ones:

- Compliance of GlobalSign operating procedures and principles with the procedures and service levels defined in the CP.
- Management of the infrastructure that implements CA services.
- Management of the physical site infrastructure.
- Adherence to the CP.
- Adherence to relevant laws.
- Asserting agreed service levels.
- Inspection of audit trials, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

With regard to conformance audits, GlobalSign undertakes the responsibility of the performance of any subcontractors it uses to carry out certification operations including those described in the section below.

9.1.1.1 Business Partnerships

To better respond to the diverse certification needs of the distributed population of electronic commerce service providers and users, GlobalSign may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration. GlobalSign may outsource in part or whole certain aspects of the delivery of its services. Regardless of the partner or agent selected to manage certain parts of the certificate life cycle or operations, GlobalSign remains ultimately in charge of the whole process. GlobalSign limits its responsibility thereof according to the conditions in this GlobalSign CP.
9.1.1.2 Secure Devices and Private Key Protection.

GlobalSign supports the use of secure devices and tamperproof equipment to securely issue, manage and store certificates. GlobalSign uses accredited trustworthy hardware to prevent compromise of its private key.
10. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of the GlobalSign CA certificates under this CP as described in this section.

10.1 Fees

The issuance and management of GlobalSign CA certificates is subject to fees which can be quoted on request.

10.1.1 Refund policy

GlobalSign accepts requests for refund in writing. Refund requests must be duly justified and addressed to the Legal Services of GlobalSign. GlobalSign reserves its right to endorse or grant refunds unless they are requested in the framework of a warranty offered by GlobalSign.

10.2 Financial Responsibility

GlobalSign maintains sufficient resources to meet its perceived obligations under this CP. The GlobalSign CA makes this service available on an “as is” basis.

10.3 Confidentiality of Business Information

The GlobalSign CA observes personal data privacy rules and confidentiality rules as described in the GlobalSign CP. Confidential information includes:

- Any personal identifiable information on subscribers, other than that contained in a certificate.
- Reason for the revocation of a CA certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificate and their content.
- Status of a certificate.

GlobalSign does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the GlobalSign CA owes a duty to keep information confidential is the party requesting such information.
- A court order.

The GlobalSign may charge an administrative fee to process such disclosures.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

10.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- Only a single certificate is delivered per inquiry by subscriber or relying party.
- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- Subscribers can consult the information the CA holds about them.
Confidential information may not be disclosed to subscribers nor relying parties. The GlobalSign CA properly manages the disclosure of information to the CA personnel.

The GlobalSign CA authenticates itself to any party requesting the disclosure of information by:
- Presenting an authentication certificate at the request of the subscriber or relying party
- Signing responses to OCSP requests and CRLs.

The GlobalSign CA encrypts all communications of confidential information including:
- The communications link between the CA and the RAs.
- Sessions to deliver certificates and certificate status information.

To incorporate information by reference the GlobalSign CA uses computer-based and text-based pointers that include URLs, etc.

**10.4 Privacy of Personal Information**

GlobalSign CA makes available a specific Data Protection Policy for the protection of personal data of the applicant applying for a GlobalSign CA certificate that they make available through their web site. The GlobalSign CA adheres to the documented Data Protection Policy of GlobalSign NV available from [http://www.globalsign.com/repository](http://www.globalsign.com/repository).


The regulation on the protection of personal data in the Belgium implements the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

GlobalSign CA also acknowledges Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The GlobalSign CA operates within the conditions for the protection of personal data asserted in this CP.

GlobalSign CA has made appropriate representations before the Belgian Data Protection Commission with regard to the archives of personal data it maintains, collects and processes. The Belgian Data Protection Commission can be contacted by post at: Ministry of Justice, Waterloolaan 115, B-1000 Brussels, Belgium (tel. +32 2 5427206)

**10.5 Intellectual Property Rights**

GlobalSign owns and reserves all intellectual property rights associated with its databases, web sites, GlobalSign CA digital certificates and any other publication whatsoever originating from GlobalSign CA including this CP.

The Distinguished names of all CAs of GlobalSign CA, remain the sole property of GlobalSign, which enforces these rights.

Certificates are and remain property of the GlobalSign CA or the rightful owner that licenses certificate management over to GlobalSign. The GlobalSign CA permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of the GlobalSign CA.
The scope of this restriction is also intended to protect subscribers against the unauthorised re-publication of their personal data featured on a certificate.

The GlobalSign CA owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

10.6 Representations and Warranties

The GlobalSign CA uses this CP and a subscriber agreement to convey legal conditions of usage of GlobalSign CA certificates to subscribers and relying parties.

Participants that may make representations and warranties include GlobalSign CA, RAs, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the GlobalSign domain, including the GlobalSign CA, RAs and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify the appropriate RA.

10.6.1 Subscriber Obligations

Unless otherwise stated in this CP, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital certificates.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with the GlobalSign CA.
- Ensuring that the public key submitted to the GlobalSign CA correctly corresponds to the private key used.
- Accepting all terms and conditions in the GlobalSign CA CP and associated policies published in the GlobalSign CA Repository.
- Refraining from tampering with a GlobalSign CA certificate.
- Using GlobalSign CA certificates for legal and authorised purposes in accordance with this CP.
- Notifying GlobalSign CA or a GlobalSign RA of any changes in the information submitted.
- Ceasing to use a GlobalSign CA certificate if any featured information becomes invalid.
- Removing a GlobalSign CA certificate when it becomes invalid.
- Using a GlobalSign CA certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting to GlobalSign CA or any GlobalSign CA directory any material that contains statements that violate any law or the rights of any party.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a GlobalSign CA certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.
- Submit accurate and complete information to GlobalSign in accordance with the requirements of this CP particularly with regards to registration.
- Only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber according to this CP or the executed CA Chaining agreement.
- Exercise absolute care to avoid unauthorized use of its private key.
- Generate subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures.
• Use a key length and algorithm, which is recognized as being fit for the purposes of electronic signatures.
• Notify GlobalSign without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
  • The subscriber's private key has been lost, stolen, potentially compromised; or
  • Control over the subscriber's private key has been lost due compromise of activation data (e.g. PIN code) or
  • Inaccuracy or changes to the certificate content, as notified to the subscriber.

The subscriber is ultimately liable for the choices he or she makes when applying for a certificate. The applicant and GlobalSign must designate the usage of a trustworthy device as well as the choice of organizational context.

As a top root authority and operator of a trust network that makes available a unique and critical service GlobalSign seeks to ensure the trustworthiness of the relationship with the CA chaining subscriber. The subscriber refrains at all times from seeking CA chaining services by other certification authorities at the same time that it use the CA chaining services of GlobalSign. This limitation applies to the whole subscriber organization and not to the designated roots alone.

10.6.2 Relying Party Obligations
A party relying on a GlobalSign CA certificate promises to:
• Have the technical capability to use digital certificates.
• Receive notice of the GlobalSign CA and associated conditions for relying parties.
• Validate a GlobalSign CA certificate by using certificate status information (e.g. a CRL) published by the GlobalSign CA in accordance with the proper certificate path validation procedure.
• Trust a GlobalSign CA certificate only if all information featured on such certificate can be verified via such a validation procedure as being correct and up to date.
• Rely on a GlobalSign CA certificate, only as it may be reasonable under the circumstances.
• Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised.

The obligations of the relying party, if it is to reasonably rely on a certificate, are to:
• Verify the validity or revocation of the CA certificate using current revocation status information as indicated to the relying party.
• Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or this CP.
• Take any other precautions prescribed in the GlobalSign CA certificate as well as any other policies or terms and conditions made available in the application context a certificate might be used.

Relying parties must at all times establish that it is reasonable to rely on a certificate under the circumstances taking into account circumstances such as the specific application context a certificate is used in.

10.6.2.1 Conveying Relying party obligations
In order to give uninhibited access to revocation information and subsequently invoke Trust in its own services, GlobalSign refrains from implementing an agreement with the relying party with regard to controlling the validity of certificate services with the purpose of binding relying parties to their obligations.

Much like it applies to any other participant of GlobalSign public services, however, the use of GlobalSign resources that relying parties make is implicitly governed by the conditions set out in GlobalSign’s policy framework instantiated by the GlobalSign CP.
Relying parties are hereby notified that the conditions prevailing in this CP are binding upon them each time they consult a GlobalSign resource for the purpose of establishing trust and validating a certificate.

10.6.3 Subscriber Liability towards Relying Parties
Without limiting other subscriber obligations stated elsewhere in this CP, subscribers are liable for any misrepresentations they make in CA certificates to third parties that, reasonably rely on the representations contained therein.

10.6.4 GlobalSign CA Repository and Web site Conditions
Parties (including subscribers and relying parties) accessing the GlobalSign CA Repository and web site agree with the provisions of this CP and any other conditions of usage that GlobalSign may make available. Parties demonstrate acceptance of the conditions of usage of the CP by submitting a query with regard to the status of a CA certificate or by anyway using or relying upon any such information or services provided. The GlobalSign CA Repositories include or contain:

- Information provided as a result of the search for a CA certificate.
- Information to verify the status of digital signatures created with a private key corresponding to a public key listed in a certificate.
- Information to verify the status of a digital certificate before encrypting data using the public key included in a certificate.
- Information published on the GlobalSign CA web site.
- Any other services that GlobalSign CA might advertise or provide through its web site.

The GlobalSign CA maintains a certificate repository during the application period and for 5 years after the expiration or revocation of a certificate. To verify its integrity the complete repository will be made available to the GlobalSign RAs for queries at any time.

Additionally, the GlobalSign CA repository is available to relying parties.

10.6.4.1 Reliance at Own Risk
It is the sole responsibility of the parties accessing information featured in the GlobalSign CA Repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a CA certificate. The GlobalSign CA takes all steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the GlobalSign Repositories and web site may result in terminating the relationship between the GlobalSign CA and the party.

10.6.4.2 Accuracy of Information
The GlobalSign CA makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information. The GlobalSign CA, however, cannot accept any liability beyond the limits set in this CP and the GlobalSign CA insurance policy.

10.6.5 GlobalSign CA Obligations
To the extent specified in the relevant sections of the CP, the GlobalSign CA promises to:

- Comply with this CP and its amendments as published under http://www.globalsign.com/repository
- Provide infrastructure and certification services, including the establishment and operation of the GlobalSign CA Repository and web site for the operation of public certificate management services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide and validate application procedures for the various types of certificates that it makes publicly available.
GlobalSign CA Certificate Policy

- Issue electronic certificates in accordance with this CP and fulfil its obligations presented herein.
- Revoke certificates issued according to this CP upon receipt of a valid and authenticated request to revoke a certificate from an RA.
- Publish accepted certificates in accordance with this CP.
- Provide support to subscribers and relying parties as described in this CP.
- Provide for the expiration and renewal of certificates according to this CP.
- Publish CRLs and/or OCSP responses of all revoked certificates on a regular basis in accordance with this CP.
- Provide appropriate service levels according to a service agreement.
- Notify relying parties of certificate revocation by publishing CRLs on the GlobalSign CA repository.

The liability of GlobalSign CA under the above stated article for proven damages is limited to 1 Euro for any individual certificate, directly caused by the occurrences listed above. This limit might be reviewed by GlobalSign. GlobalSign might seek additional insurance coverage against risks emanating from the correctness of the information included in a certificate. GlobalSign makes available a limited warranty policy.

To the extent permitted by law the GlobalSign CA cannot be held liable for:
- Any use of certificates, other than specified in this CP.
- Falsification of transactions.
- Improper use or configuration of equipment, not operated under the responsibility of the CA, used in a transaction involving certificates.
- Compromise of private keys associated with the certificates.
- Loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates.
- The submission of erroneous or incomplete data from an RA, including identification data, serial numbers and public key values.
- Erroneous or incomplete requests for operations on certificates by the RA.
- The use of certificates.
- The use of public or private keys of cross-certified (non-subordinate) CA’s and their relying parties.
- Services delivered to any subscriber that maintains a CA chaining relationship within its own organisation with another certification authority. This limitation applies to the services delivered to the whole customer organisation and not just specific root or roots that the customer has CA chained.

The GlobalSign CA acknowledges it has no further obligations under this CP.

10.6.6 Registration Authority Obligations

A GlobalSign RA operating within the GlobalSign network promises to:
- Generate securely an RA administrator key pair, using a trustworthy system directly or through an agent.
- Provide correct and accurate information in their communications with the GlobalSign CA.
- Ensure that the public key submitted to GlobalSign CA is the correct one (if applicable).
- Generating a new, secure key pair to be used in association with a certificate that they request from GlobalSign CA.
- Receive applications for the GlobalSign CA certificates in accordance with this GlobalSign CP.
- Carry out all verification and authenticity actions prescribed by the GlobalSign CA procedures and this CP.
- Submit to the GlobalSign CA the applicant’s request in a signed message (certificate request).
• Receive, verify and relay to the GlobalSign CA all requests for revocation of a GlobalSign CA certificate in accordance with the GlobalSign CA procedures and the GlobalSign CA CP.
• Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CP.

10.6.7 Information incorporated by reference into a digital certificate
The GlobalSign incorporates by reference the following information in every digital certificate it issues:
• Terms and conditions of the corresponding CP.
• Any other applicable certificate policy as may be stated on an issued GlobalSign certificate.
• The mandatory elements of the standard X.509.
• Any non-mandatory but customised elements of the standard X.509.
• Content of extensions and enhanced naming that are not fully expressed within a certificate.
• Any other information that is indicated to be so in a field of a certificate.

10.6.8 Pointers to incorporate by reference
To incorporate information by reference GlobalSign uses computer-based and text-based pointers. GlobalSign may use URLs, OIDs etc.

10.7 Disclaimers of Warranties
This section includes disclaimers of express warranties.

10.7.1 Limitation for Other Warranties
The GlobalSign CA does not warrant:
• The accuracy of any unverifiable piece of information contained in certificates except as it may be stated in the relevant product description below in this CP and in the GlobalSign CA warranty policy, if available.
• The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

10.7.2 Exclusion of Certain Elements of Damages
In no event (except for fraud or wilful misconduct) is the GlobalSign CA liable for:
• Any loss of profits.
• Any loss of data.
• Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
• Any transactions or services offered or within the framework of this CP.
• Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on, free, test or demo certificates.
• Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

10.8 Limitations of Liability
The total liability of the GlobalSign is limited in accordance with the Limited Warranty Policy of GlobalSign.

Further information on the warranty conditions can be found at: http://www.globalsign.com/repository
10.9 Indemnities

This section contains the applicable indemnities.

10.9.1 Indemnity

To the extent permitted by law the subscriber agrees to indemnify and hold the GlobalSign CA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys’ fees that the GlobalSign may incur as a result of failure to:

- Protect the subscriber's private key,
- Use a trustworthy system as required
- Taking precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber's private key
- Attend to the integrity of the GlobalSign Root.

10.10 Term and Termination

This CP remains in force until notice of the opposite is communicated by the GlobalSign CA on its web site or repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

10.11 Individual notices and communications with participants

The GlobalSign CA accepts notices related to this CP by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from GlobalSign CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individuals communications made to the GlobalSign CA must be addressed to: legal@globalsign.com or by post to the GlobalSign in the address mentioned in the introduction of this document.

10.12 Amendments

Changes to this CP are indicated by appropriate numbering.

The GlobalSign CA Policy Management Authority decides on the numbering of versions.

10.13 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify GlobalSign of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, GlobalSign convenes a Dispute Committee that advises GlobalSign management on how to proceed with the dispute. The Dispute Committee convenes within twenty (20) business days from receipt of a Dispute Notice. The Dispute Committee is composed by a counsel, a data protection officer, a member of GlobalSign operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the Dispute Committee proposes a settlement to the GlobalSign executive
management. The GlobalSign executive management may subsequently communicate the proposed settlement to the resting party.

10.13.1 Arbitration

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CP, parties submit the dispute to arbitration, in accordance with art. 1676-1723 of the Belgian Judicial Code. There will be 3 arbitrators of whom each party proposes one while both parties of the dispute choose the third arbitrator. The place of the arbitration is Leuven, Belgium and the arbitrators determine all associated costs.

For all technology related disputes and disputes related to this CP the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:

J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
Tel.: +32-47-733 82 96, Fax: +32-16-32 54 38.

10.14 Governing Law

This CP is governed, construed and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of GlobalSign digital certificates or other products and services. The law of Belgium apply also to all GlobalSign commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to GlobalSign products and services where the GlobalSign acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including GlobalSign partners, subscribers and relying parties, irrevocably submit to the jurisdiction of the district courts of Leuven, Belgium.

10.15 Compliance with Applicable Law

GlobalSign CA complies with applicable laws of Belgium. Export of certain types of software used in certain GlobalSign CA public certificate management products and services may require the approval of appropriate public or private authorities. Parties (including the GlobalSign CA, subscribers and relying parties) agree to conform to applicable export laws and regulations as pertaining in Belgium.

10.16 Miscellaneous Provisions

10.16.1 Survival

The obligations and restrictions contained under section “Legal Conditions” survive the termination of this CP.

10.16.2 Severability

If any provision of this CP, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CP will be interpreted in such manner as to effect the original intention of the parties.
11. List of definitions

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework.

ACCREDITION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.

APPLICATION FOR A CERTIFICATE
A request sent by a certificate applicant to a CA to issue a digital certificate.

ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.

ASSURANCES
A set of statements or conduct aiming at conveying a general intention.

AUDIT
Procedure used to validate compliance with formal criteria or controls.

AUTHENTICATED RECORD
A signed document containing assurances of authentication or a message with a digital signature verified by a valid Class 3 certificate by a relying party.

AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.

AUTHORIZATION
Granting of rights.

AVAILABILITY
The rate of accessibility of information or resources.

HARDWARE MODULE
The complete system of the hardware module used to keep the certificates and securely generate a key pair.

BINDING
A statement by an RA of the relationship between a named entity and its public key.

CERTIFICATE
The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber's ones.

CERTIFICATE REVOCATION LIST OR CRL
A list maintained by the CA of certificates that are revoked before their expiration time.

CERTIFICATION AUTHORITY OR CA
An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the GlobalSign CA.

CERTIFICATION PRACTICE STATEMENT OR CPS
A statement of the practices in the management of certificates during all life phases.

CERTIFICATE STATUS SERVICE OR CSS
A service, enabling relying parties and others to verify the status of certificates.

CONTRACT PERIOD
The duration of the GlobalSign CA contract between the Dutch National Register and the CA organization.

CERTIFICATE CHAIN
A hierarchical list certificates containing an end-user subscriber certificate and CA certificates.

CERTIFICATE EXPIRATION
The end of the validity period of a digital certificate.

CERTIFICATE EXTENSION
A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.

CERTIFICATE HIERARCHY
A level based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers.

CERTIFICATE MANAGEMENT
Actions associated with certificate management include, storage, dissemination, publication, revocation of certificates.

CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked certificates. Such list is to me consulted by relying parties at all times prior to relying on information featured in a certificate.

CERTIFICATE SERIAL NUMBER
A sequential number that uniquely identifies a certificate within the domain of a CA.

CERTIFICATE SIGNING REQUEST (CSR)
A machine-readable application form to request a digital certificate.

CERTIFICATION
The process to issue a digital certificate.

CERTIFICATION AUTHORITY (CA)
An authority, such as the GlobalSign CA that issues or revokes a digital certificate.

CERTIFICATE POLICY (CP)
A statement of the practices of a CA and the conditions of issuance, revocation etc. of a certificate. A CP is also used as guidance to establish the trustworthiness of a certification services infrastructure.

CERTIFICATE ISSUANCE
Delivery of X.509 v3 digital certificates for authentication and digital signature based on personal data and public keys provided by the RA and compliant with RFC 3647 and RFC 3039

CERTIFICATE REVERSION
Online service used to permanently disable a digital certificate before its expiration date

**CERTIFICATE REVOCATION LISTS**
Online publication of complete and incremental digital certificates revocation lists compliant with RFC 2459

**COMMERCIAL REASONABLENESS**
A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.

**COMPROMISE**
A violation of a security policy that results in loss of control over sensitive information.

**CONFIDENTIALITY**
The condition to disclose data to selected and authorised parties only.

**CONFIRM A CERTIFICATE CHAIN**
To validate a certificate chain in order to validate an end-user subscriber certificate.

**DIGITAL CERTIFICATE**
A formatted piece of data that relates an identified subject with a public key the subject uses.

**DIGITAL SIGNATURE**
To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer’s public key can accurately determine whether the transformation was created using the private key that corresponds to the signer’s public key and whether the initial message has been altered since the transformation was made.

**DISTINGUISHED NAME**
A set of data that identifies a real-world entity, such as a person in a computer-based context.

**DIRECTORY SERVICE**
Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier.

**END-USER SUBSCRIBER**
A subscriber other than another CA.

**ENHANCED NAMING**
The usage of an extended organisation field (OU=) in an X.509 v.3.0 certificate.

**EXTENSIONS**
Extension fields in X.509 v.3.0 certificates.

**GENERATE A KEY PAIR**
A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant’s capacity to use the private key.

**HASH**
An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:
- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

**IDENTIFICATION**
The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.

**INCORPORATE BY REFERENCE**
To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

**KEY GENERATION PROCESS**
The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process.

**KEY PAIR**
A private key and its corresponding public key in asymmetric encryption.

**NOTICE**
The result of notification to parties involved in receiving CA services in accordance with this CP.

**NOTIFY**
To communicate specific information to another person as required by this CP and applicable law.

**NOTARISED TIME STAMPING**
Online service used to timestamp and securely archive a document; the document is re-timestamped on a regular basis with up-to-date technology.

**OBJECT IDENTIFIER**
A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

**PKI HIERARCHY**
A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.

**PRIVATE KEY**
A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.

**PUBLIC KEY**
A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.

**PUBLIC KEY CRYPTOGRAPHY**
Cryptography that uses a key pair of mathematically related cryptographic keys.
PUBLIC KEY INFRASTRUCTURE (PKI)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

REGISTRATION AUTHORITY OR RA:
An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.

RELATIVE DISTINGUISHED NAME (RDN)
A set of attributes that distinguishes the entity from others of the same type.

RELIANCE
To accept a digital signature and act in a way that shows trust in it.

RELYING PARTY
Any entity that relies on a certificate for carrying out any action.

REPOSITORY
A database and/or directory listing digital certificates and other relevant information accessible on-line.

REVOKE A CERTIFICATE
To permanently end the operational period of a certificate from a specified time forward.

SECRET SHARE
A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.

SECRET SHARE HOLDER
An person that holds a secret share.

SHORT MESSAGE SERVICE (SMS)
A service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication.

SIGNATURE
A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.

SIGNER
A person who creates a digital signature for a message, or a signature for a document.

SMART CARD
A hardware token that contains a chip to implement among others cryptographic functions.

STATUS VERIFICATION
Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs.

SUBJECT OF A DIGITAL CERTIFICATE
The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.

SUBSCRIBER AGREEMENT
The agreement between a subscriber and a CA for the provision of public certification services.

TRUSTED POSITION
A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, or revocation of certificates, including operations that restrict access to a repository.

TPM
Trusted Platform Module — A hardware cryptographic device which is defined by the Trusted Computing Group. [https://www.trustedcomputinggroup.org/specs/TPM](https://www.trustedcomputinggroup.org/specs/TPM).

TRUSTWORTHY SYSTEM
Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

GLOBAL SIGN CA REGISTRATION AUTHORITY:
An entity that verifies and provides all subscriber data to the GlobalSign CA.

GLOBAL SIGN CA PUBLIC CERTIFICATION SERVICES
A digital certification system made available by GlobalSign CA as well as the entities that belong to the GlobalSign CA domain as described in this CP.

GLOBAL SIGN CA PROCEDURES
A document describing the GlobalSign CA’s internal procedures with regard to registration of end users, security etc.

WEB — WORLD WIDE WEB (WWW)
A graphics based medium for the document publication and retrieval of information on the Internet.

WRITING
Information accessible and usable for reference.

X.509
The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.
12. List of acronyms

CA: Certification Authority
CEN/ISSS: European Standardisation Committee / Information Society Standardisation System
CP: Certificate Policy
CPS: Certification Practice Statement
ETSI: European Telecommunications Standards Institute
GSCA: GlobalSign Certification Authority
IETF: Internet Engineering Task Force
ISO: International Standards Organisation
ITU: International Telecommunications Union
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RFC: Request for Comments
SSCD: Secure Signature Creation Device
VAT: Value Added Tax
# Table of Contents

**DOCUMENT HISTORY** ................................................................................................................................. 3  
**HISTORY** .......................................................................................................................................................... 3  
**ACKNOWLEDGMENTS** ........................................................................................................................................... 4  

## 1.0 INTRODUCTION ........................................................................................................................................ 5  
1.1 OVERVIEW ................................................................................................................................................... 6  
1.2 GLOBALSign CERTIFICATE TYPES ........................................................................................................... 8  
1.3 PERSONALSign DEMO AND PERSONALSign 1 ......................................................................................... 10  
1.4 PERSONALSign 2 ........................................................................................................................................... 12  
1.5 PERSONALSign 2 PRO AND DOCUMENTSign .......................................................................................... 14  
1.6 PERSONALSign 3 ........................................................................................................................................... 16  
1.7 PERSONALSign 3 PRO .................................................................................................................................. 18  
1.8 ORGANIZATIONSSL .................................................................................................................................... 20  
1.9 DOMAINSsl ................................................................................................................................................... 22  
1.10 EXTENDEDSSL ............................................................................................................................................ 24  
1.11 EDUCATIONAL SERVERSign .................................................................................................................... 30  
1.12 CODE SIGNING ............................................................................................................................................ 31  
1.13 GLOBALSign TIME STAMPING .................................................................................................................. 33  
1.14 CERTIFICATE USAGES .................................................................................................................................. 35  
1.15 DOCUMENT NAME AND IDENTIFICATION ............................................................................................. 36  
1.16 PKI PARTICIPANTS ....................................................................................................................................... 36  
1.17 CERTIFICATE USE ......................................................................................................................................... 41  
1.18 POLICY ADMINISTRATION ....................................................................................................................... 42  
1.19 DEFINITIONS AND ACRONYMS ................................................................................................................. 43  

## 2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES ................................................................................. 44  
2.1 ACCESS CONTROL ON REPOSITORIES ................................................................................................. 44  

## 3.0 IDENTIFICATION AND AUTHENTICATION .................................................................................................. 45  
3.1 NAMING ......................................................................................................................................................... 45  
3.2 INITIAL IDENTITY VALIDATION ................................................................................................................ 45  
3.3 SUBSCRIBER REGISTRATION PROCESS ..................................................................................................... 46  
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS ........................................... 50  

## 4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .......................................................................... 51  
4.1 CERTIFICATE APPLICATION ......................................................................................................................... 51  
4.2 CERTIFICATE APPLICATION PROCESSING ................................................................................................ 51  
4.3 CERTIFICATE ISSUANCE ............................................................................................................................... 52  
4.4 CERTIFICATE GENERATION ......................................................................................................................... 52  
4.5 CERTIFICATE ACCEPTANCE ......................................................................................................................... 52  
4.6 KEY PAIR AND CERTIFICATE USAGE ......................................................................................................... 52  
4.7 CERTIFICATE RENEWAL .............................................................................................................................. 54  
4.8 CERTIFICATE REVOCATION ........................................................................................................................ 54  
4.9 CERTIFICATE STATUS SERVICES ............................................................................................................. 56  
4.10 END OF SUBSCRIPTION ............................................................................................................................ 56  
4.11 CERTIFICATES PROBLEM REPORTING AND RESPONSE CAPABILITY .................................................. 56  
4.12 CERTIFICATE EXPIRY ............................................................................................................................... 56  

## 5.0 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS ........................................................................ 57  
5.1 PHYSICAL SECURITY CONTROLS ................................................................................................................ 57  
5.2 PROCEDURAL CONTROLS ............................................................................................................................ 57  
5.3 PERSONNEL SECURITY CONTROLS .......................................................................................................... 58  
5.4 AUDIT LOGGING PROCEDURES .................................................................................................................. 59
5.5 RECORDS ARCHIVAL .................................................................................................................. 59
5.6 COMPROMISE AND DISASTER RECOVERY ........................................................................... 61

6.0 TECHNICAL SECURITY CONTROLS ...................................................................................... 62
6.1 KEY PAIR GENERATION AND INSTALLATION ...................................................................... 62
6.2 KEY PAIR RE-GENERATION AND RE-INSTALLATION ............................................................... 63
6.3 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .... 64
6.4 OTHER ASPECTS OF KEY PAIR MANAGEMENT ..................................................................... 64
6.5 ACTIVATION DATA ..................................................................................................................... 65
6.6 COMPUTER SECURITY CONTROLS ......................................................................................... 65
6.7 LIFE CYCLE SECURITY CONTROLS ......................................................................................... 65
6.8 NETWORK SECURITY CONTROLS ........................................................................................... 65
6.9 TIME-STAMPING SERVICES .................................................................................................. 65
6.10 KEY PAIR AND CSR GENERATION BY GLOBALSIGN .......................................................... 65

7.0 CERTIFICATE AND CRL PROFILES .................................................................................... 67
7.1 CERTIFICATE PROFILE ............................................................................................................ 67
7.2 CRL PROFILE .......................................................................................................................... 68
7.3 OCSP PROFILE ........................................................................................................................ 68
7.4 TIME STAMPING PROFILE FOR TIME STAMPING SERVICES ............................................. 68

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENT ................................................................ 69
8.1 COMPLIANCE AUDIT AND OTHER ASSESSMENT ................................................................. 69

9.0 OTHER BUSINESS AND LEGAL MATTERS ......................................................................... 71
9.1 FEES ......................................................................................................................................... 71
9.2 FINANCIAL RESPONSIBILITY .................................................................................................. 71
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION ............................................................... 71
9.4 PRIVACY OF PERSONAL INFORMATION ............................................................................... 72
9.5 INTELLECTUAL PROPERTY RIGHTS .................................................................................... 72
9.6 REPRESENTATIONS AND WARRANTIES ............................................................................... 73
9.7 DISCLAIMERS OF WARRANTIES ................................................................................................ 77
9.8 LIMITATIONS OF LIABILITY .................................................................................................... 77
9.9 INDEMNITIES .......................................................................................................................... 78
9.10 TERM AND TERMINATION ..................................................................................................... 79
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS ................................ 79
9.12 AMENDMENTS ....................................................................................................................... 79
9.13 DISPUTE RESOLUTION PROCEDURES .................................................................................. 79
9.14 GOVERNING LAW ................................................................................................................... 80
9.15 COMPLIANCE WITH APPLICABLE LAW ............................................................................. 80
9.16 MISCELLANEOUS PROVISIONS ............................................................................................ 80

10.0 LIST OF DEFINITIONS ........................................................................................................... 81

11.0 LIST OF ACRONYMS ............................................................................................................ 87
Document History

Document Change Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Author</th>
<th>Status + Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V.5.0</td>
<td>10/07/05</td>
<td>Andreas Mitrakas</td>
<td>Draft</td>
</tr>
<tr>
<td></td>
<td>30/08/05</td>
<td>Jean-Paul Declerck</td>
<td>Final version</td>
</tr>
<tr>
<td>v.5.1</td>
<td>02/02/06</td>
<td>Johan Sys</td>
<td>Administrative clean-up</td>
</tr>
<tr>
<td>v.5.2</td>
<td>13/03/06</td>
<td>Johan Sys</td>
<td>Added GlobalSign Educational ServerSign</td>
</tr>
<tr>
<td></td>
<td>29/11/06</td>
<td>Philippe Deltombe</td>
<td>Added GlobalSign OrganizationSSL</td>
</tr>
<tr>
<td>v.5.3</td>
<td>6/12/06</td>
<td>Johan Sys</td>
<td>Removed Sureserver products</td>
</tr>
<tr>
<td></td>
<td>23/01/07</td>
<td>Johan Sys</td>
<td>Added GlobalSign DomainSSL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Added GlobalSign Root CA R2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Adjusted liability gaps</td>
</tr>
<tr>
<td>v.5.4</td>
<td>30/03/07</td>
<td>Johan Sys</td>
<td>Administrative update / clarifications</td>
</tr>
<tr>
<td>v.5.5</td>
<td>19/6/07</td>
<td>Johan Sys</td>
<td>Renamed product names</td>
</tr>
<tr>
<td>v.5.6</td>
<td>25/06/07</td>
<td>Steve Roylance</td>
<td>Final modification for EV Issue 1.0</td>
</tr>
<tr>
<td>v.6.0</td>
<td>17/12/07</td>
<td>Steve Roylance</td>
<td>Major Release supporting new certificate lifecycle solutions</td>
</tr>
<tr>
<td>v.6.1</td>
<td>20/05/08</td>
<td>Steve Roylance</td>
<td>Administrative update/clarifications</td>
</tr>
<tr>
<td>v.6.2</td>
<td>13/10/08</td>
<td>Steve Roylance</td>
<td>Administrative update/clarifications</td>
</tr>
<tr>
<td>v.6.3</td>
<td>16/12/08</td>
<td>Steve Roylance</td>
<td>Administrative update/clarifications</td>
</tr>
<tr>
<td>v.6.4</td>
<td>11/02/09</td>
<td>Steve Roylance</td>
<td>Administrative update/clarifications</td>
</tr>
<tr>
<td>v.6.5</td>
<td>12/05/09</td>
<td>Steve Roylance</td>
<td>Administrative update/clarifications</td>
</tr>
<tr>
<td>v.6.6</td>
<td>03/02/10</td>
<td>Lila Kee</td>
<td>Administrative update</td>
</tr>
</tbody>
</table>

History

Changes in v.6.6 (publication date : 27th January 2010) with respect to v.6.5
- Administrative changes supporting delivery of ObjectSign to Individuals. Rename ObjectSign to CodeSigning

Changes in v.6.5 (publication date : 12th May 2009) with respect to v.6.4
- Administrative changes

Changes in v.6.4 (publication date : 11th February 2009) with respect to v.6.3
- Administrative changes
- Support of timestamping certificate services.
- Support of TrustedRoot TPM and DocumentSign

Changes in v.6.3 (publication date : 16th December 2008) with respect to v.6.2
- Administrative changes
- Support of enhanced validation and application processes – higher degree of automation.

Changes in v.6.2 (publication date : 13th October 2008) with respect to v.6.1
- Administrative changes

Changes in v.6.1 (publication date : 20th May 2008) with respect to v.6.0
- Administrative changes
- SubjectAlternativeName and non public domain support

Changes in v.6.0 (publication date : December 17th 2007) with respect to v.5.6
- Removal of the HyperSign product range
- The addition of role and department based PersonalSign Pro 2 certificates.
- The option for GlobalSign to generate Private Key pairs and CSRs on behalf of the applicant
- The use of API functions for all products.
- Minor administrative changes to aid readability.

Changes in v.5.6 (publication date : June 25 2007) with respect to v.5.6
- Administrative changes
- Incorporation of modifications to support EV Guidelines at Issue 1.0

Changes in v.5.5 (publication date : June 19 2007) with respect to v.5.5
- Administrative changes
- Renamed some products
Changes in v.5.4 (publication date: March 30 2007) with respect to v.5.3
- Administrative changes

Changes in v.5.3 (publication date: Jan 26 2007) with respect to v.5.2
- Added GlobalSign DomainSSL product
- Added GlobalSign Root CA R2
- Adjusted Liability gap for OrganizationSSL and ExtendedSSL

Changes in v.5.2 (publication date: December 2006) with respect to v.5.1
- Added GlobalSign ExtendedSSL product
- Removed Sureserver products, Renamed GlobalSign Educational ServerSign to GlobalSign Education
  GlobalSign OrganizationSSL.
- Administrative changes

Changes in v.5.1 (Publication Date: 13 March 2006) with respect to v.5.0
- Added GlobalSign Educational ServerSign product

Changes in v.5.0 (Publication Date: 10 July 2005) with respect to v.4.3.2
- Adaptation to the RFC 3647 format
- Separation of Data protection policy, warranty policy and consumer policy.
- Updated references to GlobalSign Certificate Policy

Changes in v.4.3.2 (Publication Date: 8 April 2005) with respect to v.4.3.1
- Separated references to GlobalSign Qualified Certificates product

Changes in 4.3.1 (Publication Date: 10 October 2003) with respect to v.4.3
- Added SureServer product

Changes in 4.3 (Publication Date: 10 October 2003) with respect to v.4.2
- Section 1.4: Updated wording
- Section 4.3.6: Updated wording
- Section 5.13: Updated reference to logs retention period.
- Section 21.10: Updated wording
- Section 21.22: Updated wording
- Section 21.23: Updated wording

Changes in v.4.2 (Publication Date: 1 August 2003) with respect to v.4.1
- New Chapter 21 GlobalSign PersonalSign 3 Qualified certificates issued under Belgian Law of 9 July 2001
  Framework on Electronic Signatures.
- Updated Chapter 10 GlobalSign Limited Warranty Policy to include warranty requirements for product
  named GlobalSign PersonalSign 3 Qualified certificate.
- Updated Section 5.12 on records retention period for Personalsign 3 Qualified certificate.
- Appropriate additions to the definitions list with regard to qualified certificates.
- Minor editorial updates to accommodate PersonalSign 3 Qualified in the Introduction.

Acknowledgments

This GlobalSign CA CPS endorses in whole or in part the following industry standards:
  (obsoletes RFC 2527)
- RFC 3039: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- ETSI TS 101 862: Qualified certificate profile.
- ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised
  level only).
- The ISO 1-7799 standard on security and infrastructure
- CA/Browser Forum EV Certificate Guidelines Version 1.1

GlobalSign® and the GlobalSign Logo are registered trademarks of GlobalSign K.K.
1.0 Introduction

This Certification Practice Statement (CPS) of the GlobalSign Certification Authority (hereinafter, GlobalSign CA) applies to the services of the GlobalSign CA that are associated with the issuance of and management of digital certificates. Digital certificates can be used to create or rely upon electronic signatures. This CPS can be found on the GlobalSign CA repository at: http://www.globalsign.com/repository. This CPS may be updated from time to time.

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements”. This CPS is a certificate policy in broad sense and meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format. An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and certificate management. While certain section titles are included in this policy according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the certificate management services of the GlobalSign CA. These sections have been removed from this document. Where necessary additional information is presented as subsections added to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability of the GlobalSign CA with other third party CAs and provides relying parties with advance notice on the practices and procedures of the GlobalSign CA. Additional assertions on standards used in this CPS can be found under section “Acknowledgements”.

This CPS addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by the GlobalSign CA.

Request for information on the compliance of the GlobalSign CA with accreditation schemes as well as any other inquiry associated with this CPS can be addressed to:

GlobalSign NV
attn. Legal Practices,
Ubicenter,
Philipssite 5
B-3001 Leuven,
Belgium.
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

The GlobalSign CA operates within the scope of activities of GlobalSign NV. This CPS addresses the requirements of the CA that issues certificates of various certificate types. More information can be obtained from http://www.globalsign.com/repository.

This CPS is final and binding between GlobalSign NV/SA, a company under public law, with registered office at Ubicenter, Philipssite 5, B-3001 Leuven, VAT Registration Number BE 0459134256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (Hereinafter referred to as "GlobalSign")

and

the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the GlobalSign CA.

For subscribers this CPS becomes effective and binding by accepting a subscriber agreement. For relying parties this CPS becomes binding by merely addressing a certificate related request.
on a GlobalSign certificate to a GlobalSign directory. The subscriber, through acceptance of the subscriber agreement, is bound by the agreement to inform their relying parties that the CPS is itself binding toward those relying parties.

1.1 Overview

This CPS applies to the specific domain of the GlobalSign CA. The purpose of this CPS is to present the GlobalSign practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to GlobalSign's own and industry requirements pursuant to the standards set out above. Additionally the Belgian Law of 9 July 2001 implementing the European Directive 1999/93/EC of the Council and the Parliament on a Community Framework on Electronic Signatures provides for the recognition of electronic signatures that are used for the purposes of authentication or non repudiation. In this regard GlobalSign operates within the scope of the applicable sections of the Law when delivering its services. This CPS applies to the above-stated domain to the exclusion of any other. This CPS aims at facilitating the GlobalSign CA in delivering certification services through discrete CA issuing Client end entity certificates. The certificate types addressed in this CPS are the following:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PersonalSign 1 Demo</td>
<td>A personal certificate of low assurance</td>
</tr>
<tr>
<td>PersonalSign 2</td>
<td>A personal certificate of medium assurance</td>
</tr>
<tr>
<td>PersonalSign 2 Pro</td>
<td>A personal certificate of medium assurance with reference to professional context</td>
</tr>
<tr>
<td>PersonalSign 3</td>
<td>A personal certificate of high assurance</td>
</tr>
<tr>
<td>PersonalSign 3 Pro</td>
<td>A personal certificate of high assurance with reference to professional context</td>
</tr>
<tr>
<td>OrganizationSSL</td>
<td>A certificate to authenticate web servers</td>
</tr>
<tr>
<td>DomainSSL</td>
<td>A certificate to authenticate web servers</td>
</tr>
<tr>
<td>ExtendedSSL</td>
<td>A certificate to authenticate web servers *</td>
</tr>
<tr>
<td>Educational ServerSignSSL</td>
<td>A certificate to authenticate web servers</td>
</tr>
<tr>
<td>GlobalSign TimeStamping</td>
<td>A certificate to authenticate time sources</td>
</tr>
<tr>
<td>DocumentSign</td>
<td>A personal certificate of medium hardware assurance with reference to professional context</td>
</tr>
<tr>
<td>Code Signing</td>
<td>A certificate to authenticate data objects</td>
</tr>
<tr>
<td>TrustedRoot</td>
<td>A certificate for CAs that enter the GlobalSign hierarchy</td>
</tr>
<tr>
<td>TrustedRoot TPM</td>
<td>A certificate for CAs that enter the GlobalSign TPM hierarchy</td>
</tr>
</tbody>
</table>

* These certificates are issued and managed in accordance with CA/Browser Forum Guidelines for Extended Validation Certificates, which are incorporated by reference into this CPS.

GlobalSign certificates:

- Can be used for electronic signatures in order to replace handwritten signatures where transacting parties choose for them
- Can be used to authenticate web resources, such as servers and other devices.
- Can be used to digitally sign code, documents and other data objects.
- Can be used to authenticate and trust other certification authorities.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of GlobalSign certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved including the GlobalSign CA, GlobalSign RA, subscribers and relying parties. Certain provisions might also apply to other entities such as the certification service provider, application providers etc.

This CPS describes the requirements to issue, manage and use certificates issued by the GlobalSign CA under a managed Brand Root. As a top root CA, GlobalSign manages a hierarchy
of certificates according to publicised practices to be found under www.globalsign.com/repository

A GlobalSign Certificate Policy (CP) complements this CPS. The purpose of the GlobalSign CP is to state the “what is to be adhered to” and, therefore, set out an operational rule framework for the broad range of GlobalSign products and services. Such level is generally defined by the entity wishing to ensure a level of trust by managing the life cycle of digital certificates. The GlobalSign CP addresses the requirements of the entire application domain of GlobalSign certificates focusing on top root certificates and not just the end-entity certificate area.

This CPS states, “how the Certification Authority adheres to the Certificate Policy”. In doing so this CPS features a greater amount of detail and provides the end user with an overview of the prevailing processes, procedures and overall prevailing conditions that the Certification Authority uses in creating and maintaining the certificates that it manages. In addition to the CP and CPS GlobalSign maintains a range of adjacent documented polices which include but are not limited to addressing such issues as:

- Business continuity
- Security policy
- Personnel policies
- Key management policies
- Registration procedures

Additionally, other pertinent documents include:

- The GlobalSign Limited Warranty Policy that addresses issues on insurance.
- The GlobalSign Data Protection Policy on the protection of personal data
- The GlobalSign Certificate Policy that addresses the trust objectives for the domain of the GlobalSign top root.

A subscriber or relying party of a GlobalSign CA certificate must refer to the GlobalSign CPS in order to establish Trust in a certificate issued by the GlobalSign Root CA as well as for notices with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire certificate chain of the GlobalSign certificate hierarchy, including the Top Root CA and operational roots, which can be established on the basis of the assertions of this CPS.

A full list of accreditation(s), and recognition of service is available upon request.

The exact names of the GlobalSign CA certificates that make use of this CPS are:

- GlobalSign Root CA*
- GlobalSign Root CA - R2*
- GlobalSign Root CA - R3*

GlobalSign actively promotes the inclusion of these Roots into hardware and software platforms that are capable of supporting digital certificates and associated cryptographic services. Where possible, GlobalSign will seek to enter into a contractual agreement with platform providers to ensure effective GlobalSign CA Root certificate lifecycle management. However, GlobalSign also actively encourages platform providers at their own discretion to include GlobalSign CA Root certificates without contractual obligation.

In addition, the name of the GlobalSign CA certificate that also makes use of this CPS, but which is not actively promoted for inclusion into hardware and software platforms is:

- GlobalSign Trusted Platform Module Root CA*

* Collectively these are known as the GlobalSign CA Root

Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants or sign data electronically. By means of a digital certificate, GlobalSign provides confirmation of the relationship between a named entity (subscriber) and its public key. The process to obtain a digital certificate includes the identification, naming, authentication and
registration of the client as well as aspects of certificate management such as the issuance, revocation and expiration of the digital certificate. By means of this procedure to issue digital certificates, GlobalSign provides adequate and positive confirmation about the identity of the user of a certificate and a positive link to the public key that such entity uses. An entity on this instance might include an end user, another certification authority, as it might be required under the circumstances. GlobalSign makes available general-purpose digital certificates that can be used for non-repudiation and authentication. The use of these certificates can be further limited to a specific business or contractual context or transaction level according a warranty policy or other limitations imposed by the applications that certificates are used in.

This CPS is maintained by the GlobalSign CA, which is the issuing authority of certificates in the GlobalSign Public Key Infrastructure. In a certificate management environment based on Public Key Infrastructure (PKI), an Issuing Authority is the entity that manages a Trust hierarchy from which all end user certificates inherit Trust.

This CPS governs the issuance of certificates during the application period of the GlobalSign CA Roots. An application period is for example, the time during which a certain CA may issue GlobalSign CA certificates. The application period is indicated in the certificate issued to the appropriate Root by a hierarchically superior CA within the GlobalSign hierarchy.

This CPS is made available on-line in the Repository of the issuing CA under http://www.globalsign.com/repository.

The GlobalSign CA accepts comments regarding this CPS addressed to the address mentioned above in the Introduction of this document.

### 1.2 GlobalSign Certificate types

This part describes the public GlobalSign products.

#### 1.2.1 Personal Certificates

GlobalSign offers several types of certificates for use by individuals and organizations. These certificates may be used to provide authentication services, secure e-mail capabilities, inter organizational communications, access to personal financial information and to authenticate the subscriber in online Internet transactions. In all cases a licence is granted by GlobalSign to the subscriber to create a personal backup of both the certificate and associated private key pair for business continuity purposes. With the exception of a Department or Role based certificate type, no licence is granted to transfer or duplicate the certificate and associated key pair for any other purpose.

- **PersonalSign Demo and PersonalSign 1**: provides only an unambiguous e-mail address within the GlobalSign repository while GlobalSign performs no authentication of the identity of the applicant. PersonalSign Demo certificates are meant for test and demonstration purposes only and they are valid for one month or one year.
- **PersonalSign 2**: provides a limited identity authentication by requiring a signed copy of an identity element from the subscriber. These digital certificates can be used for most low-value/low risk commercial transactions like online purchases. They are valid for one, two or three years.
- **PersonalSign 2 Pro and DocumentSign**: provides limited identity authentication through an attestation of identity from the legal person identified within the certificate. Role based identity information may be incorporated into the subject of the certificate. These digital certificates can be used for most low-value/low risk commercial transactions like online purchases. They are valid for one, two or three years.
- **PersonalSign 3**: provides a high level of identity assurance by requiring that the applicant appear personally before a Registration Authority to prove its identity. These certificates can be used for high-value/high risk commercial transactions such as electronic banking. They are valid for one, two or three years.
- **PersonalSign 3 Pro**: provides a high level of identity assurance by requiring that the applicant appears personally before a Registration Authority to prove its identity.
PersonalSign 3 Pro certificates require professional context affiliation. These certificates can be used for high-value/high risk commercial transactions such as electronic banking. They are valid for one, two or three years.

1.2.2 Server Certificates

GlobalSign offers several types of certificates for servers/hardware which may be used for web based transactions. In all cases, a licence is granted by GlobalSign to the subscriber to create a backup of both the certificate and associated private key pair for business continuity purposes. No licence is granted to transfer or duplicate the certificate and associated key pair for any other purpose unless specifically indicated during the purchasing process by virtue of a suitable offer or promotion which may or may not be advertized on the appropriate GlobalSign web site:

- **OrganizationSSL**: OrganizationSSL is meant for entities that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in commercial and financial transactions. The identity of the certificate-holder is fully authenticated by GlobalSign.

- **DomainSSL**: DomainSSL is meant for entities that wish to participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in secured transactions. The identity of the certificate-holder is not authenticated by GlobalSign, only the ownership of the domain or the capability to use the domain as represented by the Domain Name System.

- **ExtendedSSL**: ExtendedSSL is meant for entities that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in commercial and financial transactions. The identity of the certificate-holder is fully authenticated by GlobalSign in accordance with the CA/browser forum Guidelines for Extended Validation Certificates.

- **Educational ServerSign**: Educational ServerSign is meant for entities within the education and research space that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based education and research institutes.

1.2.3 Object Publishing Certificates

GlobalSign offers one type of object publishing certificate. A licence is granted by GlobalSign to the subscriber to create a personal backup of both the certificate and associated private key pair for business continuity purposes. No licence is granted to transfer or duplicate the certificate and associated key pair for any other purpose.

- **Code Signing** ensures the identity of an entity that distributes software or software objects such as applets on the Internet, and guarantees the integrity of the software being distributed utilizing Microsoft’s Authenticode or Netscape’s Code Signing standards or Sun’s Java Keytools or Adobe’s AIR for example. Code Signing assures relying parties of the integrity of an object and verifies the identity of the sender of a software object to ensure that the certified software object originates from a trusted source.

1.2.4 Acceptable Subscriber Names

For publication in its certificates GlobalSign accepts subscriber names that are meaningful and can be authenticated as required for each product type or class.

1.2.4.1 Pseudonyms

For certain types of products GlobalSign may allow the use of pseudonyms, reserving its right to disclose the identity of the subscriber as may be required by law or a following a reasoned and legitimate request.
1.2.4.2 Role or Department

A Registration Authority may incorporate a role or department into the certificate. In this case GlobalSign may allow the use of a ‘role’ or ‘department’ names, reserving its right to disclose the identity of the organization’s registration authority as may be required by law or a following a reasoned and legitimate request.

1.2.5 Registration procedures

For all types of certificates GlobalSign reserves the right to update registration procedures and subscriber submitted data to improve the identification and registration process.

1.3 PersonalSign Demo and PersonalSign 1

1.3.1 General

- PersonalSign Demo and PersonalSign 1 (referred later as PersonalSign 1 Demo) certificates are issued to natural persons (individuals) only.
- PersonalSign 1 Demo certificates confirm that a user’s e-mail address forms an unambiguous subject name within the GlobalSign repository.
- PersonalSign 1 Demo certificates are communicated electronically to subscribers and added to its set of available certificates.
- They are typically used for Web browsing and personal E-mail, to establish continuity in the sequence of communications (providing assurances that follow-up communications are from the same user). They are not intended for commercial use where proof of identity is required and should not be relied upon for such uses.
- PersonalSign 1 Demo certificates are intended for test purposes only.
- PersonalSign 1 Demo certificates can be distributed as an introduction to digital certificates, for applications that do not require authentication of the communicating parties and for encryption of the e-mail communications.
- PersonalSign 1 Demo certificates validity period is between 30 days and one year.
- Although PersonalSign 1 Demo certificates are not essentially technically different from other classes of GlobalSign personal certificates, as there is no verification process, the identity of the applicant cannot be warranted.

1.3.2 Assurance level

PersonalSign 1 Demo certificates do not facilitate the authentication of the identity of the subscriber as they merely represent a simple check of the non-ambiguity of the e-mail address within the GlobalSign repository.

The subscriber’s E-mail address contained in a PersonalSign 1 Demo certificate consists of non-verified subscriber information for the accuracy of which GlobalSign carries no responsibility.

1.3.3 Individuals

The procedure for a certificate request can be made as follows:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. If required, the applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant to the e-mail address from which the certificate application had originated. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

API: The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the
applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.3.4 Content
Typical of information published in a PersonalSign 1 Demo certificate includes the following elements.
- Subscriber’s e-mail address
- Subscriber’s public key
- Issuing certification authority (GlobalSign):
- GlobalSign electronic signature
- GlobalSign’s unique Policy OID for PersonalSign certificates
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.3.5 Submitted documents to identify the applicant
No registration documents are necessary for PersonalSign 1 Demo certificates.

1.3.6 Time to confirm submitted data
GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame.

1.3.7 Issuing procedure
The following steps describe the milestones to issue a PersonalSign 1 Demo certificate:
1. The applicant fills out the online registration form, as part of the online request
2. The applicant accepts the online subscriber agreement
3. Either a key pair is generated on an applicant’s device (e.g. computer, smart card device etc.) or the subscriber requests that GlobalSign generates a key pair on their behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism
4. The public key and online request are sent to GlobalSign.
5. GlobalSign verifies by checking copy of verification method and payment.
6. RA may positively verify the applicant.
7. GlobalSign may issue the certificate to the applicant.
8. If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will be protected by the strong password provided by the applicant during the registration process.
9. Renewal: not allowed
10. Revocation: allowed but remains at GlobalSign’s discretion

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.3.8 Limited Warranty
GlobalSign accepts no liability and offers no insurance for issuing PersonalSign 1 Demo certificates.
1.3.9 Relevant GlobalSign Legal Documents

The applicant must take notice and is bound by the following documents available on http://www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Data Protection Policy
4. Warranty Policy

1.4 PersonalSign 2

1.4.1 General

- PersonalSign 2 certificates are intended for communications and transactions that require a minimum verification of the identity.
- PersonalSign 2 certificates can be distributed for communications and transactions with a low value and little risk with a need to authenticate the communicating parties and encrypt the exchange of communications.
- PersonalSign 2 certificates validity period is between one and three years.
- PersonalSign 2 certificates are issued to natural persons (individuals) only.
- PersonalSign 2 applicant verification is undertaken by a registration authority by using a copy of an identity proof.
- PersonalSign 2 certificates are issued primarily for low value and low risk personal communications and purposes.
- Records retention period does not fulfill professional records requirements according to the Laws of Belgium.

1.4.2 Assurance Level

PersonalSign 2 certificates may provide reasonable, but not foolproof, assurance of a subscriber’s identity, based on an automated on-line process that compares the applicant’s name, address, and other personal information on the certificate application against a signed identity proof.

Although GlobalSign’s PersonalSign 2 on-line identification process is a high level method of authenticating a certificate applicant’s identity, it does not require the applicant’s personal appearance before a registration authority.

1.4.3 Certificate Requests:

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant to the e-mail address from which the certificate application had originated. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

API: The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.
1.4.4 Content

Typical information published on a PersonalSign 2 certificate includes the following elements:

- Subscriber’s e-mail address
- Subscriber’s name
- Applicant’s public key
- Code of applicant’s country
- Issuing certification authority (GlobalSign):
- GlobalSign electronic signature
- GlobalSign’s unique Policy OID for PersonalSign certificates
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.4.5 Documents Submitted to Identify the Applicant

The applicant must submit to a GlobalSign Registration Authority either a signed copy of an identification document such as an identity card, driver’s license, passport, or the applicant may authenticate the request through a proof of possession challenge-response. Any signature from the applicant must include the date of signing and a phrase ‘I have read and approved the subscriber agreement’ or similar wording.

1.4.6 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm the certificate application information and issue a digital certificate within a reasonable time frame. For PersonalSign 2, a verification time of 1 - 3 working days might be required.

1.4.7 Issuing Procedure

The following steps describe the milestones in the procedure to issue a PersonalSign 2 certificate:

1. The applicant fills out the outline registration form: e-mail address, common name, country code, verification method, billing information as part of the online request.
2. The applicant accepts online subscriber agreement.
3. Either a key pair is generated on an applicant’s device (e.g. computer, smart card device etc.) or the subscriber requests that GlobalSign generates a key pair on their behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism.
4. The public key and online request are sent to GlobalSign.
5. GlobalSign verifies by checking copy of verification method and payment.
6. RA may positively verify the applicant.
7. GlobalSign may issue the certificate to the applicant.
8. If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will be protected by the strong password provided by the applicant during the registration process.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.4.8 Limited Warranty

GlobalSign accepts liability up to 2500 EURO per damage caused by a false identity in a PersonalSign 2 certificate issued according to the CPS.
1.4.9 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

- CPS
- Subscriber Agreement
- Data Protection Policy
- Warranty Policy

1.5 PersonalSign 2 Pro and DocumentSign

This part describes the specific requirements for PersonalSign 2 Pro and DocumentSign certificates.

1.5.1 General

- PersonalSign 2 Pro and DocumentSign certificates are intended for certain communications and transactions that require a minimum verification of the identity of a subscriber within a professional context.
- PersonalSign 2 Pro and DocumentSign certificates can be distributed for communications and transactions with a low value and little risk with a need to authenticate the communicating parties and encrypt the exchanged communications.
- PersonalSign 2 Pro and DocumentSign certificates validity period is between one and three years.
- PersonalSign 2 Pro and DocumentSign certificates are issued to natural persons (individuals) within their professional context. A Registration Authority may incorporate role based identity information into the certificate.
- PersonalSign 2 Pro and DocumentSign subject identification is performed by a registration authority or via a local registration authority approved and authorized by the organization mentioned within the subject of the certificate.
- PersonalSign 2 Pro and DocumentSign certificates are typically used primarily for intra-organizational and inter-organizational E-mail; small, “low-risk” transactions; personal/individual E-mail; password replacement; software validation; online purchases and on-line subscription services.
- DocumentSign certificates are also typically used to sign PDF documents.
- Period retention for records and documentation is at least seven years after certificate based on these documents ceases to be valid, conform Document Retention policy specified by the CA/B forum.

1.5.2 Certificate Requests

A certificate request can be made by the following means:

**On-line:** Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. If required the applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant to the e-mail address from which the certificate application had originated. The applicant downloads and installs the certificate to the applicant’s device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of changes to the information to be included in the certificate.

**API:** The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application
had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

In the case of a DocumentSign certificate the applicant downloads and installs the digital ID onto an approved cryptographic hardware module that a) meet or exceed FIPS 140-1 Level 2 standards or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-1 Level 2 status within the previous year without receiving a notice of non-compliance or other communication indicating that such device fails to meet such standard (an “Approved Hardware Device”). GlobalSign shall restrict applicant's Cryptographic Service Provider to a 2048 key generation and FIPS 140-1 level 2 cryptographic device. Applicant may have the option of requesting GlobalSign or approved Registration Authority to generate a Public and Private Key Pair onto the Approved Hardware Device at GlobalSign’s facilities and deliver the Approved Hardware Device containing the digital ID to the applicant.

1.5.3 Content

Typical content of information published in a PersonalSign 2 Pro or DocumentSign certificate includes the following elements:

- Subscriber’s e-mail address or Departmental e-mail address
- Subscriber’s name
- Where the subscriber’s organization wishes to accept the responsibilities of being a Local Registration Authority, role based identity information may be incorporated into the certificate.
- Applicant’s professional organization
- Applicant’s public key
- Code of applicant’s country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- GlobalSign’s unique Policy OID for PersonalSign certificates
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.5.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must either submit to a GlobalSign Registration Authority a signed registration form and a signed subscriber agreement or maintain a GlobalSign Certificate Centre Account allowing click through agreements to be presented and approved. In all cases a GlobalSign Registration Authority will validate the business existence and registration details via a source such as a Qualified Government Information Source or a Qualified Independent Information Source in order to verify the authenticity of the request.

In the case of a Role or Departmental name, the organizational approved registration authority takes on the responsibility to authenticate the role, and as such, may be required to provide confirmation of their employment relationship.

For self-employed applicants who work independently of an association or professional group an extract of the register of commerce may be required in addition to the above-mentioned documents.

For self-employed applicants belonging to an association or professional group an official document from the professional group and a membership card will be required in addition to the above-mentioned documents.

GlobalSign may require additional proof of identity in support of the verification of the applicant.
1.5.5 Time to Confirm Submitted Data
GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For PersonalSign 2 Pro or DocumentSign products, a verification time of 1 - 5 working days might be required.

1.5.6 Issuing Procedure
The issuing procedure for a PersonalSign 2 Pro or DocumentSign certificate is as follows:

1. The applicant submits online the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
2. The applicant accepts the online subscriber agreement.
3. Either a key pair is generated on an applicant's device (e.g. computer, smart card device etc.) or the subscriber requests that GlobalSign generates a key pair on their behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism.
4. The public key and the online request are sent to GlobalSign automatically.
5. If required during the application process, the applicant must send to the RA the requested information.
6. RA may positively verify the applicant.
7. GlobalSign may issue the certificate to the applicant.
8. If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will be protected by the strong password provided by the applicant during the registration process.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.5.7 Limited Warranty
GlobalSign accepts liability up to 2500 EURO per damage caused by a false identity in a PersonalSign 2 Pro or DocumentSign certificate issued according to the CPS.

1.5.8 Relevant GlobalSign Documents
The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Data Protection Policy
4. Warranty Policy

1.6 PersonalSign 3

1.6.1 General
- PersonalSign 3 certificates are intended for high value commercial transactions such as electronic banking and contract execution.
- PersonalSign 3 certificates offer a high level of identity assurance requiring personal presence before a registration authority.
- PersonalSign 3 certificates are issued to natural persons (individuals) without a professional context.
- PersonalSign 3 certificates validity period is between one and three years.
- PersonalSign 3 certificates are issued primarily for medium risk personal communications and usages.
1.6.2 Certificate Requests

A certificate request can be made as follows: 

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. The applicant must in person appear in front of a GlobalSign RA or LRA. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant to the e-mail address from which the certificate application had originated. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

API: The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.6.3 Content

Typical content of information published on a PersonalSign 3 certificate includes the following elements:

- Subscriber’s e-mail address
- Subscriber’s name
- Applicant’s public key
- Code of applicant’s country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- GlobalSign’s unique Policy OID for PersonalSign certificates
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.6.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit to a GlobalSign Registration Authority in person a signed registration form, a signed subscriber agreement and a copy of identity proof.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant’s identity.

1.6.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For PersonalSign 3, a verification time of 1 - 5 working days might be required.

1.6.6 Issuing Procedure

The issuance procedure for a PersonalSign 3 certificate is as follows:

1. The applicant submits online the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
2 The applicant accepts the on-line subscriber agreement.
3 Either a key pair is generated on an applicant’s device (e.g. computer, smart card device etc.) or the subscriber requests that GlobalSign generates a key pair on their behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism.
4 The public key and the online request are sent to GlobalSign automatically.
5 GlobalSign verifies by personal appearance before a LRA or RA and checking identity elements of the applicant as well as payment. Personal presence may occur prior to the time of the application.
6 RA may positively verify the applicant.
7 GlobalSign may issue the certificate to the applicant.
8 If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will be protected by the strong password provided by the applicant during the registration process.
9 Renewal: allowed.
10 Revocation: allowed.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.6.7 Limited Warranty

GlobalSign accepts liability up to 37500 EURO per damage caused by a false identity in a PersonalSign 3 certificate issued within the terms of this CPS.

1.6.8 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1 CPS
2 Subscriber Agreement
3 Data Protection Policy
4 Warranty Policy

1.7 PersonalSign 3 Pro

1.7.1 General

- PersonalSign 3 Pro certificates are intended for high value commercial transactions such as electronic banking and contract execution.
- PersonalSign 3 Pro certificates offer a high level of identity assurance requiring personal presence before a registration authority.
- PersonalSign 3 Pro certificates are issued to natural persons (individuals) within their professional context only.
- PersonalSign 3 Pro certificates validity period is between one and three years.
- PersonalSign 3 Pro certificates are issued primarily for professional usages.
- Records retention period meets professional records requirements according to the Laws of Belgium.

1.7.2 Certificate Requests

A certificate request can be made as follows:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. The applicant must in person appear in front of a GlobalSign RA or LRA. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant to the e-mail address from which the certificate application
had originated. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

**API:** The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

### 1.7.3 Content

Typical content of information published on a PersonalSign 3 Pro certificate includes the following elements:

- Applicant's e-mail address
- Applicant's name
- Applicant's public key
- Applicant's professional organization or affiliation
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- GlobalSign's unique Policy OID for PersonalSign certificates
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

### 1.7.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit in person to a GlobalSign Registration Authority a signed registration form, a signed subscriber agreement and the articles of association or proof of professional context and a copy of identity proof.

For an employee it is required to submit the articles of association of its employer and confirmation by a legal representative of such organization.

For a self-employed person that works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For self-employed persons belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional identification proof in support of the verification of the applicant.

### 1.7.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For PersonalSign 3 Pro, a verification time of 1 - 5 working days might be required.

### 1.7.6 Issuing Procedure

The following steps describe the milestones in the issuance of a PersonalSign 3 Pro certificate:

1. The applicant submits online the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
2. The applicant accepts the online subscription agreement.
3. Either a key pair is generated on an applicant’s device (e.g., computer, smart card device etc.) or the subscriber requests that GlobalSign generates a key pair on their behalf. In the latter case, the application requires a strong password from the applicant to facilitate a secure delivery mechanism.
4. The public key and the online request are sent to GlobalSign automatically.
5. GlobalSign verifies by personal appearance before a LRA or RA and checking articles of association, proof of professional context and payment. Personal presence may occur prior to the time of the application.
6. RA may positively verify the applicant.
7. GlobalSign may issue the certificate to the applicant.
8. If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will be protected by the strong password provided by the applicant during the registration process.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.7.7 Limited Warranty

GlobalSign accepts liability up to 37500 EURO per damage caused by a false identity in a PersonalSign 3 Pro certificate issued according to the CPS.

1.7.8 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Data Protection Policy
4. Warranty Policy

1.8 OrganizationSSL

1.8.1 General

OrganizationSSL certificates are meant for secure communication with for example a web-site through an SSL or TLS link. OrganizationalSSL certificates may also be used to secure Intranet Servers and Unified Communications Servers. Any non-publicly resolvable domain names, server names or IP addresses may be incorporated within the Subject or within the Subject Alternative Name extension of the certificate.

The applicant is an organization that has an Internet Server such as a website. OrganizationSSL certificates are used to assure the Internet Server’s identity to the visitor and to assure a confidential communication with the Internet Server.

OrganizationSSL certificates validity period is between one and five years according to the choice of the applicant.

OrganizationSSL certificates are issued to legal persons and self-employed professionals registered with a professional organization.

The period retention for records meets professional records requirements of the Laws of Belgium.

1.8.2 Certificate Requests

A certificate request can be made in the following ways:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the
application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity of the Internet Server, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

API: The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.8.3 Content

Typical information published on an OrganizationSSL certificate includes the following elements:

- Applicant’s domain name and/or host name or Public or non Public IP address
- Applicant’s name of organization
- Optional Subject Alternative Name entries which may detail hostnames, IP addresses or additional domains owned or controlled by the Applicant.
- Applicant's public key
- Code of applicant’s country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- GlobalSign’s unique Policy OID for OrganizationSSL certificates
- Type of algorithm
- Organizational Unit (OU) (Non Verified)
- Validity period of the digital certificate
- Serial number of the digital certificate

1.8.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must either submit to a GlobalSign Registration Authority a signed registration form or maintain a GlobalSign Certificate Centre Account allowing click through agreements to be presented and approved. In all cases a GlobalSign Registration Authority will validate the business existence and registration details via a source such as a Qualified Government Information Source or a Qualified Independent Information Source in order to verify the authenticity of the request.

1.8.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For OrganizationSSL, a verification time of 1 - 5 working days might be required.

1.8.6 Issuing Procedure

The issuing procedure for an OrganizationSSL certificate is as follows:

1. The Applicant creates a Certificate Signing Request (CSR) and a key pair using appropriate server software or the Applicant requests GlobalSign to generate the key pair on its behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism.
2. The Applicant follows the on line registration procedure.
3 The Applicant submits the required information including organizational information, technical contact, server information, payment information. Optional Subject Alternative Names will be submitted as well.
4 The Applicant accepts the on line subscriber agreement.
5 Data is sent with certificate request to GlobalSign automatically.
6 GlobalSign verifies the submitted information by checking organizational, payment and any other information as it sees fit. This may also include checks in third party databases or resources, against standard bodies such as the Internet Engineering Task Force (IETF) or the Internet Corporation for Assigned Names and Numbers (ICANN), and independent verification through telephone.
7 GlobalSign may positively verify the Applicant.
8 GlobalSign may issue the certificate to the Applicant.
9 If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will do so in a secure manner protected by the strong password provided by the applicant during the registration process. GlobalSign will then delete all instances of the Applicant’s private key.
10 Renewal: allowed
11 Revocation: allowed
12 Reissue: allowed. (Subject Alternative Names might be removed or added in a reissued certificate.)

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.8.7 Limited Warranty

GlobalSign accepts liability up to 100,000 EURO per loss due to a false identity in a certificate issued following this CPS with the exception of Certificates for intranet use. GlobalSign disclaims any and all warranties (including name verification) for Unified Communications Certificates and other Certificates issued to intranets (e.g. where a non-public or non-standard Top Level Domain is used or where they are addressed to IP space allocated as private by RFC1918), which are not intended to be relied upon by the general public.

1.8.8 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1 CPS
2 Subscriber Agreement
3 Data Protection Policy
4 Warranty Policy

1.9 DomainSSL

1.9.1 General

DomainSSL certificates are meant for secure communication with for example a web-site through an SSL or TLS link. DomainSSL certificates may also be used to secure Intranet Servers or Unified Communications Servers, however, any non-publicly resolvable domain names, server names or IP addresses may only be incorporated as a Subject Alternative Name extension.

The applicant is an individual or organization that has an Internet Server such as a website. DomainSSL certificates are used to assure a confidential communication with the Internet Server.

DomainSSL certificates validity period is between one and five years. DomainSSL certificates are issued to entities and individuals who own a domain name, or have the right to request a DomainSSL for a specific domain. The period retention for records fulfils professional records requirements of the Laws of the Belgium.
1.9.2 Certificate Request

A certificate request can be made in the following ways:
**On-line, via the Web (https).** The certificate applicant submits an application via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies that the domain name belongs to the applicant, or that the applicant is authorized to request a certificate for that domain name. The applicant submits to GlobalSign the additional documentation. Upon verification of ownership or right to use of the domain name, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

**API:** The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.9.3 Content

Typical information published in a DomainSSL certificate includes the following elements

- Applicant’s domain name
- Applicant’s public key
- Code of applicant’s country (Non Verified)
- Issuing certification authority (GlobalSign CA)
- GlobalSign electronic signature
- GlobalSign’s unique Policy OID for DomainSSL certificates
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate
- Optional Subject Alternative Name entries which may detail hostnames, IP addresses or additional domains owned or controlled by the Applicant.

1.9.4 Information Submitted to verify ownership or right to use of the Domain name or IP Address

The applicant must provide contact details to GlobalSign and underwrite those by a click-through process. GlobalSign has the right to request a signed registration form or a signed subscriber agreement. GlobalSign has the right to request proof of the ownership of any of the domain names or IP addresses in the certificate (including those incorporated as Subject Alternative Names) or can ask the owner of the domain name to validate the request of the applicant. GlobalSign will not verify the country code within the certificate request.

1.9.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For DomainSSL, a verification time of 1 - 3 working days might be required.

1.9.6 Issuing Procedure

The issuing procedure for a DomainSSL certificate is as follows:

1. The Applicant creates a Certificate Signing Request (CSR) and a key pair using appropriate server software or the Applicant requests GlobalSign to generate the key pair...
on its behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism.

2 The applicant follows the on line registration procedure.

3 The applicant submits the required information including technical contact, server information and if required payment information. Optional Subject Alternative Names will be submitted as well.

4 The applicant accepts by click-through the on line subscriber agreement.

5 Data is sent with certificate request to GlobalSign automatically.

6 GlobalSign verifies the submitted information by checking domain ownership or domain right to use and any other information as it sees fit. This may also include checks in third party databases or resources, against standard bodies such as the Internet Engineering Task Force (IETF) or the Internet Corporation for Assigned Names and Numbers (ICANN), and independent verification through telephone.

7 GlobalSign may positively verify the applicant.

8 GlobalSign may issue the certificate to the applicant.

9 If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will do so in a secure manner protected by the strong password provided by the applicant during the registration process. GlobalSign will then delete all instances of the Applicant’s private key.

10 Renewal: allowed

11 Revocation: allowed

12 Reissue: allowed. Subject Alternative Names might be removed or added in a reissued certificate.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.9.7 Limited Warranty

GlobalSign accepts liability up to 10,000 EURO per loss due to a false domain name (lack of ownership or lack of right to use domain) in a certificate issued following this CPS with the exception of Certificates for intranet use. GlobalSign disclaims any and all warranties (including name verification) for Unified Communications Certificates and other Certificates issued to intranets (e.g. where a non-public or non-standard Top Level Domain is used or where they are addressed to IP space allocated as private by RFC1918), which are not intended to be relied upon by the general public.

1.9.8 Relevant Globalsign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1 CPS
2 Subscriber Agreement
3 Data Protection Policy
4 Warranty Policy

1.10 ExtendedSSL

1.10.1 General

ExtendedSSL certificates are used to assure the Internet Server’s identity to the visitor and to assure a confidential communication with the Internet Server through an SSL or TLS link.

ExtendedSSL certificates validity period is between one year and 27 months.
1.10.1.1 Extended Validation Certificates

ExtendedSSL certificates are issued under the minimum requirements described in the Guidelines for Extended Validation certificates. A Certificate Authority (CA) must meet such requirements in order to issue Extended Validation Certificates (“EV Certificates”).

Organization information from valid EV Certificates may be displayed in a special manner by certain software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the website they are accessing.

1.10.1.2 Guidelines for Extended Validation Certificates

The Guidelines address basic issues relating to the verification of information regarding Subjects named in EV Certificates and certain related matters. The Guidelines for Extended Validation Certificates (or EV guidelines) are an integral part of the present Certification Practice Statement and are incorporated by reference herein.

Questions on the Guidelines for Extended Validation Certificates may be directed to the CA/Browser Forum at questions@cabforum.org.

1.10.1.3 Extended Validation Guidelines Compliance

ExtendedSSL certificates related sections and, if applicable, other sections of this CPS have been written out to reflect the Guidelines for EV certificates requirements.

ExtendedSSL issuance and management practices comply with the current version of the said Guidelines.

In the event of any inconsistencies between the ExtendedSSL related provisions of this document and the Guidelines for Extended Validation Certificates, the Guidelines for Extended Validation Certificates take precedence over this document.

1.10.1.4 ExtendedSSL Subjects

ExtendedSSL certificates may be issued to private organizations, government entities Business Entities and International Organizations, provided they are either duly incorporated in the jurisdiction of incorporation where GlobalSign acts as a CA, or the principle individuals and the legal existence of the business have been verified in accordance to the guidelines incorporated into this document by reference.

GlobalSign may not issue ExtendedSSL certificates to individuals (natural persons).

The period retention for records fulfils professional records requirements of the Laws of the United States.

1.10.1.5 ExtendedSSL Issuance Specific Roles

The following applicant roles are required for the issuance of an ExtendedSSL Certificate

The Certificate Requester is an applicant’s employee, or an authorized agent who has express authority to represent the applicant or a third party (such as an ISP or hosting company), who is responsible for completing and submitting a GlobalSign Extended certificate request on behalf of the applicant.

The Certificate Approver is responsible for approving the certificate request. He is an applicant’s employee, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve ExtendedSSL Certificate Requests submitted by other Certificate Requesters.
The Contract Signer is responsible for signing the Subscriber Agreement applicable to the requested ExtendedSSL Certificate. He is an applicant’s employee, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant.

One person, whether an Applicant’s employee or an authorized agent, may be authorized by the applicant to fill one, two, or all three of these roles, as the case may be. An applicant may also authorize more than one person to fill each of these roles.

1.10.2 Certificate Requests

A certificate request can be made in the following ways:

**On-line:** Via the Web (https) Prior to the issuance of an ExtendedSSL certificate, GlobalSign must obtain from the applicant (via a certificate Requester authorized to act on applicant’s behalf) a properly signed ExtendedSSL certificate request that includes a certification by or on behalf of the applicant that all of the information contained therein is true and correct. The certificate applicant submits the certificate request via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity of the Internet Server, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

**API:** The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Prior to the issuance of an ExtendedSSL certificate, GlobalSign must obtain from the applicant (via a certificate Requester authorized to act on applicant’s behalf) a properly signed ExtendedSSL certificate request that includes a certification by or on behalf of the applicant that all of the information contained therein is true and correct. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.10.3 Content

Typical information published in an ExtendedSSL certificate MAY include the following elements:

- Applicant’s organization Name
- Applicant’s Domain Name
- Jurisdiction of Incorporation
- Registration Number or Date of Registration (Incorporation)
- Business Category as defined in section 6(a)(3) of the EV guidelines
- Physical Address of Place of Business (City, State, Country)
- Applicant’s public key
- Code of applicant’s country
- Issuing certification authority (GlobalSign CA)
- GlobalSign electronic signature
- GlobalSign’s unique Policy OID for ExtendedSSL certificates
- Type of algorithm
- Organizational Unit (OU) (Non Verified)
- Validity period of the digital certificate
- Serial number of the digital certificate
• Optional Subject Alternative Name entries which may detail additional domains owned or controlled by the Applicant.

1.10.4 Information Submitted to Identify the Applicant

The certificate request must contain complete and accurate data WHEN relating to the following:

• organization Name (formal legal organization name)
• Assumed Name (optional)
• Domain Name
• An optional Subject Alternative Name entry which may detail additional domains owned or controlled by the Applicant.
• Jurisdiction of Incorporation (city, state, province, country)
• Incorporating Agency (name)
• Registration Number (assigned by the incorporating agency) or date of incorporation if no number is allocated by the incorporating agency
• Business Category as defined in section 6(a)(3) of the EV guidelines
• Applicant Address (including phone number)
• Certificate Approver (name and contact information)
• Certificate Requester (name and contact information)

1.10.5 Data Verification

As to data verification, GlobalSign ensures that the following Subject organization information has been submitted by the applicant and shall be verified by the CA in accordance with the EV Guidelines (Sections 14 through 25) by taking all verification steps reasonably necessary:

1 Applicant’s existence and identity, including where applicable:
   (a) Applicant’s legal existence and identity (as established with an Incorporating Agency),
   (b) Applicant’s physical existence (business presence at a physical address), and
   (c) Applicant’s operational existence (business activity) and where applicable to the Business Category type,
   (d) The principle individual(s)
2 Applicant’s exclusive control of the domain name and applicable Subject Alternative Name domains to be included in certificate;
3 Applicant’s authorization for the ExtendedSSL certificate, including:
   (a) Contract Signer, certificate Approver and certificate Requester name, title, and authority
   (b) Subscriber Agreement signing by Contract Signer
   (c) Approval by the certificate Approver of the certificate Request.

In this regard, GlobalSign acknowledges that a satisfactory data verification process requires an appropriate assessment of the legal and administrative practices that are applicable in the applicant’s jurisdiction. GlobalSign shall consequently take all reasonable steps to conform to the said practices.

In all cases, GlobalSign is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the EV Guidelines Verification Requirement (e.g. Verification through verified Legal Opinion, verified Accountant letter, or other Qualified Independent Information Sources or Qualified Government Information source). In addition, GlobalSign shall take reasonable steps to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks (phishing and other fraudulent schemes), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under the EV Guidelines.

1.10.5.1 Data Validation Dual Role

After all of the verification processes and procedures are completed, GlobalSign reviews all of the information and documentation assembled in support of the ExtendedSSL certificate and look for discrepancies or other details requiring further explanation.
GlobalSign assigns such review to a person (Validation Specialist) who is not responsible for the collection of information.

GlobalSign enforces control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an ExtendedSSL certificates.

GlobalSign ensures that the Validation Specialists pass an internal examination and qualify for each skill level required by the corresponding validation task before granting privilege to perform said task.

GlobalSign provides Validation Specialists with skills training that covers basic PKI knowledge, authentication and verification policies and procedures and common threats to the validation process including phishing and other social engineering tactics.

### 1.10.5.2 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For ExtendedSSL, a verification time of 1 - 10 working days might be required.

### 1.10.5.3 Data Validity

The maximum validity period for validated data that can be used to support issuance of an ExtendedSSL certificate (before revalidation is required) is one year.

### 1.10.5.4 Issuance Prohibition

GlobalSign shall not issue any ExtendedSSL Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant’s Jurisdiction of Incorporation or Place of Business is identified on any government denied list, list of prohibited persons, list of prohibited countries, or other list that prohibits doing business with such organization or person under the laws of the country of the CA’s jurisdiction(s) of operation.

### 1.10.6 Issuing Procedure

The issuing procedure for an ExtendedSSL certificate is as follows:

1. The Certificate Requester acting on behalf of the applicant follows the on line and off line registration procedure.
2. The Certificate Requester gathers the required information as specified under 1.10.4 of this CPS including but not limited to technical contact, server information, and payment information.
3. The Contract Requester ensures that the subscriber agreement is signed by the Contract Signer on behalf of the applicant.
4. The Contract Requester ensures that the certificate request is properly filled out.
5. The Certificate Requester sends both the subscriber agreement and the certificate request to GlobalSign on behalf of the applicant.
6. GlobalSign ensures that the Certificate Approver approves the certificate request submission on behalf of the applicant.
7. GlobalSign verifies the submitted information as specified under 1.10.5 of this CPS and the related provisions of the EV Guidelines incorporated by reference herein.
8. The Applicant creates a Certificate Signing Request (CSR) and a key pair using appropriate server software or the Applicant requests GlobalSign to generate the key pair on its behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism.
GlobalSign may issue the certificate to the applicant.

If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will do so in a secure manner protected by the strong password provided by the applicant during the registration process. GlobalSign will then delete all instances of the Applicant’s private key.

GlobalSign may publish the issued certificate in an online database.

Renewal: allowed
Revocation: allowed
Reissue: not allowed

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.10.7 Limited Warranty

1.10.7.1 Subscribers and Relying Parties

In cases where GlobalSign has issued and managed the ExtendedSSL certificate in compliance with these Guidelines, GlobalSign shall not be liable to the ExtendedSSL certificate beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such certificate beyond those specified in this CPS. Refer to 9.8.1 for ExtendedSSL Warranty.

1.10.7.2 Indemnification of Application Software Vendors

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, GlobalSign acknowledges that the Application Software Vendors who has a root certificate distribution agreement in place do notassume any obligation or potential liability of GlobalSign under these Guidelines or that otherwise might exist because of the issuance or maintenance of ExtendedSSL certificates or reliance thereon by Relying Parties or others.

Thus, GlobalSign shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an ExtendedSSL Certificate, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an ExtendedSSL certificate issued by GlobalSign where such claim, damage, or loss was directly caused by such Application Software Vendor’s software displaying as not trustworthy an ExtendedSSL certificate this is still valid, or displaying as trustworthy: (1) an ExtendedSSL certificate that has expired, or (2) an ExtendedSSL certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the browser software either failed to check such status or ignored an indication of revoked status).

1.10.7.3 Root CA Indemnification

In cases where the Subordinate CA and the Root CA are different legal entities and the Root CA specifically enables the Subordinate CA to issue ExtendedSSL Subscriber Certificates, the Root CA shall also be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA’s compliance with the EV Guidelines, and for all liabilities and indemnification obligations of the Subordinate CA under the EV Guidelines, as if the Root CA was the Subordinate CA issuing the ExtendedSSL Certificates.

However, this Section shall not apply to cases where a Root CA, Root CA “A”, from a different legal entity, cross-certifies Root CA “B” to enable certificates issued by “B” to be trusted in older, non-EV enabled browsers. The cross certificate issued by “A” to “B” does not enable EV according to these guidelines. Certificates issued by “B” are EV enabled only when an EV enabled browser can build a certificate chain to the root certificate of “B”.
1.10.8 Insurance Plan
As to ExtendedSSL Certificates, GlobalSign maintains an appropriate insurance related to its respective performance and obligations under this CPS and the EV Guidelines.

1.10.9 Relevant GlobalSign Documents
The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Data Protection Policy
4. CA/Browser Forum Guidelines for Extended Validation Certificates
5. Warranty Policy

1.11 Educational ServerSign

1.11.1 General
Educational ServerSign certificates are meant for secure communication with for example a website through an SSL or TLS link.

The applicant is an organization within the educational or research environment that has an Internet Server such as a website. Educational ServerSign certificates are used to assure the Internet Server’s identity to the visitor and to assure a confidential communication with the Internet Server.

Educational ServerSign certificates validity period is between one and three years. Educational ServerSign certificates are issued to entities and self employed professionals registered with a professional organization which is operating in the educational or research space.

The period retention for records fulfills professional records requirements of the Laws of the Belgium.

1.11.2 Certificate Requests
A certificate request can be made in the following way:
On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity of the Internet Server, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

1.11.3 Content
Typical information published on a GlobalSign Educational ServerSign certificate includes the following elements:

- Applicant’s domain name
- Applicant’s name of organization
- Applicant’s public key
- Code of applicant’s country
- Issuing certification authority (GlobalSign CA)
- GlobalSign electronic signature
- Type of algorithm
1.11.4 Information Submitted to Identify the Applicant

The applicant must provide business and contact details to GlobalSign and underwrite those by click-through process. GlobalSign has the right to request a signed registration form, a signed subscriber agreement, the articles of association of the applying organization and proof of the applying organization belonging to the educational or research market if it deems necessary. Independent verification through consulting industry or other database with telephone confirmation will be performed.

1.11.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For GlobalSign Educational ServerSign, a verification time of 1 - 5 working days might be required.

1.11.6 Issuing Procedure

The issuing procedure for an Educational ServerSign certificate is as follows:

1. The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
2. The applicant follows the on line registration procedure.
3. The applicant submits the required information including organizational information, technical contact, server information and if required payment information.
4. The applicant accepts by click-through the on line subscriber agreement.
5. Data is sent with certificate request to GlobalSign automatically.
6. GlobalSign verifies the submitted information by checking organizational and any other information as it sees fit. This may also include checks in third party databases or resources and independent verification through telephone.
7. GlobalSign may positively verify the applicant.
8. GlobalSign may issue the certificate to the applicant.
9. Renewal: allowed
10. Revocation: allowed

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.11.7 Limited Warranty

Educational ServerSign is exempt from GlobalSign’s limited warranty program. To the extent permitted by law, GlobalSign Educational warranty is limited to 1 Euro for any case of proven damages to a subscriber.

1.11.8 Relevant Globalsign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1. GlobalSign CPS
2. Subscriber Agreement

1.12 Code Signing

1.12.1 General

Code Signing certificates are used for the signing of software objects, such as software packages or applets.
Code Signing certificates validity period is between one and three years.

Code Signing certificates are issued to natural persons, legal persons and self-employed professionals. For self-employed persons belonging to an association or professional group, an official document from the professional group and membership card may be required.

GlobalSign may require additional identification proof in support of the verification of the applicant.

The period retention for records meets professional records requirements according to the Laws of Belgium.

1.12.2 Certificate Requests

A certificate request can be done according to the following means:

**On-line:** Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

**API:** The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.12.3 Content

Typical information published on a Code Signing certificate includes the following elements:

- Applicant's e-mail address
- Applicant's organization name for legal persons, or in the case of natural persons, the full legal name.
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- GlobalSign's unique Policy OID for Code Signing certificates
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.12.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must either submit to a GlobalSign Registration Authority a signed registration form or maintain a GlobalSign Certificate Centre Account allowing click through agreements to be presented and approved. For legal persons a GlobalSign Registration Authority will validate the business existence and registration details via a source such as a Qualified Government Information Source or a Qualified Independent Information Source in order to verify the authenticity of the request. In the case of a natural person, the applicant must submit to a GlobalSign Registration Authority a signed copy of an identification document such as an identity card, driver's license or passport. In addition, third party independent verification checks may be performed.
1.12.5 Time to Confirm Submitted Data
GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For Code Signing verification might require 1 to 5 working days.

1.12.6 Issuing Procedure
Below following the steps to issue a Code Signing certificate:

1. The applicant fills out online the registration form: e-mail address, organizational information if appropriate, common name, country code, payment info
2. The applicant accepts the online subscriber agreement
3. Either a key pair is generated on an applicant’s device (e.g. computer, smart card device etc.) or the subscriber requests that GlobalSign generates a key pair on their behalf. In the latter case the application requires a strong password from the applicant to facilitate a secure delivery mechanism.
4. The public key and online request are sent to GlobalSign automatically
5. GlobalSign verifies the submitted information by checking organizational, payment and any other information as it sees fit also through third party databases or resources. This may also include checks in third party databases or resources and independent verification through telephone.
6. GlobalSign may positively verify the applicant.
7. If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will be protected by the strong password provided by the applicant during the registration process.
8. GlobalSign may issue the certificate to the applicant.
9. Renewal: allowed
10. Revocation: allowed

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.12.7 Limited Warranty
GlobalSign accepts liability up to a maximum of 37500 EURO per loss due to a false identity in a Code Signing certificate issued within the terms of the CPS.

1.12.8 Relevant GlobalSign Legal Documents
The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Data Protection Policy
4. Warranty Policy

1.13 GlobalSign Time stamping

1.13.1 General
GlobalSign Time stamping certificates are used by Applicants to provide time stamping services and non repudiation services for the time stamping and signing of software objects, documents and time critical events. In general:-

- GlobalSign Time stamping certificate validity period is 11 years.
- GlobalSign Time stamping certificates shall only be installed on hardware (FIPS 140-1 level 2 or equivalent)
- GlobalSign Time stamping certificates are issued to legal persons.
• The period retention for records meets professional records requirements according to the Laws of Belgium.

1.13.2 Certificate Requests

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

1.13.3 Content

Typical information published in a GlobalSign Time stamping certificate includes the following elements:

• Applicant’s e-mail address
• Applicant’s name of organization
• Applicant’s public key
• Code of applicant’s country
• Issuing certification authority (GlobalSign)
• GlobalSign electronic signature
• GlobalSign’s unique Policy OID for Time stamping certificates
• Type of algorithm
• Validity period of the digital certificate
• Serial number of the digital certificate

1.13.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit to a GlobalSign Registration Authority a signed registration form. In all cases a GlobalSign Registration Authority will validate the business existence and registration details via a source such as a Qualified Government Information Source or a Qualified Independent Information Source in order to verify the authenticity of the request.

1.13.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. For GlobalSign Time stamping certificates verification might require 5 working days.

1.13.6 Issuing Procedure

Below following the steps to issue a GlobalSign Time stamping certificate:

1. The applicant fills out the registration form: e-mail address, organizational info, common name, country code, payment info
2. The applicant accepts the obligations of the relevant subscriber agreement
3. Either a key pair is generated on an applicant’s device (e.g. HSM, smart card device etc.)
4. The public key and online request are sent to GlobalSign automatically
5. GlobalSign verifies the submitted information by checking organizational, payment and any other information as it sees fit also through third party databases or resources. This may also include checks in third party databases or resources and independent verification through telephone.
6. GlobalSign may positively verify the applicant.
7. GlobalSign may issue the certificate to the applicant.
8. Renewal: allowed
9. Revocation: allowed
10. Rekey/Reissuance: allowed
GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.13.7 Limited Warranty
GlobalSign accepts liability up to a maximum of 2500 EURO per loss due to a false identity in an GlobalSign Time stamping certificate issued within the terms of the CPS.

1.13.8 Relevant GlobalSign Legal Documents
The applicant must take notice and is bound by the following documents available on www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Data Protection Policy
4. Warranty Policy

1.14 Certificate usages

Certain limitations apply to the use of GlobalSign certificates. A GlobalSign certificate can only be used for purposes explicitly permitted as they are listed below:

**Electronic signature:** Electronic signature can only be used for specific electronic transactions that support electronic signing of electronic forms, electronic documents, electronic mail etc. The signature certificate is only warranted to produce electronic signatures in the context of applications that support digital certificates. To describe the function of an electronic signature, the term non-repudiation is often used. Certificates that are appropriate for electronic signature are the following:

- PersonalSign 2: non repudiation of a transaction (medium level assurance)
- PersonalSign2 Pro: non repudiation of the transaction by a party acting in an organizational context (medium level assurance)
- DocumentSign: non repudiation of the transaction by a party acting in an organizational context (medium level assurance)
- PersonalSign 3: non repudiation of the transaction (high level assurance)
- PersonalSign 3 Pro: non repudiation of the transaction by a party acting in an organizational context (high level assurance)

**Authentication (Users):** User authentication certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail etc. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a digital certificate. To describe the function of authentication, the term digital signature is often used.

- PersonalSign 1: authentication of the existence of an email address
- PersonalSign 2: authentication of a natural person (medium level assurance)
- PersonalSign2 Pro: authentication of a natural person within an organizational context or a role within an organizational context (medium level assurance)
- DocumentSign: authentication of a natural person within an organizational context or a role within an organizational context (medium level assurance)
- PersonalSign 3: authentication of a natural person (high level assurance)
- PersonalSign 3 Pro: authentication of a natural person within an organizational context (high level assurance)

**Authentication (Devices and objects):** Device authentication certificates can be used for specific electronic authentication transactions that support the identifying of web sites and other on line resources, such as software objects etc. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating a device that the...
subscriber seeks to secure through a digital certificate. To describe the function of authentication, the term digital signature is often used.

- DomainSSL: authentication of a remote domain name and webservice and encryption of the communication channel.
- OrganizationSSL: authentication of a remote domain name and webservice and encryption of the communication channel.
- ExtendedSSL: authentication of a remote domain name and webservice and encryption of the communication channel.
- Educational ServerSign: authentication of a remote domain name and webservice and encryption of the communication channel.
- Code Signing: authentication of a data object.
- GlobalSign Timestamping: authentication of a time and date related to a service.

**Assurance levels:** Low assurance (Class 1) certificates are not suitable for identity verification as no authenticated identity information is included within the certificate. This in turn does not support non-repudiation services.

Medium assurance (Class 2) certificates are certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the subject identity contained within the certificate.

High assurance (Class 3) certificates are individual and organizational certificates that provide a high level of assurance of the identity of the subject in comparison with Class 1 and 2.

High assurance with extended validation certificates are Class 3 certificates issued by GlobalSign in conformance with the Guidelines for Extended Validation Certificates.

**Confidentiality:** All certificate types can be used to ensure the confidentiality of communications effected by means of digital certificates. Confidentiality is required to assure the confidentiality of business and personal communications as well as for purposes of personal data protection and privacy.

Any other use of a digital certificate is not supported by this CPS. When using a digital certificate the functions of electronic signature (non-repudiation) and authentication (digital signature) are permitted together with the same certificate. The different terms used i.e. electronic signature as opposed to non-repudiation and authentication as opposed to digital signature relate to the different terminology in the IETF and the vocabulary adopted in the legal framework in the European Union manifested by the Directive 1999/93/EC on a Community framework on electronic signatures.

### 1.15 Document Name and Identification

GlobalSign ensures compliance of its certificates with the requirements and assertions of this CPS.

### 1.16 PKI participants

The GlobalSign CA makes its services available to GlobalSign subscribers. These subscribers include without limitation entities that use certificates for the purposes of:

- Authentication (digital signature)
- Electronic signature (non-repudiation)
- Encryption

Where appropriate to the product type a subject is a natural person that successfully applies for a certificate. Any other uses of certificates are restricted. Certificates can be used for any public purposes. As “public” this CPS considers any use that takes place among subscribers who are not restricted to uses governed by voluntary agreements under private law among participants.
NB. Under the scope of this policy general-purpose uses associated with services made available by the Belgian government are allowed. GlobalSign reserves its right to evaluate uses within various application environments that it does not specifically prohibit. Subscribers and relying parties are hereby notified to contact GlobalSign before applying for or using a certificate in an application domain, which mandates proprietary or non-public requirements with a view to ensure the functionality of certificates.

1.16.1 GlobalSign Certification Authority

A Certification Authority, such as GlobalSign, is an organization that issues digital certificates to be used in public or private domains, within a business framework, a transactions context etc. A certification authority is also referred to as the Issuing Authority to denote the purpose of issuing certificates at the request of an RA.

The GlobalSign CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates. The GlobalSign CA is a Policy Authority with regard to issuing GlobalSign CA certificates. The GlobalSign CA has ultimate control over the lifecycle and management of the GlobalSign CA Root and any subsequent root belonging to its hierarchy.

The GlobalSign CA ensures the availability of all services pertaining to the management of certificates under the GlobalSign CA Root, including without limitation the issuing, revocation, status verification of a certificate, as they may become available or required in specific applications. The GlobalSign CA also manages a core online registration system for all certificate types, issued under the GlobalSign CA Root.

Appropriate publication is necessary to ensure that relying parties obtain notice or knowledge of functions associated with the revoked certificates. Publication is manifested by including a revoked certificate in a certificate revocation list that is published in an online directory. Issued certificates also appear on directories of issued certificates. The GlobalSign CA operates such directories.

The domain of responsibility of the GlobalSign CA’s comprises of the overall management of the certificate lifecycle including the following actions:

- Issuance
- Revocation
- Renewal
- Status validation
- Directory service

Some of the tasks attributed to the certificate lifecycle are delegated to selected GlobalSign RAs that operate on the basis of a service agreement with GlobalSign.

1.16.1.1 GlobalSign outsource agent

Through an outsource agent GlobalSign operates a secure facility in order to deliver CA services including the issuance, revocation, renewal and status validation of GlobalSign CA certificates. The GlobalSign outsource agent operates a service to GlobalSign on the basis of a service agreement. The scope of the service is the support in certificate management. The GlobalSign outsource agent warrants designated services and service levels that meet those required by GlobalSign. The GlobalSign outsource agent carries out tasks associated with the administration of services and certificates on behalf of GlobalSign.

1.16.1.2 Roles of GlobalSign

GlobalSign operates under two discrete roles.

Firstly, as a Trust Service Provider to deliver Trust Services to a user community, directly or through an agent. An agent in this case includes third party entities, called Registration...
Authorities (RAs) that operate under agreement with and within the conditions laid out by GlobalSign.

Secondly GlobalSign operates an international network of Trusted Third Parties (TTP’s) sharing the GlobalSign procedures and using suitable brand name to issue high quality and highly trusted digital certificates to public and private entities. Such partners include GlobalSign accredited Certification Authorities and RAs that operate under an agreement with GlobalSign. This role is typically limited to the issuance of certificates to other certification authorities, which seek to inherit trust that is usually vested in the GlobalSign CA root and brand name.

The main activities of GlobalSign are to:
- Manage an international network of RAs, establishing the brand name of GlobalSign as a universal Trusted Third Party leveraging on in PKI technology.
- Manage the life cycle of digital certificates issued to end user entities as well as to other certification authorities and administrators within the GlobalSign domain.

The GlobalSign public certification services aim at supporting secure electronic commerce and on-line business services to address the business and personal requirements of the users of electronic signatures.

Responding to the need for secure electronic transactions among users and service providers in a global market place, GlobalSign published or documented practices support the GlobalSign infrastructure and to deliver high quality trust services to diverse user communities in Europe and the world GlobalSign is a subsidiary of GlobalSign.

1.16.1.3 GlobalSign root and hierarchy

GlobalSign makes available to subscribers a dedicated root hierarchy to ensure the integrity of the end user certificate and the uniqueness of the resources made available for digital certificates. The GlobalSign CA manages a broader range of the GlobalSign trust network that includes roots that have been set up to fulfil specific purposes such as the issuance of end user certificates at levels defined by GlobalSign etc. as well as other participating CAs that take advantage from GlobalSign’s root, which is embedded in applications. The GlobalSign Certificate Policy addresses the Root level of the GlobalSign hierarchy.

The GlobalSign CA root has been used to certify each of the private keys of the subsequent third party CA roots. By validating the certificate of such a CA, trust vested in GlobalSign can also be extended to the certified third party CA root.

GlobalSign periodically rekeys or refreshes Intermediate CAs. Third party applications or platforms that have an intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. GlobalSign therefore does not warrant the use of intermediate CAs as root certificates.

The roots that are addressed under this CPS include roots used for issuing the following type of certificates:
- PersonalSign 1
- PersonalSign 2 / Pro 2
- PersonalSign 3 / Pro 3
- DocumentSign
- OrganizationSSL
- DomainSSL
- ExtendedSSL
- Educational ServerSign
- Timestamping
- Code Signing
1.16.2 Registration Authorities

A Registration Authority (RA) is an entity that identifies and authenticates applicants for certificates. A Registration Authority may also initiate or pass along revocation requests for certificates and requests for re-issuance (sometimes referred to as rekey) and renewal of certificates. GlobalSign may act as a Registration Authority for certificates that it issues.

Third parties, who enter into a contractual relationship with GlobalSign may operate their own RA and authorize the issuance of certificates. Third parties must abide by all the requirements of the GlobalSign CP and this CPS and the terms of their enterprise services agreement. RA’s may implement more restrictive vetting practices if their internal policy dictates.

1.16.2.1 RA role description

A GlobalSign RA interacts with the subscriber to deliver public certificate management services to the end-user. A GlobalSign RA:

- Accepts, evaluates, approves or rejects the registration of certificate applications.
- Registers subscribers to GlobalSign CA certification services.
- Attends all stages of the identification of subscribers as assigned by the GlobalSign CA according to the type of certificates they issue.
- Uses official, notarised or otherwise authorised documents to evaluate a subscriber application.
- Following approval of an application, notify the GlobalSign CA to issue a certificate.
- Initiates the process to revoke a certificate and request a certificate revocation from the GlobalSign CA Root.

The GlobalSign RA acts locally on approval and authorisation by the GlobalSign CA. The GlobalSign RA acts in accordance with the approved practices and procedures of the GlobalSign CA including this CPS and documented GlobalSign RA procedures.

In order to issue certain specific certificate type, GlobalSign RAs might need to rely on certificates issued by third party certification authorities or other third party databases and sources of information. Identity cards and drivers licenses are such sources of authoritative subscriber information. Relying Parties are hereby prompted to seek specific information by referring to the appropriate certificate policies prevailing in managing specific certificate types issued under the GlobalSign Root.

If successful, the evaluation is followed by the issuance of the certificate to the applicant organization.

Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of RAs.

1.16.2.2 RA specific requirements for ExtendedSSL certificates

For the issuance of ExtendedSSL certificates, GlobalSign contractually obligates each RA and/or subcontractor to comply with all applicable requirements in the EV Guidelines incorporated by reference herein and to perform them as required of the CA itself.

Under the terms of the EV Guidelines, GlobalSign may contractually authorize the Subject of a specified valid EV certificate to perform the RA function and authorize GlobalSign to issue additional EV Certificates at third and higher domain levels that contain the domain that was included in the original EV Certificate (also known as “Enterprise EV Certificates”). In such case, the Subject shall be considered an Enterprise RA, and shall not authorize the CA to issue any ExtendedSSL certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA.

---

1 An example of a third party RA is a customer of an Enterprise PKI solution
GlobalSign shall not delegate the performance of the Final Cross-Correlation and Due Diligence requirements of Section 24 of Extended Validation Guidelines, which are briefly described under this CPS (1.10.1.5 - final paragraph).

1.16.3 Subscribers

The GlobalSign CA reaches its subscribers through designated Registration Authorities (‘RA’). An RA requests the issuance and revocation of a certificate under this CPS. An RA submits the necessary data for the generation and revocation of the certificates to the CA.

Subscribers of GlobalSign services are natural persons or legal persons that successfully apply for a certificate. Subscribers use electronic signature services within the domain of the GlobalSign CA. Subscribers are parties that:

- Set the framework of providing certification services with the GlobalSign CA to the benefit of the subject mentioned in a certificate.
- Have authority over the private key corresponding to the public key that is listed in the certificate.
- Natural persons that are subscribers typically hold a valid identification document, such as an identity card, passport or equivalent, which is used as credential in order to issue electronic certificates.

Legal persons are identified on the basis of the published by-laws and appointment of Director as well as the subsequent government gazette (e.g. Staatsblad/Moniteur Belge in Belgium etc.) or other QIIS or QGIS third party databases. Self-employed subjects are identified on the basis of proof of professional registration supplied by the competent authority in the country in which they reside.

For all categories of subscribers, additional credentials are required as explained on the online process for the application for a certificate.

Subscribers of end entity certificates issued under the GlobalSign CA include employees and agents involved in day-to-day activities within GlobalSign that require access to GlobalSign network resources.

Subscribers are also sometimes operational or legal owners of signature creation devices that are issued with for the purpose of generating a key pair and storing a certificate.

It is expected that a subscriber organization has an employment or service agreement or otherwise a pre-existing contract relationship with GlobalSign authorising it to carry out a specific function within the scope of an application that uses GlobalSign certificate services. Granting a certificate to a subscriber organization is only permitted pursuant to such an agreement between GlobalSign and the subscribing end entity.

1.16.4 Subjects

Subjects of GlobalSign CA certificate services may be natural persons in that they are themselves subscribers or are associated with a subscriber. Subjects may be individuals, organizations, or infrastructure components such as firewalls, routers, servers or other devices used within an Organization. Subjects use electronic signature services under authorisation of and within the domain that is designated by the subscriber (if applicable). Subjects are parties that:

- Are identified in a certificate or are the custodian of a digital ID with a subject DN containing a department, role-based common name
- Hold the private key corresponding to the public key that is listed in a subscriber certificate.

A subject enrolls with the GlobalSign RA or a Service Provider that requires it to use a certificate within the designated service. A subject nominates a named Certificate Applicant also called a
Subscriber, to apply for a certificate. A certificate applicant can be any natural person acting on behalf of the subject.

Natural persons can be listed as subjects of the following certificates:
- PersonalSign 2
- PersonalSign 2 Pro
- DocumentSign
- PersonalSign 3
- PersonalSign 3 Pro
- Code Signing

Department or role-based entities can be listed as Subjects of the following certificates:
- PersonalSign 2 Pro
- DocumentSign

Legal persons created through all recognized forms of incorporation or government entities can be listed as subjects of the following certificates:
- ExtendedSSL
- GlobalSign Timestamping

Legal persons or self-employed professionals can be listed as subjects of the following certificates:
- OrganizationSSL
- Educational ServerSign
- Code Signing

1.16.5 Certificate Applicants
A certificate applicant is a party wishing to become a subscriber of a certificate. A certificate applicant is a party designated by the subject to act on the subject’s behalf in:
- Applying for a certificate.
- Agreeing with and accepting the CA’s subscriber agreement.

The applicant may be:
- The same as the subject itself, where this is a named individual.
- A custodian of a department or role-based subject name.
- An individual employed by the subject.
- An individual employed by a contractor, or sub-contractor acting upon explicit authorisation.

1.16.6 Relying Parties
Relying parties are natural persons or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber’s certificate. For example, the GlobalSign operators that receive signed requests from GlobalSign CA subjects are relying parties of the GlobalSign certificates.

To verify the validity of a digital certificate, relying parties must always refer to GlobalSign CA revocation information, currently a Certificate Revocation List (CRL). Certificate validation takes place prior to relying on information featured in a certificate. Alternatively, relying parties may refer to an automated response by using the OCSP protocol where available. Relying parties meet specific obligations as described in this CPS.

1.17 Certificate use
Certain limitations apply to the use of GlobalSign CA certificates.
1.17.1 Appropriate certificate usage

Certificates issued under the GlobalSign CA can be used for public domain transactions that require:

- Non-repudiation and
- Authentication
- Confidentiality

Additional uses are specifically designated once they become available to end entities. Unauthorised use of GlobalSign certificates may result in an annulment of warranties offered by the GlobalSign CA to subscribers and relying parties of GlobalSign certificates.

1.17.2 Prohibited certificate usage

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not authorised. GlobalSign certificates are not authorised for use within Closed Groups unless such Groups have notified GlobalSign thereof and GlobalSign has consented to it. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the Limited Warranty Policy.

1.17.3 Certificate extensions

GlobalSign issues certificates that contain extensions defined by the X.509 v.3 standard other standards as well as any other formats including those used by Microsoft and Netscape. GlobalSign uses certain constraints and extensions for its public PKI services as per the definition of the International Standards organization (ISO). Such constraints and extensions may limit the role and position of a CA or subscriber certificate so that such subscribers can be identified under varying roles.

As key usage extension limits the technical purposes for which a public key listed in a certificate may be used. GlobalSign’s own certificates may contain a key usage extension that limits the functionality of a key to only signing certificates, certificate revocation lists, and other data.

A certificate policy extension limits the usage of a certificate to the requirements of a business or a legal context. GlobalSign pro-actively supports and participates in the proliferation of industry, government or other certificate policies for its public certificates as it sees appropriate.

1.17.4 Critical Extensions

GlobalSign uses certain critical extensions in the certificates it issues such as:

- A basic constraint in the certificate to show whether a certificate is meant for a CA or not.
- To show the intended usage of the key.
- To show the number of levels in the hierarchy under a CA certificate.

1.18 Policy Administration

The GlobalSign CA is a top root authority (also known as trust anchor) that manages certificates services within its own domain. The GlobalSign CA might also interact with or seek recognition by third party certification authorities.

The Policy Managing Authority of the GlobalSign CA manages this GlobalSign CPS. The GlobalSign CA registers, observes the maintenance, and interprets this CPS. The GlobalSign CA makes available the operational conditions prevailing in the life-cycle management of certificates issued under the GlobalSign CA root. The operational conditions for each root are publicised in this CPS.

1.18.1 Scope

In an effort to invoke credibility and Trust in the publicised GlobalSign CPS and to better correspond to accreditation and legal requirements, GlobalSign may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all
certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CP and/or CPS.

1.18.2 GlobalSign Policy Management Authority

New versions and publicized updates of GlobalSign policies are approved by the GlobalSign Policy Management Authority. The GlobalSign Policy Management Authority in its present organizational structure comprises members as indicated below:

- At least one member of the management of GlobalSign.
- At least two authorised agents directly involved in the drafting and development of GlobalSign practices and policies.

The Management member chairs the GlobalSign Policy Management Authority ex officio.

All members of the GlobalSign Policy Management Authority have one vote. There are no other voting rights reserved for any other party. In case of lock vote the vote of the Chair of the GlobalSign Policy Management Authority counts double.

1.18.3 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the GlobalSign Policy Management Authority that CPS is published in the GlobalSign online Repository at http://www.globalsign.com/repository.

GlobalSign publishes a notice of such updates on its public web site at http://www.globalsign.com. The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CPS is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the GlobalSign CPS.

Subscribers that are affected by changes may file comments with the policy administration organization within 15 days from notice. Only subscribers and the supervisory authority may submit objections to policy changes. Relying parties that are not subscribers do not have the right to submit objections and any such submissions will be regarded as never received.

GlobalSign publishes on its web site at least the two latest versions of its CPS.

1.18.3.1 Changes with notification

Updated versions of this CPS are notified to parties that have a legal duty to receive such updates, e.g. auditors with a specific mandate to do so.

1.18.4 Version management and denoting changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

1.19 Definitions and acronyms

A list of definitions can be found at the end of this CPS.
2.0 Publication and Repository Responsibilities

GlobalSign reserves its right to publish information about the digital certificates that it issues in an online publicly accessible repository. GlobalSign reserves its right to publish certificate status information on third party repositories.

GlobalSign retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain policies including this CPS. GlobalSign reserves its right to make available and publish information on its policies by any appropriate means within the GlobalSign repository.

All parties who are associated with the issuance, use or management of GlobalSign certificates are hereby notified that GlobalSign may publish submitted information on publicly accessible directories in association with the provision of electronic certificate status information.

GlobalSign refrains from making publicly available certain elements of documents including security controls, procedures, internal security polices etc. However these elements are disclosed in audits associated with formal accreditation schemes that GlobalSign adheres to, such as Web Trust for CAs and EV WebTrust for CA.

2.1 Access control on repositories

While GlobalSign strives to keep access to its public repository and access to its policy is (e.g. CP, CPS etc.) free of charge, it might charge for services such as the publication of status information on third party databases, private directories, etc.
3.0 Identification and Authentication

GlobalSign operates RAs that verify and authenticate the identity and/or other attributes of an end-user certificate applicant for a certificate.

Prior to requesting the CA to issue a certificate, GlobalSign RAs verify the identity of applicants of a certificate.

Certificate Applicants are prohibited from using names in their certificate that infringe upon the Intellectual Property Rights of others. GlobalSign does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in the certificate application or arbitrate, mediate or otherwise resolve any dispute concerning the ownership of any domain name, trademark, trade name or service mark. GlobalSign is entitled without liability to any Certificate Applicant, to reject any certificate Application because of such dispute. GlobalSign RAs authenticate the requests of parties wishing to revoke certificates under this policy.

3.1 Naming

To identify a subscriber, the GlobalSign CA follows and the GlobalSign RAs apply certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names, RFC-822 names or X.400 names. The GlobalSign CA issues certificates to applicants that submit a documented application containing a verifiable name.

3.2 Initial Identity Validation

The identification of the applicant for a certificate is carried out according to a documented procedure to be implemented by the GlobalSign RAs.

For the identification and authentication procedures of the initial subscriber registration GlobalSign takes the following steps:

- The natural person identified in the subject field must demonstrate possession of the private key corresponding to the public key presented to the GlobalSign CA. The subject itself or its designated representative must demonstrate this.
- GlobalSign RAs might rely on such resources as third party databases to identify and authenticate natural persons applying for a certificate.

For the identification and authentication of appropriately authorised third party agents applying for a GlobalSign certificate include the following:

- Controlling physical identification documents such as an identity card or passport issued by a designated authority in the country of origin of the applicant.
- Authenticating the identity of the applicant based on other documentation or credentials provided.
- Requesting an applicant to physically appear before a GlobalSign RA prior to issuing a certificate.
- Requesting a third party agent or his/her principal (e.g. a GlobalSign contractor) to produce evidence with regard to the relationship between GlobalSign and the third party agent (e.g. an outsource contract etc.).

A GlobalSign RA may refuse issuing a certificate to an applicant unless sufficient evidence is produced with regard to the applicant’s identity. If an application is rejected applicants may subsequently reapply.

To issue certificates, a GlobalSign RA endeavours to provide the applicant with sufficient credentials (enrollment URL, password) such that the enrollment process can then proceed online.
At GlobalSign’s discretion any such credentials may be two-factor, communicated by independent channels using agreed and proven contact methods.

The identification of an applicant for a certificate is carried out according to a documented procedure to be implemented by the GlobalSign RAs.

### 3.3 Subscriber registration process

Unless otherwise provided in this CPS in connection with the EV guidelines (ExtendedSSL certificates), the following rules applies as to the Subscriber Registration Process.

GlobalSign ensures that:
- Subscribers of certificates are properly identified and authenticated
- Subscriber certificate requests are complete, accurate and duly authorized.

In particular:
- GlobalSign provides notice to the applicant through its web site at www.globalsign.com and the dedicated policy framework published on its repository at www.globalsign.com/repository.
- Before entering any contractual relationship with the subscriber, GlobalSign makes available a subscriber agreement, which the applicant must approve prior to placing a request with GlobalSign. This agreement can also be consulted in advance on GlobalSign’s repository at www.globalsign.com/repository.
- GlobalSign’s policy framework is limited under data protection and consumer protection laws and warranty, as explained in the GlobalSign CPS as well as GlobalSign’s Limited Warranty framework.
- GlobalSign maintains documented contractual relationships with all third party registration authorities or outsourced agents it uses to deliver certificates.

#### 3.3.1 Documents used for subscriber registration

GlobalSign or an authorized GlobalSign RA typically verifies by appropriate means and on the basis of a documented procedure, the identity and, if applicable, all specific attributes thereof of applicants of certificates.

Evidence on identity is checked against a natural person either directly or indirectly using means which provide equivalent assurance to physical presence. Submitted evidence may be in the form of either paper or electronic documentation. Examples of evidence checked indirectly against a natural person is documentation presented for registration that was acquired as the result of an application requiring physical presence.

Evidence on identity of organizations is checked through third-party databases such as Qualified Government Information Sources or Qualified Independent Information Sources to establish the existence of organizations. Any submitted evidence may be in the form of either paper or electronic documentation.

Self-employed professionals that are eligible to be issued with certificates typically have to prove their identity as individuals as well as their professional registration.

Specific documents required include the following:

#### 3.3.1.1 PersonalSign 1

No specific documented proof of identity is required

#### 3.3.1.2 PersonalSign 2

The applicant must submit to a GlobalSign Registration Authority a signed copy of an identification document such as an identity card, driver’s license or passport, or the applicant may authenticate the request through a proof of possession challenge-response.
3.3.1.3 PersonalSign 2 Pro and DocumentSign

Where a natural person’s identity is included within the certificate then if required, the applicant must submit to a GlobalSign Registration Authority a signed registration form and a signed subscriber agreement. When an Organization takes on the obligations of acting as a Local Registration Authority the Organization assumes the obligation of verifying identity. This obligation by the organization must be accepted if a role or department identity is to be included within the certificate.

For self-employed applicants who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional proof of identity in support of the verification of the applicant.

3.3.1.4 PersonalSign 3

In all cases, the applicant must submit to a GlobalSign Registration Authority in person a signed registration form, a signed subscriber agreement and a copy of identity proof.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant’s identity.

3.3.1.5 PersonalSign 3 Pro

In all cases, the applicant must submit to a GlobalSign Registration Authority in person a signed registration form, a signed subscriber agreement and the articles of association or proof of professional context and a copy of identity proof.

For an employee it is required to submit the articles of association of its employer and confirmation by a legal representative of such organization.

For a self-employed person that works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For self-employed persons belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional identification proof in support of the verification of the applicant.

3.3.1.6 OrganizationSSL

The applicant must either submit or apply to a GlobalSign Registration Authority via a signed registration form and a signed Subscriber Agreement or via a web based registration and application process encompassing applicable click through agreements as appropriate.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant’s identity.

3.3.1.7 DomainSSL

The applicant must submit or apply to a GlobalSign Registration Authority via a signed registration form and a signed Subscriber Agreement with the articles of association of the applying organization or via a web based registration and application process encompassing applicable click through agreements as appropriate.
GlobalSign may prescribe additional identification proof in support of the verification of the applicant ownership or right to use of the domain.

3.3.1.8 ExtendedSSL

The applicant (the Certificate Requester) must submit to a GlobalSign Registration Authority a registration form and a subscriber agreement, approved by the Certificate Approver and signed by the Certificate Signer to in accordance with the EV guidelines which are incorporated by reference herein.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant’s identity according to the EV Guidelines.

3.3.1.9 Educational ServerSign

The applicant must submit to GlobalSign Registration Authority a registration form and a Subscriber Agreement, both accepted and agreed to through a click-through acceptance process.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant’s identity.

3.3.1.10 Code Signing

The applicant must either submit or apply to a GlobalSign Registration Authority via a signed registration form and a signed Subscriber Agreement or via a web based registration and application process encompassing applicable click through agreements as appropriate.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant’s identity.

3.3.1.11 GlobalSign Timestamping

The applicant must either submit or apply to a GlobalSign Registration Authority via a signed registration form and a signed Subscriber Agreement or via a web based registration and application process encompassing applicable click through agreements as appropriate.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant’s identity.

3.3.2 Data needed for subscriber registration

Where the applicant is a natural person evidence shall be provided of the following data prior to accepting an application for a certificate:
- Full name (including last name and given names).
- A nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

Where the applicant is a person who is identified in association with an organizational entity, proof will be produced in terms of:
- Full name (including last name and given names) of the subscriber.
- Attributes of the subscriber may be used as far as possible, to distinguish the person from others with the same name.
- Full name and legal status of the associated legal or organizational entity.
- Any relevant existing registration information (e.g. company registration) of the associated legal or organizational entity.

Where the applicant is an organization, proof will be produced in terms of:
- Full name and legal status of the associated legal or organizational entity.
- Company registration number, VAT number or other attributes of the applicant which may be used to, as far as possible, distinguish it from others with a similar same name.
• Any relevant existing registration information (e.g. company registration) of the associated legal or organizational entity.

GlobalSign neither recommends nor encourages any specific choice of an end user product. Applicants and subscribers are entirely responsible to make the appropriate requests for the issuance of their certificates. Should support in identifying the features of each option be deemed necessary in order to make an informed selection, applicants are prompted to contact GlobalSign at: legal@globalsign.com

3.3.3 Pseudonyms

GlobalSign may conditionally accept the use of pseudonyms in its certificates. GlobalSign reserves its right to refuse granting a pseudonym certificate following a reasonably justified application assessment. Reasons for rejecting a pseudonym application include but are not limited to a pseudonym being:
- Already in use
- Violating third party rights
- Constituting slander etc.

3.3.3.1 Role or Department

For certain types of products GlobalSign may allow the use of a ‘role’ or ‘department’ names, reserving its right to disclose the identity of the organization’s registration authority as may be required by law or a following a reasoned and legitimate request. GlobalSign reserves its right to refuse granting a role or department certificate following a reasonably justified application assessment. Reasons for rejecting a role application include but are not limited to a role:
- Violating third party rights
- Constituting slander etc.

GlobalSign maintains documented records of a pseudonym and role based applications and application rejections.

Notice is hereby given that GlobalSign may disclose the real identity of the pseudonym certificate holder to any party, which can demonstrate a justified and legitimate interest to it.

The subscriber provides a physical address, or other attributes, which describe how the subscriber may be contacted.

GlobalSign reserves its right to insert names with pseudonyms in its certificates on a case-by-case basis. GlobalSign might make such designations in guidance documentation supplied to its RAs.

3.3.4 Records for subscriber registration

GlobalSign records all information used to verify the subscriber identity, including any reference number on the documentation used for verification, and any limitations on the validity thereof.

GlobalSign maintains records of the executed subscriber agreement and any material or documents that support the application which also include but are not limited to:
- GlobalSign subscriber agreement as approved of, and executed by, the applicant.
- Consent to the keeping of a record by GlobalSign of information used in registration and any subsequent certificate status change and passing of this information to third parties under the same conditions as required by this CPS in the case of the CA terminating its services.
- That information held in the certificate is correct and accurate.
- Full name of the subscriber.
- A nationally recognized identity number, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name.
- A specifically designed attribute that uniquely identifies the applicant within the context of the GlobalSign CA.
- Proof of organization context where necessary.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Any evidence produced in support of an application with a pseudonym.
- In the case of a role based certificate the applicant’s organization must submit to a GlobalSign RA acceptance of Local Registration Authority responsibilities.

The records identified above shall be kept for a period of no less than 5 years following the expiration of a certificate. A GlobalSign RA maintains such records. For organizational purposes a GlobalSign LRA may also maintain duplicates of these records for a shorter period of time.

### 3.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests of its subject types (CA, RA, subscriber, and other participants) GlobalSign requires using an online authentication mechanism (e.g. digital certificate authentication, PIN etc.) and a request addressed to the GlobalSign CA or an RA.
4.0 Certificate Life-Cycle Operational Requirements

Unless otherwise provided in this CPS in connection with the EV guidelines (ExtendedSSL certificates), the following operational requirements apply to Certificate Life-Cycle.

All entities within the GlobalSign domain including the RAs and subscribers or other participants have a continuous duty to inform the GlobalSign CA of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or gets revoked.

The GlobalSign CA issues or revokes certificates following an authenticated and duly signed request issued by a GlobalSign RA.

To carry out its tasks GlobalSign may use third party agents. GlobalSign assumes full responsibility and accountability for all acts or omissions of all third party agents it may use to deliver services associated with CA operations within the GlobalSign CA.

4.1 Certificate Application

A GlobalSign RA has the duty to provide the GlobalSign CA with accurate information on certificate requests it lodges on behalf of the end user applicants.

The GlobalSign CA acts upon request of an RA that has the authority to make a request to issue a certificate.

Subscribers undergo an enrollment process that requires:

- Filling out an application form.
- Generating a key pair, directly or through an agent which could be GlobalSign itself, of minimum key length 1024 bits. (2048 bits after 31st December 2010)
- Delivering the generated public key corresponding to a private key to GlobalSign CA.
- Accepting the subscriber agreement.

In case of a subject that can be distinguished from a subscriber, then the above listed requirements, are met by the subject; else, the subject’s designated applicant meets them. The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the GlobalSign CA. The subscriber agreement incorporates by reference this CPS.

In general, an online enrollment process will be sufficient, only as explicitly permitted by GlobalSign.
In all other cases (including EV certificates) credentials are requested, as appropriate, in a way that the exact identity of the applicant can reasonably be established. This includes a manually signed copy of the subscriber agreement, and a copy of identity card, or physical appearance before the RA.

4.2 Certificate Application Processing

A GlobalSign RA acts upon a certificate application to validate an applicant’s identity. Subsequently, an RA either approves or rejects a certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

The RA acts upon a certificate application to validate an applicant’s identity as foreseen in a documented procedure.

Pursuant to a certificate application the RA either approves or rejects a certificate application. If the application is approved the RA transmits the registration data to GlobalSign.

For rejected applications of certificate requests, the RA notes the reason for rejecting the application.
4.3 Certificate Issuance

The GlobalSign RA subsequently sends a certificate issuance request to the GlobalSign CA. Requests from the RA are granted approval provided that they are validly made and they contain valid subscriber data, formatted according the GlobalSign CA specifications.

The GlobalSign CA verifies the identity of the GlobalSign RA on the basis of credentials presented (a special RA administrator certificate). The GlobalSign CA retains its right to reject the application, or any applicant for RA certificates.

Following issuance of the certificate, the GlobalSign CA delivers the issued certificate to the subscriber directly or through an agent.

4.4 Certificate generation

With reference to the issuance and renewal of certificates GlobalSign represents towards all parties that certificates are issued securely according to the conditions set below:

- The procedure to issue a certificate is securely linked to the associated registration, including the provision of any subscriber generated public key.
- The confidentiality and integrity of registration data is ensured at all times through appropriate SSL (Secure Socket layer) links, especially when the applicant carries out CA/RA communications.
- The authentication of registrars is ensured through appropriate credentials issued to them.
- Certificate requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.
- GlobalSign verifies that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are ever used.
- GlobalSign accepts independent audits of its services and practices.

4.5 Certificate Acceptance

An issued GlobalSign CA certificate is deemed accepted by the subscriber when the RA confirms the acceptance of a certificate the CA issues.

Any objection to accepting an issued certificate must explicitly be notified to the GlobalSign CA. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

The GlobalSign CA might post the issued certificate on a repository (X.500 or LDAP). The GlobalSign CA also reserves its right to notify the certificate issuance by the GlobalSign CA to other entities.

4.6 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

4.6.1 Subscriber

The obligations of the subscriber include the following ones:

4.6.1.1 Subscriber duties

Unless otherwise stated in this CPS, the duties of subscribers include the following:
1. Accepting all applicable terms and conditions in the CPS of GlobalSign published in the
GlobalSign Repository.
2. Notifying the GlobalSign CA or a GlobalSign RA of any changes in the information
submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a GlobalSign certificate when it becomes invalid.
4. Using a GlobalSign certificate, as it may be reasonable under the circumstances.
5. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use
of their private key or of the strong password used to protect the private key in a scenario
where GlobalSign is required to generate the key.
6. Using secure devices and products that provide appropriate protection to their keys.
7. For any acts and omissions of partners and agents subscribers use to generate, retain,
   escrow, or destroy any private keys.
8. Refraining from submitting to GlobalSign or any GlobalSign directory any material that
   contains statements that violate any law or the rights of any party.
9. Request the revocation of a certificate in case of an occurrence that materially affects the
   integrity of a GlobalSign CA certificate.
10. Refraining from tampering with a certificate.
11. Only using certificates for legal and authorised purposes in accordance with the CPS.
12. Refrain from using a certificate outside possible license restrictions imposed by
    GlobalSign.

The Subscriber has all above stated duties towards the CA at all times. When the subscriber
applies on behalf of a different named Subject certain duties can be mitigated to the Subject,
which in return shall have to inform the Subscriber of any eventualities affecting the life cycle of a
certificate. In such case of mitigation, duties 2, 3, 4, 5, 6, 8, 9 10, 11 above apply to the Subject
and not to the Subscriber.

4.6.1.1 Certificate Life-Cycle Operational Requirements

Subscribers are hereby notified of their continuous duty to inform directly a GlobalSign RA of any
and all changes in the information featured in a certificate during the validity period of such
certificate or of any other fact that materially affects the validity of a certificate. This duty can be
exercised either directly by the subscriber or through an agent.

GlobalSign issues or revokes certificates only at the request of the RA following a successful
application of a certificate applicant.

4.6.1.2 Subscriber Duty Towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CPS, subscribers have a
duty to refrain from any misrepresentations they make in certificates to third parties that
reasonably rely on the representations contained therein.

4.6.1.3 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign CA
repositories and web site to assess and rely on information featured therein. Parties acknowledge
that they have received adequate information to decide whether to rely upon any information
provided in a certificate. The GlobalSign CA takes steps necessary to update its records and
directories concerning the status of the certificates and issue warnings about. Failure to comply
with the conditions of usage of the GlobalSign CA Repositories and web site may result in
terminating the relationship between the GlobalSign CA and the party.

4.6.2 Relying party

The duties of a relying party are as follows:

4.6.2.1 Relying party duties

A party relying on a GlobalSign certificate will:
GlobalSign Certification Practice Statement

- Receive notice of the GlobalSign CA and associated conditions for relying parties.
- Validate a GlobalSign certificate by using certificate status information (e.g. a CRL or OCSP) published by GlobalSign, in accordance with the certificate path validation procedure and validate at least those certificate attributes that materially affect the relying party's own signature policy if available.
- Trust a GlobalSign CA certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a GlobalSign certificate, only as it may be reasonable under the circumstances.
- Trust a certificate only if it has not been revoked.
- Validate at least those certificate attributes that materially affect the relying party's own signature policy or practices.

4.6.2.2 GlobalSign CA Repository and Web site Conditions

Parties, including subscribers and relying parties, accessing the GlobalSign CA Repository and web site agree with the provisions of this CPS and any other conditions of use that the GlobalSign CA may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided:
- Obtaining information as a result of the search for a digital certificate.
- Verifying the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Validating the status of a digital certificate before encrypting data using the public key included in a certificate.
- Obtaining information published on the GlobalSign CA web site.

4.7 Certificate Renewal

Subscribers may request the renewal of GlobalSign certificates. To request the renewal of a GlobalSign certificate, an end user lodges an online request.

Requirements for renewal of certificates, where available, may vary from those originally required for subscribing to the service.

Before renewing an ExtendedSSL certificate, GlobalSign must perform all authentication and verification tasks required by the EV Guidelines to ensure that the renewal request is properly authorized by the Applicant and that the information displayed in the ExtendedSSL certificate is still accurate and valid.

4.8 Certificate Revocation

GlobalSign shall use reasonable efforts to publish clear guidelines for revoking certificates, and maintain a 24/7 ability to accept and respond to revocation requests.

The identification of the subscriber who applies for a revocation of a certificate is carried out according to an internal documented procedure. This procedure is subject to auditing by authorised parties in compliance with the requirements set by accreditation schemes.

Subject to prior agreement with GlobalSign any GlobalSign RA may carry out the identification and authentication of holders seeking to revoke a certificate. To this effect an authenticated request is needed to initiate the procedure. The requesting party will have to be authenticated as the subscriber of that certificate or at least as an authorised agent of the subscriber of the certificate.
An RA might further challenge the requesting party until its identity is sufficiently established and distinguished from others.

Revocation requests can also be placed directly to the GlobalSign RA at:
GlobalSign nv/sa, Philippsite 5, 3001, Leuven, Belgium or ra@globalsign.com.

### 4.8.1 Circumstances for Revocation

Upon request from an RA, the GlobalSign CA revokes a digital certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate’s subject.
- The certificate’s subject or their appointed subscriber has breached a material obligation under this CPS.
- The performance of a person’s obligations under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate’s subject.
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- The information within the Certificate, other than non-verified Subscriber Information, is incorrect or has changed, or
- The continued use of that certificate is harmful to the GlobalSign Trust model.

When considering whether certificate usage is harmful to GlobalSign, GlobalSign considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

The GlobalSign RA requests the revocation of a certificate promptly upon verifying the identity of the requesting party. Verification of the identity can be done through information elements featured in the identification data that the subscriber has submitted to the GlobalSign RA. Upon request by a GlobalSign RA, the GlobalSign CA takes prompt action to revoke the certificate.

In addition to any revocation circumstances above, GlobalSign will revoke a Certificate it has issued upon the occurrence of any of the following events:

- The Subscriber requests revocation of its Certificate;
- The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
- GlobalSign obtains reasonable evidence that the Subscriber’s Private Key (corresponding to the Public Key in the Certificate) has been compromised, or that the Certificate has otherwise been misused;
- GlobalSign receives notice or otherwise becomes aware that a Subscriber uses the certificate for criminal activities such as phishing attacks, fraud, etc.
- GlobalSign receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
- GlobalSign receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber’s right to use the domain name listed in the Certificate, or that the Subscriber has failed to renew its domain name;
- GlobalSign receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
A determination, in GlobalSign’s sole discretion, that the Certificate was not issued in accordance with the terms and conditions of the Extended Validation Guidelines or GlobalSign’s Policies;

If GlobalSign determines that any of the information appearing in the Certificate is not accurate.

GlobalSign ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;

GlobalSign’s right to issue EV Certificates under the Extended Validation Guidelines expires or is revoked or terminated [unless GlobalSign makes arrangements to continue maintaining the CRL/OCSP Repository];

GlobalSign’s Private Key for its issuing CA Certificate has been compromised;

GlobalSign receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of GlobalSign’s jurisdiction of operation.

Following revocation the GlobalSign RA will send an acknowledgement e-mail to the requesting party.

4.8.2 Term and Termination of Revocation

The GlobalSign CA publishes notices of revoked certificates in the GlobalSign CA repository. The GlobalSign CA may publish its revoked certificates in its CRL and additionally, by any other means as it sees fit.

4.9 Certificate Status Services

The GlobalSign CA makes available certificate status checking services including CRLs, and appropriate Web interfaces.

4.9.1 CRL

A CRL lists all revoked certificates during the application period. CRLs for the different products are available from [http://crl.globalsign.com](http://crl.globalsign.com).

A CRL is issued each 3 hours.

4.10 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

4.11 Certificates Problem Reporting and Response Capability

In addition to certificate revocation, GlobalSign provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with clear instructions for reporting complaints or suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to certificates. GlobalSign shall use reasonable efforts to provide a 24x7 capability to accept and acknowledge and respond to such reports.

4.12 Certificate Expiry

Subscribers obtaining certificates directly from the GlobalSign RA will be pre-warned of the pending expiry date of the certificate by e-mail. In general two periods (30 days before and 7 days before) are deemed most effective, however this may vary per product type depending on whether previous authentication information can be utilised in a renewal process.
5.0 Management, Operational, And Physical Controls

This section describes non-technical security controls used by GlobalSign CA to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

Unless otherwise provided in this CPS in connection with the EV guidelines (ExtendedSSL certificates), the following requirements apply to management, operational, and physical controls:

5.1 Physical Security Controls

The GlobalSign CA implements physical controls on its own, leased or rented premises.

The GlobalSign CA infrastructure is logically separated from any other certificate management infrastructure, used for other purposes.

The GlobalSign CA secure premises are located in an area appropriate for high-security operations.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

The GlobalSign CA implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The GlobalSign CA implements a partial off-site backup.

The sites of the GlobalSign CA host the infrastructure to provide the GlobalSign CA services. The GlobalSign CA sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list, which is subject to audit.

5.2 Procedural Controls

The GlobalSign CA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The GlobalSign CA obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

The GlobalSign CA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.
Where dual control is required at least two trusted members of the GlobalSign CA staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

The GlobalSign CA ensures that all actions with respect to the GlobalSign CA can be attributed to the system and the person of the CA that has performed the action.

The GlobalSign CA implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances
The GlobalSign CA Partners perform checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks are specifically directed towards. Background checks include:
- Search of criminal record
- Check of professional references
- Confirmation of previous employment
- Confirmation of the most relevant educational degree obtained
- Misrepresentations by the candidate.
- Any other as it might be deemed necessary.

5.3.2 Background Checks and Clearance Procedures
The GlobalSign CA makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third-party statements or self-declarations.

5.3.3 Training Requirements and Procedures
The GlobalSign CA makes available training for their personnel to carry out CA and RA functions.

5.3.4 Retraining Period and Retraining Procedures
Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job Rotation
Not applicable.

5.3.6 Sanctions against Personnel
GlobalSign CA sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

5.3.7 Controls of independent contractors
Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as GlobalSign CA personnel.

5.3.8 Documentation for initial training and retraining
The GlobalSign CA, and RAs make available documentation to personnel, during initial training, retraining, or otherwise.
5.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment.

GlobalSign CA implements the following controls:

GlobalSign CA audit records events that include but are not limited to:
- Issuance of a certificate
- Revocation of a certificate
- Publishing of a CRL

Audit trail records contain:
- The identification of the operation
- The data and time of the operation
- The identification of the certificate, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation.

Documents that are required for audits include:
- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

GlobalSign CA ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of GlobalSign CA, the RA and designated auditors. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up and must be available to independent auditors upon request.

Auditing events are not given log notice.

5.5 Records Archival

GlobalSign CA keeps archives in a retrievable format.

GlobalSign CA ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of GlobalSign CA and the RA as appropriate.

The GlobalSign CA keeps internal records of the following items:
- All certificates for a period of a minimum of 1 year after the expiration of the certificate.
- Audit trails on the issuance of certificates for a period of a minimum of 1 year after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of a minimum of 1 year following the revocation of a certificate.
- CRLs for a minimum of 1 year after expiration or revocation of a certificate.
- Support documents on the issuance of certificates for a period of 5 years after expiration of a certificate. Support documents can be electronically stored.

GlobalSign maintains records for a period of 5 years for the following products:
- PersonalSign 2
GlobalSign maintains records for a period of 7 years for the following products:

- ExtendedSSL

As regards to ExtendedSSL, GlobalSign records in detail every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records must be available as auditable proof of the CA’s practices. The foregoing also applies to all registration authorities (RAs) and subcontractors as well.

5.5.1 Types of records

GlobalSign CA retains in a trustworthy manner records of GlobalSign CA digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

5.5.2 Retention period

GlobalSign CA retains in a trustworthy manner records of certificates for at least 1 year.

5.5.3 Protection of archive

Conditions for the protection of archives include:

- Only the records administrator (member of staff assigned with the records retention duty) may view the archive:
  - Protection against modification of archive, such as storing the data on a write once medium.
  - Protection against deletion of archive.
  - Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

5.5.4 Archive Collection

The GlobalSign CA archive collection system is internal.

5.5.5 Procedures to obtain and verify archive information

To obtain and verify archive information GlobalSign CA maintains records under clear hierarchical control.

The GlobalSign CA retains records in electronic or in paper-based format. The GlobalSign CA may require RAs, subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic or in paper-based format or any other format that the GlobalSign CA may see fit.

The GlobalSign CA may revise record retention terms as it might be required in order to comply with accreditation schemes including WebTrust for CAs, and the CA/browser forum EV Guidelines.
5.6 Compromise and Disaster Recovery

In a separate internal document, the GlobalSign CA documents applicable incident, compromise reporting and handling procedures. The GlobalSign CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

The GlobalSign CA establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

A business continuity plan has been implemented to ensure business continuity following a natural or other disaster.

As to the products issued under the EV guidelines, GlobalSign undertakes to develop, implement, and maintain a comprehensive Security Program reasonably designed to protect the confidentiality, integrity, and availability of the EV Data and EV Processes and comply with other security requirements applicable to the CA by law.

GlobalSign maintains a comprehensive Security Program based on a risk assessment document whereby the CA develops, implements, and maintains a Security Plan. The plan consists of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified. The Risk Assessment is commensurate with the sensitivity of the EV Data and EV Processes, as well as the complexity and scope of the activities of the CA. Such Security Plan shall include administrative, organizational, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the CA’s business and the EV Data and EV Processes. Such Security Plan shall also take into account then-available technology and the cost of implementing the specific measures, and must implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

CA or RA Termination

Before terminating its CA activities, the GlobalSign CA will take steps to transfer to a designated organization the following information at the GlobalSign CA’s own costs:

All information, data, documents, repositories, archives and audit trails pertaining to the GlobalSign CA.
6.0 Technical Security Controls

This section sets out the security measures taken by the GlobalSign CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This section also describes the security controls observed by the GlobalSign RA system when an applicant requests the GlobalSign RA system to generate a PKI key-pair and CSR.

6.1 Key Pair Generation and Installation

The GlobalSign CA protects its private key(s) in accordance with this CPS. The GlobalSign CA uses private signing keys only for signing CRLs, and OCSP responses in accordance with the intended use of each of these keys.

The GlobalSign CA will refrain from using its private keys used within the GlobalSign CA in any way outside the scope of GlobalSign CA.

6.1.1 GlobalSign CA Private Key Generation Process

The GlobalSign CA uses a trustworthy process for the generation of its root private key according to a documented procedure. The GlobalSign CA distributes the secret shares of its private key(s).

6.1.1.1 GlobalSign CA Private Key Usage

The private keys of the GlobalSign CA are used to sign GlobalSign CA issued certificates, GlobalSign CA certification revocation lists and OCSP responses. Other usages are restricted.

6.1.1.2 GlobalSign CA Private Key Type

For the CA Root key it uses, the GlobalSign CA makes use of the RSA algorithm with a key length of 2048 bits and a validity period of at least 14 years. GlobalSign may choose to re-key any or all of its public root certificates in order to effectively manage the certificate lifecycle needs of its subscribers and their relying parties. Any re-keying activity will simply extend the validity period of the public root certificate whilst preserving all other attributes. Re-keying procedures will comply with the same security principles as the creation of the original Root CA.

For the operational CA keys it uses the GlobalSign CA makes use of the RSA algorithm with a key length of 2048 bits and a validity period of up to 10 years.

6.1.2 GlobalSign CA Key Generation

The GlobalSign CA securely generates and protects its own private keys, using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of them. The GlobalSign CA implements and documents key generation procedures, in line with this CPS.

The GlobalSign key generation is carried out using an algorithm recognized as being fit for the purposes of certificates. GlobalSign uses RSA SHA-1 and RSA SHA-256.

The selected key length and algorithm for CA signing key is recognized as being fit for the purposes of certificates as issued by the CA.

6.1.3 GlobalSign Key Generation Audit (EV Guidelines)

For root keys generated after the release of EV Guidelines, GlobalSign Qualified Auditor witness the root key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of the CA root keys produced. The Qualified Auditor then issues a report opining that the CA, during its root key and certificate generation process:
- Documented its Root CA key generation and protection procedures in its Certificate Policy, version, date and its Certification Practices Statement, version, date (CP and CPS);
- Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the "Root Key Generation Script") for the Root CA;
- Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script; and
- Performed, during the root key generation process, all the procedures required by its Root Key Generation Script.
- A video of the entire key generation ceremony may be recorded for auditing purposes.

### 6.2 Key Pair re-generation and re-installation

The GlobalSign CA decommissions and destroys keys used in the past as well as the active tamper-resistant devices and all backup or escrowed copies of its private keys.

#### 6.2.1 GlobalSign CA Key Generation Devices

The generation of the private keys of the GlobalSign CA occurs within a secure FIPS 140-1 Level 3 or higher cryptographic device.

#### 6.2.1.1 GlobalSign CA Key Generation Controls

The generation of the private key of the GlobalSign CA requires the control of more than one appropriately authorised member of staff serving in trustworthy positions. This action entails dual control.

#### 6.2.2 GlobalSign CA Private Key Storage

The GlobalSign CA uses a secure cryptographic device to store its private keys meeting the appropriate requirements of FIPS 140-1 level 3.

When outside the signature-creation device the GlobalSign private signing key for a certificate is encrypted at all times.

#### 6.2.2.1 GlobalSign CA Key Storage Controls

The storage of the private key of the GlobalSign CA requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

#### 6.2.2.2 GlobalSign CA Key Back Up

The GlobalSign CA’s private keys are backed up, stored and recovered by multiple and appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

#### 6.2.2.3 Secret Sharing

The GlobalSign CA secret shares use multiple authorised holders, to safeguard and improve the trustworthiness of private keys and provide for key recovery. The GlobalSign CA stores its own private keys in several tamper-resistant devices. This action entails dual control.
6.2.2.4 Acceptance of Secret Shares

A secret shareholder receives the secret share within a physical medium, such as a GlobalSign CA approved hardware cryptographic module.

6.2.3 GlobalSign CA Public Key Distribution

Public key distribution of GlobalSign’s own public key takes place according to GlobalSign’s own practices.

6.2.4 GlobalSign CA Private Key Destruction

GlobalSign CA private keys are destroyed by at least two trusted operatives present at the end of their lifetime in order to guarantee that they cannot ever be retrieved and used again.

Key destruction process is documented and associated records are archived.

6.3 Private Key Protection and Cryptographic Module Engineering Controls

The GlobalSign CA uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs). Such devices meet formal requirements such as FIPS 140-1 Level 3 or higher, which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted.

Hardware and software mechanisms that protect CA private keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting.

GlobalSign CA custodians are assigned with the task to activate and deactivate the private key. The key is then active for a defined time period.

The GlobalSign CA private keys can be destroyed at the end of their lifetimes.

6.4 Other Aspects of Key Pair Management

The GlobalSign CA archives its own public keys. The GlobalSign CA issues subscriber certificates with usage periods as indicated on such certificates.

6.4.1 Computing resources, software, and/or data are corrupted

The GlobalSign CA establishes the necessary measures to ensure full recovery of the service in case of a disaster, corrupted servers, software or data.

If resources or services are not retained under the control of the GlobalSign CA, the CA ensures that any agreement with the resource owner or services provider is compliant with the requirements for disaster recovery.

6.4.2 CA public key revocation

If a GlobalSign CA public key is revoked the GlobalSign CA will immediately:

Notify all CAs with which it is cross-certified.
6.4.3 CA private key is compromised
If the private key of the GlobalSign CA is compromised, the corresponding certificate will immediately be revoked. Additional measures will be taken including the revocation of all end user certificates.

6.5 Activation Data
The GlobalSign CA securely stores and archives activation data associated with its own private key and operations.

6.6 Computer Security Controls
The GlobalSign CA implements computer security controls.

6.7 Life Cycle Security Controls
The GlobalSign CA performs periodic development controls and security management controls.

6.8 Network Security Controls
The GlobalSign CA maintains a high-level network of systems security including firewalls. Network intrusions are detected. In specific:
- The GlobalSign CA encrypts connections to the RA, using dedicated administrative certificates.
- The GlobalSign CA website provides certificate based Secure Socket Layer connections and anti-virus protection.
- The GlobalSign CA network is protected by a managed firewall and intrusion detection system.
- Accessing GlobalSign CA databases from outside the CAs network is prohibited.
- Internet sessions for request and delivery of information are encrypted.

6.9 Time-stamping Services
GlobalSign may provide time-stamping services for use with specific GlobalSign products such as Code Signing. In this case GlobalSign will be specifically mentioned within the subject DN of the certificate for these services. As such the details of the acceptable use policy for these services and any limitations will be provided in the subscriber agreement and/or the appropriate marketing documentation.

6.10 Key Pair and CSR Generation by Globalsign.
GlobalSign may accept a request for generation of a Key Pair and CSR on behalf of the Applicant. The products for which this service is appropriate are:-
- Server (SSL/TLS) based certificates
  - OrganizationSSL
  - DomainSSL
  - ExtendedSSL
- Personal/Organizational certificates
  - PersonalSign 2
  - PersonalSign 2 Pro
  - PersonalSign 3
  - PersonalSign 3 Pro
6.10.1 Server (SSL/TLS) based certificates

If the request is accepted by GlobalSign, then a PKI Key Pair and corresponding CSR will be generated by GlobalSign using a secure key generation process and in compliance with GlobalSign’s policy of minimum acceptable key length. GlobalSign will mandate the use of a strong password from the Applicant. In addition, GlobalSign will concatenate the Applicant’s password with a strong random string. The resulting concatenated password will be used to encrypt the final certificate package (containing the certificate and Private Key) for secure delivery to the Applicant following issuance of the certificate. The concatenated password will not be archived by GlobalSign and all instances will be destroyed following certificate delivery.

6.10.2 Personal/Organizational certificates

If the request is accepted by GlobalSign, then a PKI Key Pair and corresponding CSR will be generated by GlobalSign using a secure key generation process compliant with GlobalSign’s policy of minimum acceptable key length. In this case GlobalSign will mandate the use of a strong password from the Applicant. The password will be used to encrypt the final certificate package (containing the certificate and Private Key) for secure delivery to the Applicant following issuance of the certificate. The Registration Authority, which may be GlobalSign, will use PKI to archive the password on behalf of the individual.
7.0 Certificate and CRL Profiles

This section specifies Certificate, CRL, OCSP and Timestamping Profiles.

7.1 Certificate Profile


<table>
<thead>
<tr>
<th>Field</th>
<th>Value or Value constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Unique value per Issuer DN</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Object identifier of the algorithm used to sign the certificate – sha1RSA - in accordance with RFC 3279.</td>
</tr>
<tr>
<td>Issuer DN</td>
<td>GlobalSign together with the appropriate intermediate issuing CA appended to the description.</td>
</tr>
<tr>
<td>Valid From</td>
<td>Universal Coordinate Time base Synchronized to the Royal Observatory of Belgium. Encoded in accordance with RFC 5280.</td>
</tr>
<tr>
<td>Valid To</td>
<td>Universal Coordinate Time base Synchronized to the Royal Observatory of Belgium. Encoded in accordance with RFC 5280.</td>
</tr>
<tr>
<td>Subject DN</td>
<td>In accordance with 3.1</td>
</tr>
<tr>
<td>Subject Public Key</td>
<td>Encoded in accordance with RFC 5280</td>
</tr>
<tr>
<td>Signature</td>
<td>Generated and encoded in accordance with RFC 5280</td>
</tr>
</tbody>
</table>

7.1.1 Authority Key Identifier

GlobalSign generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

7.1.2 Authority Information Access

GlobalSign generally populates the Authority Information Access extension of X.509 Version 3 end user Subscriber Certificates and if appropriate Intermediate CA Certificates with the URL of the location where a Relying Party can obtain the issuing CA certificate. The criticality field of this extension is set to FALSE.

7.1.3 CRL Distribution Points

Most GlobalSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.4 Subject Key Identifier
Where GlobalSign populates X.509 Version 3 certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

### 7.1.5 Subject Alternative Name

Where GlobalSign populates X.509 Version 3 certificates with a subjectAlternativeName extension, the subjectAlternativeName is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

### 7.2 CRL Profile

Most GlobalSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate’s status. The criticality field of this extension is set to FALSE.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value or Value constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V2 in accordance with RFC 5280.</td>
</tr>
<tr>
<td>Issuer DN</td>
<td>The Entity who has signed and issued the CRL</td>
</tr>
<tr>
<td>Effective date</td>
<td>Issue date of the CRL. CRLs are effective upon issuance.</td>
</tr>
<tr>
<td>Next update</td>
<td>Date by which the next CRL will be issued.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Object identifier of the algorithm used to sign the certificate – sha1RSA - in accordance with RFC 3279.</td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>160-bit SHA-1 hash of the public key of the CA issuing the Certificate</td>
</tr>
<tr>
<td>CRL Number</td>
<td>A monotonically increasing sequence number in accordance with RFC 5280</td>
</tr>
<tr>
<td>This update</td>
<td>Issuance</td>
</tr>
<tr>
<td>Next Update</td>
<td>Date of Issuance + 3 hours</td>
</tr>
</tbody>
</table>

### 7.3 OCSP Profile

The GlobalSign CA maintains a record of the OCSP profile it might use in an independent technical document. This will be made available at the discretion of the GlobalSign CA, on request from parties explaining their interest.

### 7.4 Time Stamping Profile for Time Stamping Services

The GlobalSign CA maintains a record of the Time Stamping profile it might use in an independent technical document. This will be made available at the discretion of the GlobalSign CA, on request from parties explaining their interest.
8.0 Compliance Audit and Other Assessment

The GlobalSign CA accepts under condition the auditing of practices and procedures it does not publicly disclose. The GlobalSign CA gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content the GlobalSign CA accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS and accreditation schemes it publicly claims compliance with.

8.1 Compliance Audit and Other Assessment

GlobalSign has successfully been audited and currently meets the requirements of the accreditation scheme known as WebTrust for CAs and the WebTrust EV Program. GlobalSign seeks to maintain its accreditation.

GlobalSign shall also seek accreditation by Qualified Auditors and seek to maintain its accreditation under the WebTrust EV Program and WebTrust for CAs scheme on a recurrent basis.

Licensed to perform WebTrust for CA audits and WebTrust EV program Audits, Qualified Auditors must be AICPA members and have proficiency in examining PKI technology and related information security tools and techniques.

Information on GlobalSign’s conformance with the requirements of any other accreditation scheme can be sought by the organization of such accreditation scheme directly.

GlobalSign accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS. GlobalSign accepts this auditing of its own practices and procedures that it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by a party to which GlobalSign owes duty. The CA evaluates the results of such audits before further implementing them and make them publicly available.

During the period in which it issues ExtendedSSL certificates, GlobalSign strictly controls its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the said Certificates it has issued in the period beginning immediately after the last sample was taken.

8.1.1 Audit process conditions

To carry out the audits there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with GlobalSign nor having any conflicting interests thereof.

An audit is carried out in areas that include but are not limited to the following ones:

- Compliance of GlobalSign operating procedures and principles with the procedures and service levels defined in the CPS.
- Management of the infrastructure that implements CA services.
- Management of the physical site infrastructure.
- Adherence to the CPS.
- Adherence to relevant laws.
- Asserting agreed service levels.
- Inspection of audit trails, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

With regard to conformance audits, GlobalSign undertakes the responsibility of the performance of any subcontractors it uses to carry out certification operations including those described in the section below.
8.1.1.1 Business Partnerships

To better respond to the diverse certification needs of the distributed population of electronic commerce service providers and users, GlobalSign may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration. GlobalSign may outsource in part or whole certain aspects of the delivery of its services. Regardless of the partner or agent selected to manage certain parts of the certificate lifecycle or operations, GlobalSign remains ultimately in charge of the whole process. GlobalSign will ensure that compliance audits are also applied to such outsourced services. GlobalSign limits its responsibility thereof according to the conditions in this CPS and the GlobalSign CP.

8.1.1.2 Secure Devices and Private Key Protection.

GlobalSign supports the use of secure devices and tamperproof equipment to securely issue, manage and store certificates. GlobalSign uses accredited trustworthy hardware to prevent compromise of its private key.
9.0 Other Business and Legal Matters

Certain Legal conditions apply to the issuance of the GlobalSign CA certificates under this CPS as described in this section.

9.1 Fees

The issuance and management of GlobalSign CA certificates is subject to fees announced on the GlobalSign web site [www.globalsign.com](http://www.globalsign.com) or through requested quotes.

9.1.1 Refund policy

GlobalSign accepts requests for refund in writing. Refund requests must be duly justified and addressed to the Legal Services of GlobalSign. GlobalSign reserves its right to endorse or grant refunds unless they are requested in the framework of a warranty offered by GlobalSign.

9.2 Financial Responsibility

GlobalSign maintains sufficient resources to meet its perceived obligations under this CPS. The GlobalSign CA makes this service available on an “as is” basis. GlobalSign makes available a limited warranty plan published on [www.globalsign.com](http://www.globalsign.com).

9.3 Confidentiality of Business Information

The GlobalSign CA observes personal data privacy rules and confidentiality rules as described in the GlobalSign CPS. Confidential information includes:

- Any personal identifiable information on subscribers, other than that contained in a certificate.
- Reason for the revocation of a certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificate and their content.
- Status of a certificate.

GlobalSign does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the GlobalSign CA owes a duty to keep information confidential is the party requesting such information.
- A court order.

The GlobalSign may charge an administrative fee to process such disclosures.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

9.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- Only a single certificate is delivered per inquiry by subscriber or relying party.
- The status of a single certificate is provided per inquiry by a subscriber or relying party.
Subscribers can consult the information the CA holds about them.

Confidential information may not be disclosed to subscribers nor relying parties. The GlobalSign CA properly manages the disclosure of information to the CA personnel.

The GlobalSign CA authenticates itself to any party requesting the disclosure of information by:
Presenting an authentication certificate at the request of the subscriber or relying party
Signing responses to OCSP requests and CRLs.

The GlobalSign CA encrypts all communications of confidential information including:
The communications link between the CA and the RAs.
Sessions to deliver certificates and certificate status information.

To incorporate information by reference the GlobalSign CA uses computer-based and text-based pointers that include URLs, etc.

9.4 Privacy of Personal Information

The GlobalSign CA makes available a specific Data Protection Policy for the protection of personal data of the applicant applying for a GlobalSign CA certificate that they make available through their web site. The GlobalSign CA adheres to the documented Data Protection Policy of GlobalSign NV available from www.globalsign.com/repository.


The regulation on the protection of personal data in the Belgium implements the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The GlobalSign CA also acknowledges Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The GlobalSign CA operates within the conditions for the protection of personal data asserted in this CPS.

The GlobalSign CA has made appropriate representations before the Belgian Data Protection Commission with regard to the archives of personal data it maintains, collects and processes.

9.5 Intellectual Property Rights

The GlobalSign CA owns and reserves all intellectual property rights associated with its databases, web sites, GlobalSign CA digital certificates and any other publication whatsoever originating from GlobalSign CA including this CPS.

The Distinguished names of all CAs of the GlobalSign CA, remain the sole property of GlobalSign, which enforces these rights.

Certificates are and remain property of the GlobalSign CA. The GlobalSign CA permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of the GlobalSign CA. The scope of this restriction is also intended to protect subscribers against the unauthorised re-publication of their personal data featured on a certificate.
The GlobalSign CA owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

9.6 Representations and Warranties

Unless otherwise provided in this CPS in connection with the EV guidelines, the following rules apply as to Representations and Warranties.

The GlobalSign CA uses this CPS, associated CPs and a subscriber agreement to convey legal conditions of usage of GlobalSign CA certificates to subscribers and relying parties.

Participants that may make representations and warranties include GlobalSign CA, RAs, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the GlobalSign domain, including the GlobalSign CA, RAs and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify the appropriate RA.

9.6.1 Subscriber Obligations

- Unless otherwise stated in this CPS, subscribers are responsible for having knowledge and, if necessary, seeking training on using digital certificates.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with the GlobalSign CA.
- Ensuring that the public key submitted to the GlobalSign CA correctly corresponds to the private key used.
- Accepting all terms and conditions in the GlobalSign CA CPS and associated policies published in the GlobalSign CA Repository.
- Refraining from tampering with a GlobalSign CA certificate.
- Using GlobalSign CA certificates for legal and authorised purposes in accordance with this CPS.
- Notifying GlobalSign CA or a GlobalSign RA of any changes in the information submitted.
- Ceasing to use a GlobalSign CA certificate if any featured information becomes invalid.
- Ceasing to use a GlobalSign CA certificate when it becomes invalid.
- Removing a GlobalSign CA certificate when invalid from any applications and/or devices they have been installed on.
- Using a GlobalSign CA certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting to GlobalSign CA or any GlobalSign CA directory any material that contains statements that violate any law or the rights of any party.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a GlobalSign CA certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.

GlobalSign makes available a subscriber agreement in order to ensure that the subscriber is bound under the following terms:

- Submit accurate and complete information to GlobalSign in accordance with the requirements of this CPS particularly with regards to registration.
- Only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber according to this CPS.
- Exercise reasonable care to avoid unauthorized use of its private key.
Under the GlobalSign model the subscriber always generates its own keys, in which case the following terms also apply:

- Generate subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures;
- Use a key length and algorithm, which is recognized as being fit for the purposes of electronic signatures;
- Notify GlobalSign without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
  - The subscriber's private key has been lost, stolen, potentially compromised; or
  - Control over the subscriber's private key has been lost due compromise of activation data (e.g. PIN code);
- Inaccuracy or changes to the certificate content, as notified to the subscriber.

9.6.2 Relying Party Obligations

A party relying on a GlobalSign CA certificate promises to:

- Have the technical capability to use digital certificates.
- Receive notice of the GlobalSign CA and associated conditions for relying parties.
- Validate a GlobalSign CA certificate by using certificate status information (e.g. a CRL) published by the GlobalSign CA in accordance with the proper certificate path validation procedure.
- Trust a GlobalSign CA certificate only if all information featured on such certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a GlobalSign CA certificate, only as it may be reasonable under the circumstances.
- Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised.

The obligations of the relying party, if it is to reasonably rely on a certificate, are to:

- Verify the validity, revocation of the certificate using current revocation status information as indicated to the relying party.
- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or this CPS.
- Take any other precautions prescribed in the subscriber agreement, GlobalSign certificate as well as any other policies or terms and conditions made available in the application context a certificate might be used.

Relying parties must at all times establish that it is reasonable to rely on a certificate under the circumstances taking into account circumstances such as the specific application context a certificate is used in.

9.6.2.1 Conveying Relying party obligations

In order to give uninhibited access to revocation information and subsequently invoke Trust in its own services, GlobalSign refrains from implementing an agreement with the relying party with regard to controlling the validity of certificate services with the purpose of binding relying parties to their obligations.

Much like it applies to any other participant of GlobalSign public services, however, the use of GlobalSign resources that relying parties make is implied to be governed by the conditions set out in GlobalSign policy framework instigated by the GlobalSign CP and the GlobalSign CPS.

Relying parties are hereby notified that the conditions prevailing in this CPS are binding upon them each time they consult a GlobalSign resource for the purpose of establishing trust and validating a certificate.
9.6.3 Subscriber Liability towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CP, subscribers are liable for any misrepresentations they make in certificates to third parties that, reasonably rely on the representations contained therein.

9.6.4 GlobalSign CA Repository and Web site Conditions

Parties (including subscribers and relying parties) accessing the GlobalSign CA Repository and web site agree with the provisions of this CPS and any other conditions of usage that GlobalSign may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. The GlobalSign CA Repositories include or contain:

- Information provided as a result of the search for a digital certificate.
- Information to verify the status of digital signatures created with a private key corresponding to a public key listed in a certificate.
- Information to verify the status of a digital certificate before encrypting data using the public key included in a certificate.
- Information published on the GlobalSign CA web site.
- Any other services that GlobalSign CA might advertise or provide through its web site.

If a repository becomes aware of or suspects the compromise of a private key, it will immediately notify the appropriate RA. The party that operates a Repository has exclusive responsibility of all acts or omissions associated with it.

The GlobalSign CA maintains a certificate repository during the application period and for a maximum of ten years after the expiration or revocation of a certificate. To verify its integrity the complete repository will be made available to the GlobalSign RAs for queries at any time.

Additionally, the GlobalSign CA repository is available to relying parties.

9.6.4.1 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign CA Repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. The GlobalSign CA takes steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the GlobalSign Repositories and web site may result in terminating the relationship between the GlobalSign CA and the party.

9.6.4.2 Accuracy of Information

The GlobalSign CA makes every effort to ensure that parties accessing its repositories receive accurate, updated and correct information. The GlobalSign CA, however, cannot accept any liability beyond the limits set in this CPS and the GlobalSign CA insurance policy.

9.6.5 GlobalSign CA Obligations

To the extent specified in the relevant sections of the CP, the GlobalSign CA promises to:

- Comply with this CPS and its amendments as published under http://www.globalsign.com/repository
- Provide infrastructure and certification services, including the establishment and operation of the GlobalSign CA Repository and web site for the operation of public certificate management services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
• Provide and validate application procedures for the various types of certificates that it makes publicly available.
• Issue electronic certificates in accordance with this CPS and fulfil its obligations presented herein.
• Revoke certificates issued according to this CPS upon receipt of a valid and authenticated request to revoke a certificate from an RA.
• Publish accepted certificates in accordance with this CPS.
• Provide support to subscribers and relying parties as described in this CPS.
• Provide for the expiration and renewal of certificates according to this CPS.
• Publish CRLs and/or OCSP responses of all revoked certificates on a regular basis in accordance with this CPS.
• Provide appropriate service levels according to a service agreement.
• Notify relying parties of certificate revocation by publishing CRLs on the GlobalSign CA repository.

The liability of GlobalSign CA under the above stated article for proven damages is limited to 1 Euro for any individual certificate, directly caused by the occurrences listed above. This limit might be reviewed by GlobalSign. GlobalSign might seek additional insurance coverage against risks emanating from the correctness of the information included in a certificate.

To the extent permitted by law the GlobalSign CA cannot be held liable for:
• Any use of certificates, other than specified in this CPS.
• Falsification of transactions.
• Improper use or configuration of equipment, not operated under the responsibility of the CA, used in a transaction involving certificates.
• Compromise of private keys associated with the certificates.
• Loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates.
• The submission of erroneous or incomplete data from an RA, including identification data, serial numbers and public key values
• Erroneous or incomplete requests for operations on certificates by the RA.
• Acts of God.
• The use of certificates.
• The use of public or private keys of cross-certified (non-subordinate) CA’s and their relying parties.

The GlobalSign CA acknowledges it has no further obligations under this CPS.

9.6.6 Registration Authority Obligations

A GlobalSign RA operating within the GlobalSign network promises to:
• Generate securely an RA administrator key pair, using a trustworthy system directly or through an agent.
• Provide correct and accurate information in their communications with the GlobalSign CA.
• Ensure that the public key submitted to GlobalSign CA is the correct one (if applicable).
• Generating a new, secure key pair to be used in association with a certificate that they request from GlobalSign CA.
• Receive applications for the GlobalSign CA certificates in accordance with this GlobalSign CPS.
• Carry out all verification and authenticity actions prescribed by the GlobalSign CA procedures and this CPS.
• Submit to the GlobalSign CA the applicant’s request in a signed message (certificate request).
• Receive, verify and relay to the GlobalSign CA all requests for revocation of a GlobalSign CA certificate in accordance with the GlobalSign CA procedures and the GlobalSign CA CPS.
Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CPS.

9.6.7 Information incorporated by reference into a digital certificate

The GlobalSign incorporates by reference the following information in every digital certificate it issues:
- Terms and conditions of the GlobalSign CA CPS.
- Any other applicable certificate policy as may be stated on an issued GlobalSign certificate.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customised elements of the standard X.509.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

The GlobalSign also incorporates by reference the following information in every ExtendedSSL digital certificate it issues:
- The CA/Browser Forum Guidelines for Extended Validation Certificates.

9.6.8 Pointers to incorporate by reference

To incorporate information by reference GlobalSign uses computer-based and text-based pointers. GlobalSign may use URLs, OIDs etc.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

The GlobalSign CA does not warrant:
- The accuracy of any unverifiable piece of information contained in certificates except as it may be stated in the relevant product description below in this CPS (in particular, products issued under the Guidelines for Extended Validation Certificates) and in the GlobalSign CA warranty policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

9.7.2 Exclusion of Certain Elements of Damages

In no event (except for fraud or wilful misconduct) is the GlobalSign CA liable for:
- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CPS.
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on, free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

9.8 Limitations of Liability

The total liability of the GlobalSign is limited in accordance with the Limited Warranty Policy of GlobalSign.
Notice is hereby given that a certificate can only be relied upon for transactions involving a monetary value equal or lower than those published on the Limited Warranty Plan. Further information on the warranty conditions can be found at: www.globalsign.com/repository. An overview of the reliance limits is as follows:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Limit (EUR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PersonalSign 2 Certificates</td>
<td>2500</td>
</tr>
<tr>
<td>PersonalSign 2 Pro Certificates</td>
<td>2500</td>
</tr>
<tr>
<td>DocumentSign Certificates</td>
<td>2500</td>
</tr>
<tr>
<td>PersonalSign 3 Certificates</td>
<td>37,500</td>
</tr>
<tr>
<td>PersonalSign 3 Pro Certificates</td>
<td>37,500</td>
</tr>
<tr>
<td>OrganizationSSL Certificates</td>
<td>100,000</td>
</tr>
<tr>
<td>DomainSSL certificates</td>
<td>10,000</td>
</tr>
<tr>
<td>Code Signing Certificates</td>
<td>37,500</td>
</tr>
<tr>
<td>GlobalSign Timestamping Certificates</td>
<td>2500</td>
</tr>
<tr>
<td>Educational ServerSign Certificates</td>
<td>1</td>
</tr>
</tbody>
</table>

### 9.8.1 Limitations on ExtendedSSL Certificate Liability

1. **Subscribers and Relying Parties**

   In cases where GlobalSign has issued and managed ExtendedSSL certificates or any other product in compliance with the EV Guidelines, GlobalSign shall not be liable to the ExtendedSSL Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such certificate beyond those specified in the CA's EV Policies.

   In cases where GlobalSign has not issued or managed the Certificate in complete compliance with the EV Guidelines, GlobalSign will indemnify to the Subscriber and to Relying Parties for any cause of action or legal theory involved for any and all claims, losses or damages suffered as a result of the use or reliance on such ExtendedSSL certificate up to 250,000 EUR per loss, provided that all such purported limitations must also be specified in this CPS.

2. **Indemnification of Application Software Vendors**

   Notwithstanding any limitations on its liability to Subscribers and Relying Parties, GlobalSign acknowledges that the Application Software Vendors who has a root certificate distribution agreement in place do not assume any obligation or potential liability of GlobalSign under these Guidelines or that otherwise might exist because of the issuance or maintenance of Sure Server certificates or reliance thereon by Relying Parties or others.

   Thus, GlobalSign shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an ExtendedSSL Certificate, regardless of the cause of action or legal theory involved.

   This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an ExtendedSSL certificate issued by GlobalSign where such claim, damage, or loss was directly caused by such Application Software Vendor’s software displaying as not trustworthy an ExtendedSSL certificate this is still valid, or displaying as trustworthy: (1) an ExtendedSSL certificate that has expired, or (2) an ExtendedSSL certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the browser software either failed to check such status or ignored an indication of revoked status).

### 9.9 Indemnities

This section contains the applicable indemnities.

To the extent permitted by law the subscriber agrees to indemnify and hold the GlobalSign CA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and
expenses of any kind, including reasonable attorneys' fees that the GlobalSign may incur as a result of failure to:-

- Protect the subscriber's private key,
- Use a trustworthy system as required
- Taking precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber’s private key
- Attend to the integrity of the GlobalSign Root.

9.10 Term and Termination

This CPS remains in force until notice of the opposite is communicated by the GlobalSign CA on its web site or repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.11 Individual notices and communications with participants

The GlobalSign CA accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from GlobalSign CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individuals communications made to the GlobalSign CA must be addressed to legal@globalsign.com or by post to the GlobalSign in the address mentioned in the introduction of this document.

9.12 Amendments

Changes to this CPS are indicated by appropriate numbering.

9.13 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify GlobalSign of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, GlobalSign convenes a Dispute Committee that advises GlobalSign management on how to proceed with the dispute. The Dispute Committee convenes within twenty (20) business days from receipt of a Dispute Notice. The Dispute Committee is composed by a counsel, a data protection officer, a member of GlobalSign operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the Dispute Committee proposes a settlement to the GlobalSign executive management. The GlobalSign executive management may subsequently communicate the proposed settlement to the resting party.

9.13.1 Arbitration

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CPS, parties submit the dispute to arbitration, in accordance with art. 1676-1723 of the Belgian Judicial Code.

There will be 3 arbitrators of whom each party proposes one while both parties of the dispute choose the third arbitrator. The place of the arbitration is Leuven, Belgium and the arbitrators determine all associated costs.
For all technology related disputes and disputes related to this CPS the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:
J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
Tel.: +32-47-733 82 96, Fax: + 32-16-32 54 38.

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of GlobalSign digital certificates or other products and services. The law of Belgium apply also to all GlobalSign commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to GlobalSign products and services where the GlobalSign acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including GlobalSign partners, subscribers and relying parties, irrevocably submit to the jurisdiction of the district courts of Leuven, Belgium.

9.15 Compliance with Applicable Law

GlobalSign CA complies with applicable laws of Belgium. Export of certain types of software used in certain GlobalSign CA public certificate management products and services may require the approval of appropriate public or private authorities. Parties (including the GlobalSign CA, subscribers and relying parties) agree to conform to applicable export laws and regulations as pertaining in Belgium.

9.16 Miscellaneous Provisions

9.16.1 Survival

The obligations and restrictions contained under section “Legal Conditions” survive the termination of this CPS.

9.16.2 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS should be interpreted in such manner as to effect the original intention of the parties.

9.16.3 Other provisions

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CP/CPS applies to. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.
10.0 List of definitions

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework.

ACCREDITATION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.

APPLICATION FOR A CERTIFICATE
A request sent by a certificate applicant to a CA to issue a digital certificate.

APPLICATION PROGRAMMING INTERFACE (API)
An application programming interface (API) is a source code interface that an operating system or library provides to support requests for services to be made of it by computer programs.

APPLICATION SOFTWARE VENDOR:
A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.

APPROVED HARDWARE DEVICE:
Hardware devices that securely generate and store either a Certification Authority’s or a Subscriber’s key pair and certificate chain and perform signing, encryption and/or authentication. Both hardware security modules and tokens are forms of cryptographic hardware.

ASSURANCES
A set of statements or conduct aiming at conveying a general intention.

AUDIT
Procedure used to validate compliance with formal criteria or controls.

AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.

AUTHORISATION
Granting of rights.

AVAILABILITY
The rate of accessibility of information or resources.

HARDWARE MODULE
The complete system of the hardware module used to keep the certificates and securely generate a key pair.

BINDING
A statement by an RA of the relationship between a named entity and its public key.

CERTIFICATE
The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber’s ones.

CERTIFICATE REVOCATION LIST OR CRL
A list maintained by the CA of certificates that are revoked before their expiration time.

CERTIFICATION AUTHORITY OR CA
An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the GlobalSign CA.

CERTIFICATION PRACTICE STATEMENT OR CPS
A statement of the practices in the management of certificates during all life phases.

CERTIFICATE STATUS SERVICE OR CSS
A service, enabling relying parties and others to verify the status of certificates.

CONTRACT PERIOD
The duration of the GlobalSign CA contract between the Dutch National Register and the CA organization.

CERTIFICATE CHAIN
A hierarchical list certificates containing an end-user subscriber certificate and CA certificates.
certificate expiration
The end of the validity period of a digital certificate.

CERTIFICATE EXTENSION
A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.

CERTIFICATE HIERARCHY
A level-based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers.

CERTIFICATE MANAGEMENT
Actions associated with certificate management include storage, dissemination, publication, revocation of certificates.

CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked certificates. Such list is to me consulted by relying parties at all times prior to relying on information featured in a certificate.

CERTIFICATE SERIAL NUMBER
A sequential number that uniquely identifies a certificate within the domain of a CA.

CERTIFICATE SIGNING REQUEST (CSR)
A machine-readable application form to request a digital certificate.

CERTIFICATION
The process to issue a digital certificate.

CERTIFICATION AUTHORITY (CA)
An authority, such as the GlobalSign CA that issues or revokes a digital certificate.

CERTIFICATE POLICY (CP)
A statement of the practices of a CA and the conditions of issuance, revocation etc. of a certificate. A CP is also used as guidance to establish the trustworthiness of a certification services infrastructure.

CERTIFICATE ISSUANCE
Delivery of X.509 v3 digital certificates for authentication and digital signature based on personal data and public keys provided by the RA and compliant with RFC 3647 and RFC 3039

CERTIFICATE REVOCATION
Online service used to permanently disable a digital certificate before its expiration date

CERTIFICATE REVOCATION LISTS
Online publication of complete and incremental digital certificates revocation lists compliant with RFC 5280

COMMERCIAL REASONABLENESS
A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.

COMPROMISE
A violation of a security policy that results in loss of control over sensitive information.

CONFIDENTIALITY
The condition to disclose data to selected and authorized parties only.

CONFIRM A CERTIFICATE CHAIN
To validate a certificate chain in order to validate an end-user subscriber certificate.

DIGITAL CERTIFICATE
A formatted piece of data that relates an identified subject with a public key the subject uses.

DIGITAL SIGNATURE
To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.

DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context.

DIRECTORY SERVICE
Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier.

END-USER SUBSCRIBER
A subscriber other than another CA.

ENHANCED NAMING
The usage of an extended organization field (OU=) in an X.509 v.3.0 certificate.
An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels that contain the domain that was included in an original Valid EV Certificate issued to the Enterprise RA.

**Enterprise RA:** The Subject of a specified Valid EV Certificate that is authorized by the issuing CA to perform the RA function and authorize the CA to issue additional EV Certificates at third and higher domain levels that contain the domain that was included in the original EV Certificate, in accordance with the requirements of these Guidelines.

**Extensions**
Extension fields in X.509 v.3.0 certificates.

**Generate a Key Pair**
A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant’s capacity to use the private key.

**Government Entity**
A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

**Hash**
An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:
- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

**Identification**
The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.

**Incorporate by Reference**
To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

**Incorporating Agency**
In the case of a Private organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the Private organization was established (e.g., the government agency that issued the Certificate of Incorporation). In the case of a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.

**Jurisdiction of Incorporation**
In the case of a Private organization, the country and (where applicable) the state or province where the organization’s legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity’s legal existence was created by law.

**Key Generation Process**
The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process.

**Key Pair**
A private key and its corresponding public key in asymmetric encryption.

**Notice**
The result of notification to parties involved in receiving CA services in accordance with this CPS.

**Notify**
To communicate specific information to another person as required by this CPS and applicable law.

**Notarised Time Stamping**
Online service used to timestamp and securely archive a document; the document is re-timestamped on a regular basis with up-to-date technology.

**OBJECT IDENTIFIER**
A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

**PKI HIERARCHY**
A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.

**PLACE OF BUSINESS**
The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant’s business is conducted

**PRIVATE KEY**
A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.

**PUBLIC KEY**
A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.

**PUBLIC KEY CRYPTOGRAPHY**
Cryptography that uses a key pair of mathematically related cryptographic keys.

**PUBLIC KEY INFRASTRUCTURE (PKI)**
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

**QGIS (QUALIFIED GOVERNMENT INFORMATION SOURCE)**
A regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided they are maintained by a Government Entity

**QIIS (QUALIFIED INDEPENDENT INFORMATION SOURCES)**
A regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

**REGISTERED AGENT**
An individual or entity that is both:
- authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and
- listed in the official records of the Applicant’s Jurisdiction of Incorporation as acting in the role specified in (a) above.

**REGISTERED OFFICE**
The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and legal notices received.

**REGISTRATION NUMBER**
The unique number assigned to the Private organization Applicant or Subject entity by the Incorporating Agency in such entity’s Jurisdiction of Incorporation.

**REGISTRATION AUTHORITY or RA**
An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.

**RELATIVE DISTINGUISHED NAME (RDN)**
A set of attributes that distinguishes the entity from others of the same type.

**RELIANCE**
To accept a digital signature and act in a way that shows trust in it.

**RELYING PARTY**
Any entity that relies on a certificate for carrying out any action.

**REPOSITORY**
A database and/or directory listing digital certificates and other relevant information accessible on-line.

**REVOKE A CERTIFICATE**
To permanently end the operational period of a certificate from a specified time forward.

**SECRET SHARE**
A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.

**SECRET SHARE HOLDER**
An person that holds a secret share.

**SHORT MESSAGE SERVICE (SMS)**
A service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication.

**SIGNATURE**
A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.

**SIGNER**
A person who creates a digital signature for a message, or a signature for a document.

**SMART CARD**
A hardware token that contains a chip to implement among others cryptographic functions.

**STATUS VERIFICATION**
Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs

**SUBJECT OF A DIGITAL CERTIFICATE**
The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.

**SUBORDINATE CA**
Certification authority whose certificates are signed by the Root CA, or another Subordinate CA. A Subordinate CA may issue EV Certificates if the appropriate EV OID(s) or the special any Policy OID is specified in the certificatePolicies extension.

**SUBSCRIBER**
The subject of a digital certificate, or a party designated by the subject to apply for the certificate.

**SUBSCRIBER AGREEMENT**
The agreement between a subscriber and a CA for the provision of public certification services.

**TRUSTED POSITION**
A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, or revocation of certificates, including operations that restrict access to a repository.

**TRUSTWORTHY SYSTEM**
Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

**TPM**
Trusted Platform Module – A hardware cryptographic device which is defined by the Trusted Computing Group. [https://www.trustedcomputinggroup.org/specs/TPM](https://www.trustedcomputinggroup.org/specs/TPM)

**GLOBALSIGN CA REGISTRATION AUTHORITY**
An entity that verifies and provides all subscriber data to the GlobalSign CA.

**GLOBALSIGN CA PUBLIC CERTIFICATION SERVICES**
A digital certification system made available by GlobalSign CA as well as the entities that belong to the GlobalSign CA domain as described in this CPS.

**GLOBALSIGN CA PROCEDURES**
A document describing the GlobalSign CA’s internal procedures with regard to registration of end users, security etc.

**WEBTRUST EV PROGRAM**
The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.

**WEBTRUST PROGRAM FOR CAs**

**WEB -- WORLD WIDE WEB (WWW)**
A graphics based medium for the document publication and retrieval of information on the Internet.

**WRITING**
Information accessible and usable for reference.
X.509
The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.
11.0 List of acronyms

CA: Certification Authority
RA: Registration Authority
LRA: Local Registration Authority
CEN/ISSS: European Standardization Committee / Information Society Standardisation System
CP: Certificate Policy
CPS: Certification Practice Statement
ETSI: European Telecommunications Standards Institute
GSCA: GlobalSign Certification Authority
IETF: Internet Engineering Task Force
ISO: International Standards organization
ITU: International Telecommunications Union
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RFC: Request for Comments
SSCD: Secure Signature Creation Device
VAT: Value Added Tax
RFP 648260
GENERAL INFORMATION FORM

QUESTIONS: All inquiries for information regarding this solicitation should be directed to: Nancy Sterling, Sr. Contract Officer, Phone: (540) 231-9517, e-mail: nancy.sterling@vt.edu.

DUE DATE: Sealed Proposals will be received until April 16, 2010 at 3:00 PM. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

ADDRESS: Proposals should be mailed or hand delivered to Virginia Polytechnic Institute and State University (Virginia Tech) at: Virginia Tech, Attn: Nancy Sterling, IT Acquisitions Office (0214), 1700 Pratt Drive, Blacksburg, Virginia 24061 Reference the Opening Date and Hour, and RFP Number in the lower left corner of the return envelope or package.

TYPE OF BUSINESS: (Please check all applicable classifications). If your classification is certified by the Virginia Department of Minority Business Enterprise, provide your DMBE certification number: __________________ For certification assistance, please visit: http://www.dmbc.state.va.us/swamcert.html.

x Large.

___ Small. An independently owned and operated business which, together with affiliates, has 250 or fewer employees or average annual gross receipts of $10 million or less averaged over the previous three years. Department of Minority Business Enterprise (DMBE) certified women-owned and minority-owned business shall also be considered small business when they have received DMBE small business certification...

___ Women-Owned. A business concern that is at least 51% owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest is owned by one or more women who are citizens of the United States or non-citizens who are in full compliance with the United States immigration law, and both the management and daily business operations are controlled by one or more women who are U.S. citizens or legal resident aliens.

___ Minority-Owned. A business concern that is at least 51% owned by one or more minority individuals (see Section 2.2-1401, Code of Virginia) or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest in the corporation, partnership, or limited liability company or other entity is owned by one or more minority individuals and both the management and daily business operations are controlled by one or more minority individuals.

COMPANY INFORMATION/SIGNATURE: In compliance with this Request for Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods and services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

<table>
<thead>
<tr>
<th>FULL LEGAL NAME (PRINT)</th>
<th>FEDERAL TAXPAYER NUMBER (ID#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalSign, Inc.</td>
<td>45-0563843</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS NAME/DBA NAME/TA NAME</th>
<th>FEDERAL TAXPAYER NUMBER (If different than ID# above)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BILLING NAME</th>
<th>FEDERAL TAXPAYER NUMBER (If different than ID# above)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Company name as it appears on your invoice)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURCHASE ORDER ADDRESS</th>
<th>PAYMENT ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 International Dr., Ste. 105</td>
<td>Portsmouth, NH 03801</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTACT NAME/TITLE (PRINT)</th>
<th>SIGNATURE (IN INK)</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Murray/SVP Sales</td>
<td>John Murray</td>
<td>4-15-2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E-MAIL ADDRESS</th>
<th>TELEPHONE NUMBER</th>
<th>TOLL FREE TELEPHONE NUMBER</th>
<th>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:john.murray@globasign.com">john.murray@globasign.com</a></td>
<td>603-570-7061</td>
<td>877-775-4562</td>
<td>603-570-7059</td>
</tr>
</tbody>
</table>

04/09
Attachment D
Terms and Conditions for Trusted Root,
for Virginia Tech and Virginia Non-Profit Cooperative Use Only
Request for Proposal 648260
The Trusted Root Terms and Conditions ("Terms") set forth herein taken together with the Trusted Root Registration Form ("Registration Form") and the Purchase Order ("Order") constitutes the agreement ("Agreement") between GMO GlobalSign, Inc ("Supplier"), a company incorporated under the laws of New Hampshire, U.S., having its registered office at 2 International Drive, Suite 105, Portsmouth NH, 03801, and the entity that is the signatory to and identified in the Registration Form ("Customer").

1. TRUSTED ROOT

Subject to the applicable Registration Form and Order, Supplier will provide to Customer certificate chaining services ("Services"). In connection with the Services, Supplier will chain the certificate issuing authority operated by the Customer (after chaining: "Trusted Root CA") to the digital certificate hierarchy of the GlobalSign Public Certification authority ("Public CA") through digital signing a Customer-operated certification authority (after signing: "Trusted Root CA Certificate") using private keys cryptographically related to a public root certificate ("Public CA Root") issued or operated by the Public CA.

Customer acknowledges that the Public CA hierarchy is governed by the Public CA’s Certification Practice Statement, Certificate Policy and associated policies, to the extent permitted by law, as amended from time to time by that Public CA (collectively “Public CA Policies”). The Public CA Policies can be consulted on-line at the web address http://www.globalsign.com/repository. Customer shall operate and administer the Trusted Root CA in conformity with (i) the Public CA Policies, and (ii) such reasonable guidelines and/or instructions as Supplier may inform Customer from time to time. Provided, however, in no event shall Customer be: (i) required to indemnify or hold harmless Supplier or any third party for any act or omission; (ii) bound to any arbitration or to the decision of any arbitration board, commission, panel, or other entity; or (iii) bound to the application of the laws of any state or country other than Virginia in interpreting or enforcing the contract or requiring that any dispute under the contract be resolved in the courts of any state or country other than Virginia, United States.

At any time during the term of this Agreement Customer may request Supplier to perform additional services ("Additional Services"). Such Additional Services may consist of (i) the performance of services similar to the Services for one or more additional Customer-operated certification authorities; (ii) chaining one or more Customer-operated certification authorities to an Trusted Root CA; (iii) the re-performance of the Services in case of changes to the Trusted Root CA infrastructure environment and/or configuration; and/or (iv) consultancy. The provision of any Additional Services shall be subject to execution of a separate Purchase Order or similar written instrument (which may include additional terms and conditions) and payment of the applicable fees.

2. LICENSE GRANT AND RESTRICTIONS

Supplier grants Customer a limited, non-exclusive, non-transferable and non-sublicensable license to use the Trusted Root CA solely for issuing digital certificates to and for use by Authorized Users only. For the purposes of this Agreement "Authorized User" shall mean any (i) officer, director, employee or temporary staff of Customer or Customer Subsidiary, (ii) any computer server or application hosting Customer content within the context of Customer’s ordinary course of business, (iii) computer or machine-code published by Customer. "Subsidiary" means any entity that is controlled by Customer where control means the ownership of more than fifty percent (50%) of the voting securities or ownership interest or equivalent power over the management of such entity. To the extent explicitly agreed upon in writing, Customer may use the Trusted Root CA Certificate to issue certificates to members of staff of (i) companies affiliated with Customer, or (ii) Customer’s business partners, provided always that such certificates are used for non-commercial and internal business purposes only. Nothing in this Agreement grants and nothing in this Agreement shall be construed to grant Customer, any Authorized User or any third party any rights or licenses to issue, sell, re-sell or otherwise distribute certificates issued under or chained to the Trusted Root CA Certificate beyond the rights and licenses explicitly set forth herein. Issuance of certificates under the Trusted Root CA Certificate is in any event restricted to digital certificates of the type and categories set forth in the Order and/or the Registration Form.

3. REQUIREMENTS AND RESPONSIBILITIES

Customer, in its capacity as certification authority, is responsible for operating the Trusted Root CA and managing the lifecycle of the digital certificates issued under the Trusted Root CA. To that end Customer shall develop within a reasonable period of time from the date of this Agreement (such period not to exceed two (2) calendar months) its own certification practice statement and associated policies and practices (collectively “Customer Policies”). The Customer Policies must be consistent with the Public CA Policies. Customer is responsible for ensuring that only suitably skilled and qualified administrators are appointed and authorized to operate the Trusted Root CA. The Trusted Root CA must be operated in compliance with the Customer Policies and the then current industry standards, including the applicable standards regarding personnel security and physical and logical security of a certification authority infrastructure. Customer acknowledges and accepts that changes to the Trusted Root CA environment and/or configuration (such as, inter alia, changes in the software and/or hardware deployed by Customer to operate the Trusted Root CA) may affect the Trusted Root CA Certificate. Supplier shall not be responsible for any costs, expenses and liabilities incurred by Customer in connection with the operation of the Trusted Root CA.

Customer shall safeguard the Trusted Root CA Certificate and shall keep it at all times stored on a secured hardware signing module conform FIPS 140 Level 3 standards. In the event the Trusted Root CA Certificate is compromised or threatens to be compromised or the reliability of the digital certificates issued under the Trusted Root CA Certificate is otherwise degraded, Customer shall (i) refrain from making further use of the Trusted Root CA Certificate; (ii) promptly revoke the Trusted Root CA Certificate and any certificate issued thereunder; and (iii) inform Supplier and/or the Public CA promptly.

During the term of this Agreement, Customer shall not use or allow usage of the Trusted Root CA Certificate to sign or cross-sign digital certificates (including, without limitation, root certificates) of any certification service provider or certification authority. Likewise, Customer shall not allow that the Trusted Root CA Certificate is signed or cross-signed by any such certification service provider or certification authority or obtain services similar to the Services from any third party during the term of this Agreement.

At any time during the term of this Agreement, Customer may request Supplier to suspend or revoke the Trusted Root CA Certificate. Supplier reserves the right to immediately suspend the Trusted Root CA Certificate in the event of (i) a threatened or actual compromise of the Trusted Root CA Certificate, or (ii) a material breach by Customer of any of its obligations hereunder where Customer fails to remedy such breach within thirty (30) calendar days following Supplier’s written notice thereof. Any suspension and/or revocation of the Trusted Root CA Certificate shall (i) not affect the continuance into force of this Agreement, and (ii) not give rise
to any refund or reimbursement of any pre-paid fees. The immediately foregoing sentence shall apply except to the extent such suspension or revocation arises from the suspension or revocation from the Public Root Certificate or from a Force Majeure event (as defined in Section 11 below).

4. FEES AND PAYMENT

Customer shall pay Supplier the fees stated in the Order and/or Registration Form in accordance with the payment schedule set forth therein. Customer is solely responsible for any and all taxes or duties arising from or imposed on any services delivered hereunder or amounts payable hereunder, excluding taxes based on Supplier’s net income except to the extent Customer provides Supplier with a valid certificate of tax exempt status. Without limiting the foregoing, Customer shall pay such additional amounts as may be required in order that the net amount actually received by Supplier, after deduction or withholding of all applicable taxes and duties, shall be equal to the amount expressed to be payable pursuant to the terms of the Agreement and the applicable Order and/or Registration Form. Except to the extent otherwise agreed upon in the Order and/or the Registration Form, Supplier may revise its prices and/or the Registration Form, and in accordance with the payment terms set forth in the Agreement unless Customer provides written notice to Supplier in accordance with Section 5 below.

5. TERM AND TERMINATION

The effective date of this Agreement shall be as set forth in the Registration Form, and the initial term (“Initial Term”) of this Agreement shall be as set forth therein. Following the Initial Term, this Agreement may be renewed for subsequent periods of one (1) year if the parties agree in writing to extend this Agreement at least sixty (60) calendar days prior to the end of the Initial Term or the then current renewal term. This Agreement may be terminated immediately and without indemnity upon providing written notice (i) by either party, if the other party commits a material breach of any of the obligations hereunder and (if that breach is capable of remedy) fails to remedy it within thirty (30) calendar days of receipt of written notice thereof; (ii) by either party, if the other party ceases doing business, becomes insolvent or is affected by bankruptcy, liquidation or any similar procedure; (iii) by either party if the other party suffers a Force Majeure event (as defined under Section 11 below) and such event persists for (1) calendar month or more; (iv) by Supplier, if Supplier’s reputation, goodwill and/or infrastructure security posture is compromised or threatens to be compromised due to any act of failure to act by Customer. Upon termination or expiration of this Agreement (i) the rights and licenses granted hereunder to Customer shall immediately terminate; (ii) the Trusted Root CA Certificate shall be revoked; (iii) each party shall promptly return to the other all proprietary and/or confidential material in its possession or under its control and received from the other party under this Agreement, including all copies thereof. Termination or expiration of this Agreement shall not affect the continuity if force of any provision which is expressly or by implication intended to continue in force on or after such termination or expiration.

6. DATA PROTECTION AND CONFIDENTIALITY

In its performance hereunder each party shall at all times comply with the applicable legislation and regulations on data privacy and protection. Notwithstanding the above, Customer agrees that, to the extent reasonably required to perform, administer, bill or account under this Agreement, Supplier shall have the right to use, process and transfer any information and data obtained from or through Customer and disclose the same to Supplier’s employees, agents, professional advisers, subcontractors and affiliated companies, both within and outside one or more national or supra-national jurisdictions. Customer represents and warrants that all concerned natural and legal persons have given their express and unambiguous consent to allow Supplier to use, process and transfer such data as set forth above.

In relation to the confidential and/or proprietary information that may be disclosed by or originate from a party hereto, the party receiving such information agrees to (i) limit access to such information to its officers, directors and employees (including the officers, directors and employees of any related corporate body that controls, is controlled by or under common control with that party); (ii) use all reasonable care and take all reasonable measures to safeguard the other party’s confidential and/or proprietary information from inadvertent and/or unauthorized disclosure to any third party.

7. INTELLECTUAL PROPERTY RIGHTS

All title, copyrights, trademarks, service marks, patents, patent applications and all other intellectual proprietary rights now known or hereafter recognized in any jurisdiction (“IP Rights”) in and to the Supplier’s technology, web sites, documentation, products and services (collectively “Proprietary Materials”) are owned and will continue to be exclusively owned by Supplier and/or its licensors. Customer agrees to make no claim of interest in or to any such IP Rights. Customer acknowledges that no title to the IP Rights in and to the Proprietary Materials is transferred to Customer and that Customer does not obtain any rights, express or implied, in any IP Rights and Proprietary Materials other than the rights expressly granted in the Agreement.

8. LIMITED WARRANTY

Supplier warrants that Services will be performed in a professional manner using reasonable care and skill. Supplier warrants that the information embedded in each Trusted Root CA Certificate provided will, at the time of provisioning, contain no material errors resulting from Supplier’s or the Public CA’s failure to exercise reasonable care in generating the Trusted Root CA Certificate. EXCEPT TO THE EXTENT EXPLICITLY STATED OTHERWISE IN THIS AGREEMENT, ALL PRODUCTS AND SERVICES ARE PROVIDED “AS IS” AND SUPPLIER MAKES NO WARRANTIES WITH RESPECT TO USEFULNESS, FUNCTIONALITY, OPERABILITY, TIMELINESS AND NON-INFRINGEMENT. SUPPLIER HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

9. LIMITATION OF LIABILITY

SUPPLIER’S AGGREGATE LIABILITY TO CUSTOMER FOR ALL DAMAGES AND IN RESPECT OF ANY AND ALL CAUSES OF ACTION AND CLAIM AT ANY TIME OR TIMES, INCLUDING, WITHOUT LIMITATION, ANY BREACH OF WARRANTY, SHALL NOT EXCEED THE AMOUNT EQUAL TO THE LESSER OF (I) THE FEES ACTUALLY PAID BY CUSTOMER HEREUNDER DURING THE PRECEDING TWELVE (12) MONTHS, OR (II) THE EQUIVALENT OF TWO-HUNDRED AND FIFTY THOUSAND U.S. DOLLARS ($250,000). UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT OR OTHERWISE SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL SPECIAL, INDIRECT OR INCIDENTAL DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS, REVENUE, INFORMATION, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
Customer shall bear sole and exclusive responsibility and liability to Supplier and to any other entity and person for any actions or failures to act by Customer (including, without limitation, the acts or omissions by any Trusted Root CA administrators) in connection with the Agreement. The foregoing provisions shall be enforceable to the extent permitted by applicable law.

10. REPORTING AND AUDIT

Customer shall keep reasonable records relating to any of Customer’s responsibilities and obligations under this Agreement. Within thirty (30) calendar days following each anniversary date of this Agreement, Customer agrees to certify to Supplier in writing (i) the total number of certificates issued under or from the Trusted Root CA, and (ii) its compliance with the terms and conditions of this Agreement. During the Agreement and for a period of one (1) calendar year thereafter, Supplier may, upon reasonable notice and during normal business hours, periodically audit Customer’s compliance with the Agreement. In the event any such audit discloses any material breach by Customer (or its employees or agents) of its obligations hereunder, Customer shall, in addition to such other rights and remedies that may be available to Supplier, refund Supplier the reasonable costs and expenses incurred by Supplier in connection with such audit.

11. MISCELLANEOUS

Entire Agreement. This Agreement (including any Order and Registration Form) constitutes the entire agreement between the parties and supersedes all prior understandings, oral or written, between the parties with respect to the subject matter thereof. To the extent of any inconsistencies, priority of effectiveness shall be 1) Order, 2) Registration Form, and this 3) Trusted Root Terms and Conditions. The terms and conditions on any present or future Order and/or Registration Form submitted by Customer which alter, modify or conflict with the terms and conditions of this Agreement are void, irrespective of such documents are acknowledged or accepted by Supplier without making any reservation.

Export Controls. Each party agrees to comply with all applicable United States, European Union, Australian and other supra-national or national export laws and regulations (to the extent applicable). Customer shall not solicit and shall not accept any certificate applications from any person or organization that is on the most recent United States export exclusion lists, and shall not perform any Corporate CA organization that is on the most recent United States export controls or other similar restriction. Customer represents and warrants that any Authorized User is not located in, under the control of, or a national or resident of any such country or on any such list.

Notices. Any notice required or permitted by this Agreement shall be served to Supplier or Customer (as applicable) at the address indicated above or in the Registration Form or to such other address as designated by written notice. A notice takes effect from the time it is received unless a later time is specified in it. A notice is deemed to be received (i) in the case of an express couriered letter, on the date of actual delivery; (ii) in the case of a mailed letter, on the third (3rd) day, or, if mailed to or from one country to another, on the fifth (5th) day after mailing; and (iii) in the case of a facsimile, on production of a transmission report by the machine from which the facsimile was sent which indicates that the facsimile was sent in its entirety to the facsimile number of the recipient.

Force Majeure. Neither party will be liable for any default or delay in the performance of all or part of its obligations (other than an obligation to make payment of any monies) under this Agreement to the extent such default or delay is caused by acts of governments, hostilities, power failures, fire, strike, riot, or any other event beyond its reasonable control (“Force Majeure event”). Present or future restrictions and/or other regulations of any country regarding the export and/or import of products or services which would hamper Supplier to provide a product and/or service shall constitute a Force Majeure event.

Relationship of the Parties. In all matters relating to this Agreement, each party is an independent contractor and neither party will have or represent that it has the right, power or authority to bind, contract or commit the other party or to create any obligation on behalf of the other party.

References. Neither party may issue external press or publicity releases relating to this Agreement without prior written approval of the other party, except as may be required by applicable law or securities regulations. Notwithstanding the foregoing and unless otherwise agreed upon in the Registration Form, Supplier shall be allowed to use Customer’s name on its customer lists and disclose the same to its present and potential customers and partners and investors.

Amendment - Waiver. This Agreement (in whole or in part) may be amended or supplemented only by a writing signed by authorized representatives of each party. Failure by a party to require performance of any provision thereof shall not affect the right of such party to enforce the same, nor shall any waiver of a breach be deemed a waiver of any other breach.

Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement. In the event that any provision of this Agreement is determined to be invalid, unenforceable or otherwise illegal, such provision shall be deemed restated, in accordance with applicable law, to reflect as nearly as possible the original intentions of the parties, and the remainder of the Agreement shall remain in full force and effect.

Assignment. Supplier shall have the right to assign or delegate all or part of its rights under this Agreement to its affiliated companies, and may use affiliates or service providers to perform all or some of its duties and obligations. Customer may only transfer its rights and commitments under this Agreement (whether in whole or in part) to a third party with the prior written consent of Supplier, which consent will not be unreasonably withheld.

Governing Law. The Agreement shall be construed, interpreted and enforced in accordance with the laws of the state of Virginia, US. The parties agree that any and all disputes, claims or litigation arising from or related in any way to the Agreement shall be resolved by the courts located in the judicial district or region where Customer maintains its place of business as stated in the Registration Form. The parties waive any objections against and agree to submit to the aforementioned jurisdiction.
Attachment E

Pricing and Registration Form for Trusted Root,

for Virginia Non-Profit Cooperative Use Only

Request for Proposal 648260
RFP 648260 Discounted Pricing for Trusted Root for Virginia Non-Profit Cooperative Use Only based on volume

<table>
<thead>
<tr>
<th>Trusted Root SSL Certificates</th>
<th>Up to this volume</th>
<th>Price per Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50</td>
<td>$105</td>
</tr>
<tr>
<td></td>
<td>75</td>
<td>$90</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>$75</td>
</tr>
<tr>
<td></td>
<td>200</td>
<td>$60</td>
</tr>
<tr>
<td></td>
<td>500</td>
<td>$45</td>
</tr>
<tr>
<td></td>
<td>1,000</td>
<td>$32</td>
</tr>
<tr>
<td></td>
<td>2,500 and above</td>
<td>$20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trusted Root Client/User License</th>
<th>Up to this volume</th>
<th>Price per Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>500</td>
<td>$11</td>
</tr>
<tr>
<td></td>
<td>1,000</td>
<td>$8</td>
</tr>
<tr>
<td></td>
<td>3,000</td>
<td>$6</td>
</tr>
<tr>
<td></td>
<td>5,000</td>
<td>$4</td>
</tr>
<tr>
<td></td>
<td>10,000</td>
<td>$3</td>
</tr>
<tr>
<td></td>
<td>20,000 and above</td>
<td>$2</td>
</tr>
</tbody>
</table>
# TrustedRoot Registration Form

**GlobalSign contract N°:** [__]

### TrustedRoot Registration details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company (registered entity):</td>
<td>[__]</td>
</tr>
<tr>
<td>Address:</td>
<td>[__]</td>
</tr>
<tr>
<td>Registration N°:</td>
<td>[__]</td>
</tr>
<tr>
<td>TrustedRoot Agreement:</td>
<td>Effective Date: [__] Initial Term: [three (3) years from Effective Date]</td>
</tr>
<tr>
<td>TrustedRoot Terms and Conditions:</td>
<td>Version: [__]</td>
</tr>
<tr>
<td>Authorized Reseller:</td>
<td>[reseller company details] or [N/A]</td>
</tr>
<tr>
<td>Applicable Fees / Payment Terms:</td>
<td>[as agreed between Company and Authorized Reseller] or [see Payment Appendix attached hereto] or [as set forth in Quote X, version Y, dated Z]</td>
</tr>
<tr>
<td>Certificate type / category:</td>
<td>[__]</td>
</tr>
<tr>
<td>Certificate usage:</td>
<td>[NOTE: Terms specify that the following applies except to the extent detailed otherwise in this Form: <em>Pursuant to Section 2 (LICENSE GRANT AND RESTRICTIONS) of the TrustedRoot Terms and Conditions, Company shall use the Company Root's private key for its own non-commercial and internal business purposes only. Without limiting the foregoing, digital certificates signed by the Company Root's private key may only be (a) issued by a certificate issuing authority operated by Company, and (b) used for communication within Company's closed user group, i.e. for communication in the normal course of Company's business between Company's members of staff or between Company's members of staff and a third party.</em> If this is not to be changed specify [As set forth in the TrustedRoot Terms and Conditions.]]</td>
</tr>
<tr>
<td>Company CA software platform:</td>
<td>[__]</td>
</tr>
<tr>
<td>Company CA hardware signing module:</td>
<td>[__]</td>
</tr>
<tr>
<td>Specific Provisions:</td>
<td>[none]</td>
</tr>
</tbody>
</table>

### Authorization

By its signature, Company acknowledges and agrees that this Registration Form is subject to the version of the TrustedRoot Terms and Conditions indicated above, which terms and conditions that shall be deemed incorporated herein by reference.

**Signed for and on behalf of GlobalSign:**

- **Entity:** GlobalSign Inc
- **Address:** 2 International Drive, Suite 105 Portsmouth NH, 03801
- **Country:** US
- **Name:**
- **Function:**
- **Date:**
- **Signature:**

**Signed for and on behalf of Company:**

- **Entity:**
- **Address:**
- **Country:**
- **Name:**
- **Function:**
- **Date:**
- **Signature:**
Attachment F

Terms and Conditions for Managed SSL and ePKI,

for Virginia Non-Profit Cooperative Use Only

Request for Proposal 648260
SSL Managed Service Agreement

This SSL Managed Service Agreement (“Agreement”), together with all attached Schedules, is made between GlobalSign, Inc., a New Hampshire Corporation, (“GlobalSign”) and ___ (“Company”) as of _____ (the “Effective Date”), as indicated by the signatures below:

COMPANY:

______________________
Telephone: _________________
Fax: _________________
Email address: _________________
Home Page URL: _________________

______________________
Signature

______________________
Printed Name

______________________
Title

GMO GLOBALSIGN, INC.

Two International Drive, Suite 105
Portsmouth, NH 03801

Telephone: _________________
Fax:  603-570-7059
Account Manager: _________________
Telephone: _________________

______________________
Signature

______________________
Printed Name

______________________
Title

1. The Certificates. GlobalSign agrees to provide Company with OrganizationSSL certificates (“Certificates”) issued through its service named “SSL Managed Service” (further described in Schedule A), for Company’s use according to the terms of this Agreement and the Certificate Practices Statement (“CPS”) found at http://www.globalsign.com/repository. In using the Certificates, Company agrees to comply with the terms of this Agreement, all applicable laws and regulations, and the CPS. For the avoidance of doubt, CPS shall take precedent over this Agreement should they conflict with any terms set forth thereunder. Provided, however, in no event shall Company be: (i) required to indemnify or hold harmless GlobalSign or any third party for any act or omission; (ii) bound to any arbitration or to the decision of any arbitration board, commission, panel, or other entity; or (iii) bound to the application of the laws of any state or country other than Virginia in interpreting or enforcing the contract or requiring that any dispute under the contract be resolved in the courts of any state or country other than Virginia, United States.

2. Limitations on Use. Company shall not (a) use or duplicate the Certificates except as permitted by this Agreement, (b) distribute or resell the Certificates to any third party. Notwithstanding anything to the contrary herein or in the Subscriber Agreement (defined under Section 6 below), Company may install the Certificate on one server per fully qualified domain name (FQDN) and then may export the same certificate or key pair on up to two (2) additional server for the purpose of backup, redundancy and/or load balancing.

3. Payments. Company agrees to pay GlobalSign for the Certificates according to the fees and terms stated on Schedule B.

4. Designation of Certificate Administrator, Order Process, and Other Company Obligations. Company will designate one or more individuals (up to the maximum number permitted under Schedule B) with authority to submit any domain names for vetting by GlobalSign and to approve the issuance of Certificates for the
vetted domain names in accordance with this Agreement (the “Certificate Administrator(s)”). Company may only submit domain names for vetting for which Company is the registered owner. GlobalSign will provide each Certificate Administrator(s) with a user name and password (or client certificate) for the purpose of ordering and approving issuance of the Certificates. All communications concerning the approval of Certificates to be issued to Company will be made by and through the designated Certificate Administrator(s).

The Certificate Administrator(s) will be responsible for verifying the information in all Certificate orders submitted to GlobalSign, and GlobalSign shall have no responsibility for verifying the accuracy or legitimacy of these orders. The Certificate Administrator(s) must notify GlobalSign immediately in the event s/he becomes aware that a Certificate should be revoked for any reason.

5. Set-up Information. Company will provide information as necessary for GlobalSign to set up the SSL Managed Service service. Company warrants that it has authority to release any information it provides to GlobalSign pursuant to this Agreement and that providing the information does not violate any applicable contract or privacy policy.

6. Subscriber Agreement. Company acknowledges that the party requesting a Certificate (the “Subscriber”) or Company, on behalf of the Subscriber, must agree to a subscriber agreement with GlobalSign before using the Certificate.

7. Term; Changes in Fees. The initial term of this Agreement will begin on the Effective Date and, unless terminated earlier in accordance herewith, will continue for a period of one (1) years (“Initial Term”). Following the Initial Term, this Agreement may be renewed for subsequent periods of one (1) year if the parties agree in writing to extend this Agreement at least sixty (60) calendar days prior to the end of the Initial Term or the then current renewal term.

At any time following the end of the Initial Term, GlobalSign may change the fees for the Certificates by giving thirty (30) days prior written notice thereof to Company.

Funds deposited under this Agreement must be used by Company within one year from the date of purchase. If an additional deposit is made within the initial twelve (12) months of this agreement, unused funds from the initial deposit will be automatically be available twelve (12) months from the new deposit date.

In the event of termination of this Agreement pursuant to Section 13, Company may continue to install any Certificates purchased prior to termination until their expiration (and will not be entitled to any refund or credit therefor), and the parties agree that the terms and conditions of this Agreement and the Subscriber Agreement shall continue to apply to those Certificates following termination.

8. Limited Warranty and Disclaimer. GlobalSign warrants that the Certificates conform to any specific standards set forth under the CPS. Except for the foregoing, GlobalSign does not make any representations or warranties, express or implied, to Company, the Certificates viewers or users, or any other person, including, without limitation, any merchantability, or fitness for a particular purpose.

9. Limitation of Liability. Each party’s aggregate liability to the other (either directly or as a third party defendant in any action or proceeding) for any claim arising out of or relating to this Agreement or the use of or inability to use the Certificates will in no event exceed the amount of fees paid by Company for the Certificates within the one (1) year period immediately prior to the event that gave rise to its claim.

10. Limitation of Damages. Neither party shall be liable to the other or any third party for any special, consequential, incidental or indirect damages including, but not limited to, loss of profits, revenue, or damage to data arising out of the use of or inability to use the Certificates whether or not the party has been advised of the possibility of such damages.

11. Ownership of Intellectual Property. Neither party shall obtain any ownership or other interest in the intellectual property of the other by reason of this Agreement.

12. Use of Logos, Trademarks, and URLs. Each party grants the other a limited license during the term of this Agreement to use the party’s corporate name, URL, and product names (the “Names”) on the other’s Web site for listing the party as a provider/purchaser of the Certificates and to promote the Certificates. Use of Company logo and/or trademark, if permissible, requires a separate signed agreement. Each party agrees to provide the other with the current version of the Names and any subsequent changes together with the party’s style guide to ensure proper placement and use by the other party. Each party may withdraw this limited license at any time upon reasonable notice to the other. Other than the rights granted in this section or by subsequent agreement, each party agrees that it has no other rights to the Names of the other party.

13. Termination. Notwithstanding anything to the contrary contained in this Agreement, this Agreement may be terminated immediately by one party giving the other a written notice of termination if (a) the other party breaches any of the terms of this Agreement and such breach continues for a period of thirty (30) days after notice thereof has been given by a party; (b) the other party files for bankruptcy, ceases to carry on business, or undergoes liquidation; or (c) the other party is unable to perform a material portion of its obligations under this Agreement as a result of an event or events of force majeure for a period of not less than thirty (30) days.

Upon termination of this Agreement in any manner, (1) Company shall immediately pay GlobalSign the fees outstanding for the period ending on the day of termination; (2) all rights of the parties under this Agreement shall cease immediately (except for those which, by their nature, would continue after termination); and (3) each party shall immediately remove the other party’s Names and references thereto and any hypertext links on their Web sites.

14. Miscellaneous. This Agreement may not be assigned by either party without the other party’s prior written consent. This Agreement may not be modified except in a subsequent writing signed by both parties. This Agreement shall be interpreted under
the laws of Virginia without regard to its conflict of law provisions. Venue shall be in the courts of the Commonwealth of Virginia.

15. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties related to SSL Managed Service and supersedes any prior written or oral agreement or understanding with respect to the subject matter thereof.
Schedule A

Description of SSL Managed Service

SSL Managed Service: SSL Managed Service is the issuance of OrganizationSSL (OV) certificates, OrganizationSSL (OV) Wildcard certificates, and ExtendedSSL (EV) certificates for domain names owned by Company and vetted by GlobalSign. OrganizationSSL and ExtendedSSL are SGC enabled SSL Certificates that is widely compatible with (i.e., treated as a trusted root by) the current Web browser user base. All certificates include a subscription to GlobalSign’s Secure Site Seal - an active digital icon for web sites that allows viewers to ascertain the web site owner’s verified business identity. Certificates are managed through a web based interface called the GlobalSign Certificate Center (“GCC”).

GCC provides full SSL certificate issuance and lifecycle management capabilities through a web based user interface. The “Company” submits domains for a onetime pre-vetting process and once approved this allows the company to issue both OV and EV SSL certificates to sub domains of those authenticated domains without further vetting. This pre-vetting is valid for one year after which it will be refreshed.

OrganizationSSL (OV) Standard Certificate: An OrganizationSSL standard certificate is a 128-bit SSL server certificate issued by GlobalSign that is widely compatible with (i.e. treated as a trusted root by) the current Web browser user base. They are bound to and secure a single fully qualified domain name (i.e. www.globalsign.com) on up to three (3) physical servers per license. The certificates are vetted to a second level domain according to authentication processes as stated in GlobalSign’s applicable Certification Practices Statement located on the GlobalSign website at http://www.Globalsign.com, and may be used in connection with all third level and higher domains that contain the second level domain.

OrganizationSSL (OV) Wildcard Certificate: An OrganizationSSL Wildcard certificate is a standard 128-bit SSL server certificate issued by GlobalSign that is widely compatible with (i.e. treated as a trusted root by) the current Web browser user base. Wildcard certificates allow multiple sub domains to be secured using a single certificate that match a specific pattern or syntax using the wildcard character “*” (i.e.*.globalsign.com). A single license covers up to three (3) physical servers. The certificates are vetted to a second level domain according to authentication processes as stated in GlobalSign’s applicable Certification Practices Statement located on the GlobalSign website at http://www.Globalsign.com, and may be used in connection with all third level and higher domains that contain the second level domain.

ExtendedSSL (EV) Certificate: An ExtendedSSL certificate is a 128-bit SSL server certificate issued by GlobalSign that is widely compatible with (i.e. treated as a trusted root by) the current Web browser user base. They are bound to and secure a single fully qualified domain name (i.e. www.globalsign.com) on up to three (3) physical servers per license. The certificates are vetted to a second level domain according to authentication processes as stated in GlobalSign’s applicable Certification Practices Statement located on the GlobalSign website at http://www.Globalsign.com, and may be used in connection with all third level and higher domains that contain the second level domain.

GlobalSign ExtendedSSL Certificates activate the “Extended Validation Support” in new browsers including Microsoft IE 7, Opera, Mozilla Firefox, Google Chrome and Apple Safari. Turns the address bar “green” and clearly shows who owns the certificate in the browser user interface.

The Extended Validation vetting process establishes the legitimacy of an organization within a specific jurisdiction of incorporation. It also clearly identifies the organizations principle place of business through a rigorous and stringent set of well defined validation processes. The process encompasses authentication of the organizations domain ownership rights as well as contractually binding the organization to a subscriber agreement which benefits relying parties and strengthens the security of the internet as a whole.

Enrollment & Disclosure: The Company’s Certificate Administrator provides GlobalSign with an approved list of a domain names for vetting (up to the maximum number purchased by Company under Schedule B). Additional domain names and Certificate Administrators may be purchased at the prices shown in Schedule B. GlobalSign checks the applicant’s domain name against the Company’s pre-vetted domain name list and forwards certificate
requests that coincide with the Company’s pre-approved domain names to the designated account under GCC, where the Company’s Certificate Administrator approves or rejects the Certificate request. If the request is approved, GlobalSign proceeds with issuing a Certificate to the individual who submitted the request. If denied, the order is cancelled and Company is not charged for the Certificate.
Schedule B
Fees and Payment Information

Company may cancel a Certificate or request revocation of a Certificate at any time, but Company will not be entitled to any refund, prorated or otherwise, for such cancellations or revocations unless cancellation or revocation is requested within 7 days of issuance of the Certificate.

Company agrees to pay GlobalSign the following fees for Certificates that are ordered and approved by the Certificate Administrator. Requests for Certificates that are denied will not be charged. Company agrees that GlobalSign may revoke or cancel Certificates previously provided by GlobalSign in the event of non-payment by Company. Fees are stated in U.S. dollars.

Initial Order:
On the Effective Date, Company agrees to purchase the following OrganizationSSL and ExtendedSSL Certificates where applicable in the quantities at the price(s) indicated below:

<table>
<thead>
<tr>
<th>Block Size</th>
<th>Validity Period of Certificates (1, 2, 3, 4, or 5 yr)</th>
<th>Price per Certificate</th>
<th>Price per block</th>
<th>Number of Domain Names Included</th>
<th>Number of Certificate Administrators Included</th>
<th>Net Price</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$</td>
<td>$</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
</tbody>
</table>

Net Block Price (from table above): $
Fee for Additional Domain Names: Not applicable (0 x $75 per Domain Name per year)
Fee for Additional Certificate Administrators: Not applicable (0 x $100 per Certificate Administrator per year)

Initial Order: $

Support Fees: $0, Standard (0% of list price of Initial Order)

Total Initial Order: $(list price for Initial Order + Applicable Support Fee)

Subsequent Orders:
During the Initial Term, Company may continue to purchase Certificates in block purchases in the quantities at the prices indicated below. Company will only be entitled to the discounted price for a specific block size if the Certificates are all purchased and paid for at the same time as a single block. The purchase of blocks at one time will not be counted toward the purchase of additional blocks at a later time for the purpose of obtaining a lower price per block for the later purchase.

During the Initial Term, Company may purchase additional domain names and/or Certificate Administrators at the prices indicated below:

<table>
<thead>
<tr>
<th>Additional Domain Names</th>
<th>Additional Certificate Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Charge</td>
<td>No Charge</td>
</tr>
</tbody>
</table>

Billing Contact Information:

Name: ________________________ Phone: ________________________
Address: ______________________ Fax: ________________________
_________________________________ Email: ________________________

GlobalSign will invoice Company for the Initial Order on the Effective Date. Subsequent Orders will be invoiced at the time the order is placed. All payments are due and payable net thirty (30) days from Company’s receipt of invoice. Company agrees to pay interest at the rate of 1.5 percent per month or the maximum legal rate on all amounts over seven (7) days overdue. Company will pay any applicable taxes, fees and similar governmental charges related to the execution or performance of this Agreement, other than applicable income taxes imposed on GlobalSign related to its receipt of payments from Company. Fees may change as provided in Section 7.
This ePKI Service Agreement (this "Agreement") is made as of __________, 2010 ("Effective Date") by and between GMO GlobalSign, Inc., 2 International Drive, Suite 105, Portsmouth, NH 03801 ("GlobalSign") and _______________ with a principal place of business at ____________________ ("Company"), and governs Company’s use of the GlobalSign ePKI service, a service under which Company applies for, issues, manages, and uses certificates, and GlobalSign generates such certificates and provides related services to Company on an out-source basis (the "Service").

Company understands that a certificate serves to identify the party named in the certificate (the “Subscriber”) for the purposes of electronic commerce, access, and communication.

This GlobalSign ePKI Service Agreement ("Agreement") shall become effective between GlobalSign ("GlobalSign") and the organization agreeing to this Agreement ("Local RA" or "LRA") upon LRA agreeing to terms and conditions stated herein through clicking the agree button below (the "Effective Date"). Except for governing law and jurisdiction under the GlobalSign Certification Practice Statement (CPS), GlobalSign CPS is incorporated by reference hereto and is available at www.globalsign.com/repository. Provided, however, in no event shall Company be: (i) required to indemnify or hold harmless GlobalSign or any third party for any act or omission; (ii) bound to any arbitration or to the decision of any arbitration board, commission, panel, or other entity; or (iii) bound to the application of the laws of any state or country other than Virginia in interpreting or enforcing the contract or requiring that any dispute under the contract be resolved in the courts of any state or country other than Virginia, United States.

1. Definitions

For the purposes of this Agreement, all capitalized terms used in this Agreement shall have the meaning ascribed to them in this Section 1 and elsewhere in this Agreement.

Digital Certificate

A record that, at a minimum (a) identifies the Certification Authority issuing it, (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber, (d) identifies its operational period, and (e) contains a serial number and is Digitally Signed by the issuing Certification Authority.
GlobalSign ePKI Service Agreement Version 1.1

Certification Authority ("CA")

GlobalSign or an entity which is certified by GlobalSign to issue Digital Certificate.

Digital Signature

Information encrypted with a Private Key which is appended to electronic data to identify Subscriber and verify the integrity of the electronic data. Digitally Signed shall refer to electronic data to which a Digital Signature has been appended.

Local Registration Authority (LRA)

An entity appointed (other than GlobalSign) that has the responsibility to identify and authenticate Subscribers requesting Digital Certificates. The LRA does not issue Digital Certificates. It merely requests the issuance of Digital Certificates on behalf of Subscriber whose identity it has verified. Under this Agreement, the organization agreeing to this Agreement shall be the LRA.

Private Key

A mathematical key which is kept private to the owner and which is used to create Digital Signatures or to decrypt electronic data.

Public Key

A mathematical key which is available publicly and which is used to verify Digital Signatures created with the matched Private Key and to encrypt electronic data which can only be decrypted using the matched Private Key.

Subscriber

An individual or an organization who (a) is the subject named or identified in a Digital Certificate issued to such an individual or organization, (b) holds a Private Key that corresponds to a Public Key listed in that Digital Certificate, and (c) the individual or organization to whom Digitally Signed messages verified by reference to such Digital Certificate are to be attributed.

Service

The ePKI service provided by GlobalSign to LRA and Subscribers. Under Section 3 below.

Trustworthy System
GlobalSign ePKI Service Agreement Version 1.1

Trustworthy System means computer hardware, software, and procedures that (a) are reasonably secure from intrusion and misuse, (b) provide a reasonable level of availability, reliability, and correct operation, (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

2. Authority to Use ePKI service

Grant of Authority

As of the Effective Date, GlobalSign hereby grants to LRA the authority to use ePKI service under the terms set forth in this Agreement.

Limitations on Authority

LRA shall use the ePKI service only for purposes that are permitted by (a) this agreement and GlobalSign CPA, and (b) any applicable laws and regulations, including any laws regarding the export of data or software.

3. Services Provided by GlobalSign

GlobalSign shall be the CA) issuing the Digital Certificate upon approval of LRA who shall authenticate and validate the application and enrollment information of Subscriber. LRA shall (1) receive and process the Digital Certificate application from Subscriber, (2) send an acknowledgment to Subscriber of either the approval or rejection of the Digital Certificate application, (3) if the Digital Certificate application is approved, instruct GlobalSign to issue the Digital Certificate, and (d) process all requests for revocation of the Digital Certificate upon the receipt of an authenticated request from Subscriber. Subscriber or LRA shall have the right to revoke the Digital Certificate upon, (1) any change to the information on the Digital Certificate or the Digital Certificate application, including, but not limited to the change of the name or domain name registration of Subscriber or (2) any actual or suspected loss, disclosure, or other compromise of Subscriber’s Private Key.

This Service is provided as a web-based service. If this Service is used in conjunction with any third party products, GlobalSign may specify certain specifications to be met by LRA.

a. ePKI for DocumentSign Digital IDs for Adobe PDF

Specific features include:
GlobalSign ePKI Service Agreement Version 1.1

* Certificate management portal capable of issuing Adobe CDS Digital IDs to Subscriber for use in conjunction with Adobe PDF and third party cryptographic products in compliance with the GlobalSign CPS for Adobe Certified Document Services (CDS)

* Reports depicting Digital Certificate enrollment and issuance status

* Revocation capability

* Email management and template customization

* Optional bulk shipment of minimum FIPS 140-1 Level 2 standards cryptographic devices

* Optional time-stamping support

Specific features include:

* Certificate management portal capable of issuing Digital Certificate to Subscriber for use in conjunction with products that utilize Digital Certificate for authentication and digital signing among other applications in compliance with the GlobalSign CPS.

* Reports depicting Digital Certificate enrollment and issuance status

* Revocation capability

* Email management and template customization

* Optional Bulk shipment of minimum FIPS 140-1 Level 2 standards cryptographic devices

4. LRA’s Obligations

LRA shall comply with each of the following obligations:

(1) Perform the registration authority functions necessary for issuance of the Digital Certificate provided by the Service, including application process of the Digital Certificate, and be solely responsible for verifying the identity and information stipulated in the Digital Certificate;

(2) Appoint administrator(s) with an authority to review and approve requests for Digital Certificate and to order, manage, and revoke the Digital Certificate provided under the Service;

(3) Ensure the digital ID or user name and password issued to the administrator which enables an individual to perform the local registration authority functions (collectively, the "Administrator Digital ID") is secure and accessible only by the individual(s) authorized to use;
GlobalSign ePKI Service Agreement Version 1.1

(4) Ensure that information provided on the enrollment requests is complete and accurate;

(5) Protect the confidentiality of the private keys from unauthorized use, access or disclosure by use of
the Trustworthy System, and require the same of Subscriber;

(6) Promptly revoke or request GlobalSign to revoke the Digital Certificate in the event of 1) Subscriber's
violation of this Agreement, or 2) any actual or suspected loss, disclosure, or other compromise of the
private key;

(7) Promptly request that GlobalSign revoke the Administrator Digital ID upon 1) any change to the
information on the Administrator Digital ID, or 2) any actual or suspected loss, disclosure, or other
compromise of the Administrator Digital ID;

(8) Ensure that LRA and Subscriber enter into an agreement that governs the Subscriber's use of the
Digital ID ("Subscriber Agreement"), and that all Subscribers accept and comply with the terms and
conditions of the Subscriber Agreement;

(9) Act as the sole intermediary for all communications with Subscriber;

(10) In the case of ePKI for DocumentSign Digital IDs for Adobe CDS, 1) ensure and enforce all private
key generations are performed on the required cryptographic device (as defined in the GlobalSign CPS
for Adobe Certified Document Services (CDS) ) and are never exported from the device, and 2) distribute
minimum FIPS 140-1 Level 2 standards cryptographic devices to Subscriber;

(11) If applicable, develop code and integrate into GlobalSign's API; and

(12) Create and keep records of 1) Subscriber identity verification and 2) certificate revocation;

(13) Cooperate to audit by either GlobalSign or a third party auditor designated by GlobalSign.

GlobalSign may provide LRA with certain software components solely for LRA’s use in connection with
the Service during the term of this Agreement. In such case, LRA shall not, and LRA shall ensure that
Subscriber will not: (1) alter, copy, or duplicate any aspect of the software; or (2) modify, adapt,
translate, decompile, disassemble or reverse engineer the software or any part thereof in any form
whatsoever, or otherwise attempt to derive source code or create derivative works there from, and shall
not authorize or allow any third party to do any of the above.

Failure to comply with any of the obligations under this Section 4 shall be a breach of this
Agreement.
5. Fees and Payments

LRA shall pay to GlobalSign the applicable fees associated with the Service in accordance with the payment terms agreed between the parties. Company agrees to pay GlobalSign for the Certificates according to the fees and terms stated on Schedule B.

6. DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY

IN NO EVENT (EXCEPT FOR FRAUD OR WILFULL MISCONDUCT) SHALL GLOBALSIGN BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE OR NONPERFORMANCE OF DIGITAL CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS AGREEMENT, EXCEPT FOR DAMAGE DUE TO RELIANCE (IN ACCORDANCE WITH THE CPS) ON THE VERIFIED INFORMATION AS OF THE ISSUANCE OF THE DIGITAL CERTIFICATE UP TO AN AMOUNT SET FORTH UNDER WARRANTY POLICY (AVAILABLE UNDER http://www.globalsign.com/repository/) FOR PERSONALSIGN 2 PRO AND ADOBE CDS CERTIFICATE. NOTWITHSTANDING, GLOBALSIGN WILL NOT BE LIABLE IN ANY CASE IF 1) THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILFULL MISCONDUCT OF THE SUBSCRIBER, OR 2) THERE IS A BREACH OF THIS AGREEMENT BY THE SUBSCRIBER.

7. Term and Termination

7.1 Following the Initial Term, this Agreement may be renewed for subsequent periods of one (1) year if the parties agree in writing to extend this Agreement at least sixty (60) calendar days prior to the end of the Initial Term or the then current renewal term.

7.2 This Agreement shall terminate on the earliest of:

(1) One year from the Effective Date; or

(2) Failure by LRA to perform any of its obligations under this Agreement if such breach is not cured within thirty (30) days after receipt of notice thereof from GlobalSign.

8. Effect of Termination
Upon the termination of this Agreement for any reason, LRA shall have no right in issuing any new Digital Certificate. Notwithstanding the foregoing, any use or effectiveness of the Digital Certificate prior to the termination of this Agreement shall not be affected thereby, and terms and conditions of this Agreement shall continuously apply to the Digital Certificate issued prior to the termination until maturity of such Digital Certificate.


Governing Laws and Jurisdiction

This Agreement shall be governed by, construed under and interpreted in accordance with the laws of Commonwealth of Virginia, US without regard to its conflict of law provisions. Venue shall be in the courts of Virginia.

Binding Effect

Except as otherwise provided herein, this Agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. Neither this Agreement nor Subscriber's Digital Certificate shall be assignable by LRA or Subscriber. Any such purported assignment or delegation shall be void and of no effect and shall permit GlobalSign to terminate this Agreement.

Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto.

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS AGREEMENT WHICH PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES OR EXCLUSION OF DAMAGES IS INTENDED BY THE PARTIES TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND TO BE ENFORCED AS SUCH.

Entire Agreement

This Agreement constitutes the entire understanding and agreement of the parties hereto with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements or understandings between the parties related to the Service.
GlobalSign ePKI Service Agreement Version 1.1

Trade Names, Logos.

By reason of this Agreement or the performance hereof, LRA and GlobalSign shall not acquire any rights of any kind in any trademark, brand name, logo or product designation of the other party and shall not make any use of the same for any reason except as otherwise authorised in writing by the party which owns all rights to such trademarks, trade names, logos or product designation.

10. NOTICE

LRA shall notify GlobalSign through any of our international offices as listed on http://www.globalsign.com/company/contact.htm immediately in case of any error in the Digital Certificate. Without notification from LRA or Subscriber within 7 days from receipt of the Digital Certificate, the Digital Certificate shall be deemed accepted.

Agreed and Accepted:

GlobalSign, Inc.                          Company

By:                                          By:

______________________________              ________________________________

Print Name:                                 Print Name:

______________________________              ________________________________

Title:                                      Title:

______________________________              ________________________________

Date:                                       Date:

______________________________              ________________________________

Schedule B
GlobalSign ePKI Service Agreement Version 1.1

**Fees and Payment Information**

Company may cancel a Certificate or request revocation of a Certificate at any time, but Company will not be entitled to any refund, prorated or otherwise, for such cancellations or revocations unless cancellation or revocation is requested within 7 days of issuance of the Certificate.

Company agrees to pay GlobalSign the following fees for Certificates that are ordered and approved by the Certificate Administrator. Requests for Certificates that are denied will not be charged. Company agrees that GlobalSign may revoke or cancel Certificates previously provided by GlobalSign in the event of non-payment by Company. Fees are stated in U.S. dollars.

**Initial Order:**

On the Effective Date, Company agrees to purchase the following PersonalSign and/or DocumentSign Certificates where applicable in the quantities at the price(s) indicated below:

<table>
<thead>
<tr>
<th>Block Size</th>
<th>Validity Period of Certificates (1, 2, or 3 Yr)</th>
<th>Certificate Type</th>
<th>Price per block</th>
<th>Number of Certificate Administrators Included</th>
<th>Net Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>500* Annually</td>
<td>1 Year Validity</td>
<td>PersonalSign Digital ID’s</td>
<td>$12,500.00 Annually</td>
<td>Unlimited</td>
<td>$12,500.00 Annually</td>
</tr>
</tbody>
</table>

*Additional 10% (50) of annual quantity added automatically.

**Net Block Price (from table above):** $12,500.00 annually

**Fee for Additional Certificate Administrators: Not applicable** (0 x $100 per Certificate Administrator per year)

**Initial Order:** $37,500.00 **

**Support Fees:** $0, Standard

(0% of list price of Initial Order)

**Total Initial Order: $37,500.00** *(list price for Initial Order + Applicable Support Fee)*

**Special Provisions:** Three (3) Years Fees due at time of order per customer request. Annual five hundred (500) certificate licenses loaded annually on agreement renewal date.
Subsequent Orders:

During the Initial Term, Company may continue to purchase Certificates in block purchases in the quantities at the prices indicated below. Company will only be entitled to the discounted price for a specific block size if the Certificates are all purchased and paid for at the same time as a single block. The purchase of blocks at one time will not be counted toward the purchase of additional blocks at a later time for the purpose of obtaining a lower price per block for the later purchase.

<table>
<thead>
<tr>
<th>Block Size</th>
<th>Validity Period of Certificates (1, 2, or 3 Yr)</th>
<th>Certificate Type</th>
<th>Price per block</th>
<th>Number of Certificate Administrators Included</th>
<th>Net Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>1 Year Validity</td>
<td>PersonalSign Digital ID’s</td>
<td>$12,500</td>
<td>Unlimited</td>
<td>$12,500.00</td>
</tr>
</tbody>
</table>

During the Initial Term, Company may purchase additional domain names and/or Certificate Administrators at the prices indicated below:

<table>
<thead>
<tr>
<th>Additional Certificate Administrators</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No Charge</td>
<td></td>
</tr>
</tbody>
</table>
Billing Contact Information:

Name: ________________________  Phone: ________________________
Address: ________________________  Fax: ________________________
______________________________  Email: ________________________

GlobalSign will invoice Company for the Initial Order on the Effective Date. Subsequent Orders will be invoiced at the time the order is placed. All payments are due and payable net thirty (30) days from Company’s receipt of invoice. Company agrees to pay interest at the rate of 1.5 percent per month or the maximum legal rate on all amounts over seven (7) days overdue. Company will pay any applicable taxes, fees and similar governmental charges related to the execution or performance of this Agreement, other than applicable income taxes imposed on GlobalSign related to its receipt of payments from Company.
Attachment G

Pricing and Information for Managed SSL and ePKI,

for Virginia Non-Profit Cooperative Use Only

Request for Proposal 648260
### Product Description

<table>
<thead>
<tr>
<th>Product Description</th>
<th>List Price</th>
<th>Discounted Price, 1 year</th>
<th>Discounted Price, 2 years</th>
<th>Discounted Price, 3 years</th>
<th>Discounted Price, 4 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational SSL</td>
<td>$349</td>
<td>$105</td>
<td>$189</td>
<td>$259</td>
<td>$315</td>
</tr>
<tr>
<td>Wild Card SSL</td>
<td>$949</td>
<td>$286</td>
<td>$514</td>
<td>$703</td>
<td>$857</td>
</tr>
<tr>
<td>Extended SSL</td>
<td>$899</td>
<td>$553</td>
<td>$860</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### PersonalSign 2 Pro for Individuals 1 Year

<table>
<thead>
<tr>
<th>Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 5 pack</td>
<td>$440</td>
<td>$361</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 10 pack</td>
<td>$855</td>
<td>$701</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 25 pack</td>
<td>$2,025</td>
<td>$1,661</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 50 pack</td>
<td>$3,825</td>
<td>$3,137</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 100 pack</td>
<td>$5,000</td>
<td>$4,100</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 250 pack</td>
<td>$8,500</td>
<td>$6,970</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 500 pack</td>
<td>$12,500</td>
<td>$10,250</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 1 yr 1,000 pack</td>
<td>$15,000</td>
<td>$12,300</td>
</tr>
</tbody>
</table>

### PersonalSign 2 Pro for Individuals 2 Year

<table>
<thead>
<tr>
<th>Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 5 pack</td>
<td>$590</td>
<td>$484</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 10 pack</td>
<td>$1,140</td>
<td>$935</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 25 pack</td>
<td>$2,690</td>
<td>$2,206</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 50 pack</td>
<td>$5,085</td>
<td>$4,170</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 100 pack</td>
<td>$6,650</td>
<td>$5,453</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 250 pack</td>
<td>$11,305</td>
<td>$9,270</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 500 pack</td>
<td>$16,630</td>
<td>$13,637</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 2 yr 1,000 pack</td>
<td>$19,950</td>
<td>$16,359</td>
</tr>
</tbody>
</table>

### PersonalSign 2 Pro for Individuals 3 Year

<table>
<thead>
<tr>
<th>Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 5 pack</td>
<td>$740</td>
<td>$607</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 10 pack</td>
<td>$1,430</td>
<td>$1,173</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 25 pack</td>
<td>$3,380</td>
<td>$2,772</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 50 pack</td>
<td>$6,385</td>
<td>$5,236</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 100 pack</td>
<td>$8,350</td>
<td>$6,847</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 250 pack</td>
<td>$14,195</td>
<td>$11,640</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 500 pack</td>
<td>$20,880</td>
<td>$17,122</td>
</tr>
<tr>
<td>Enterprise PKI Lite For Personal Digital ID 3 yr 1,000 pack</td>
<td>$25,050</td>
<td>$20,541</td>
</tr>
</tbody>
</table>
### Adobe CDS (DocumentSign for Adobe) Products

#### Adobe CDS Tokens for Departments Low Volume (2000 signatures per year)

<table>
<thead>
<tr>
<th>Product Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Low Volume 1 year</td>
<td>$595</td>
<td>$524</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Low Volume 2 year</td>
<td>$995</td>
<td>$876</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Low Volume 3 year</td>
<td>$1,339</td>
<td>$1,178</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Low Volume 4 year</td>
<td>$1,549</td>
<td>$1,363</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Low Volume 5 year</td>
<td>$1,639</td>
<td>$1,442</td>
</tr>
</tbody>
</table>

#### Adobe CDS Tokens for Department Med. Volume (5000 signatures per year)

<table>
<thead>
<tr>
<th>Product Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Medium Volume 1 year</td>
<td>$949</td>
<td>$835</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Medium Volume 2 year</td>
<td>$1,619</td>
<td>$1,425</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Medium Volume 3 year</td>
<td>$2,139</td>
<td>$1,882</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Medium Volume 4 year</td>
<td>$2,469</td>
<td>$2,173</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Department&gt;USB&gt;Medium Volume 5 year</td>
<td>$2,599</td>
<td>$2,287</td>
</tr>
</tbody>
</table>

#### Adobe CDS Tokens for individuals Low Volume (500 signatures per year)

<table>
<thead>
<tr>
<th>Product Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>DocumentSign for Adobe PDF Personal Pro &gt;USB &gt;Low 1 year</td>
<td>$395</td>
<td>$348</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Personal Pro &gt;USB &gt;Low 2 year</td>
<td>$669</td>
<td>$589</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Personal Pro &gt;USB &gt;Low 3 year</td>
<td>$899</td>
<td>$791</td>
</tr>
</tbody>
</table>

#### Adobe CDS Tokens for individuals Medium Volume (1,500 Signatures per year)

<table>
<thead>
<tr>
<th>Product Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>DocumentSign for Adobe PDF Personal Pro &gt;USB &gt;Medium 1 year</td>
<td>$525</td>
<td>$462</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Personal Pro &gt;USB &gt;Medium 2 year</td>
<td>$899</td>
<td>$791</td>
</tr>
<tr>
<td>DocumentSign for Adobe PDF Personal Pro &gt;USB &gt;Medium 3 year</td>
<td>$1,189</td>
<td>$1,046</td>
</tr>
</tbody>
</table>

#### Enterprise PKI Adobe CDS Tokens for Department 1 Year Packs

<table>
<thead>
<tr>
<th>Product Description</th>
<th>List Price</th>
<th>Discount Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 1 yr 5 pack</td>
<td>$4,035</td>
<td>$3,551</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 1 yr 10 pack</td>
<td>$7,590</td>
<td>$6,679</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 1 yr 25 pack</td>
<td>$17,795</td>
<td>$15,660</td>
</tr>
</tbody>
</table>
### Enterprise PKI Adobe CDS Tokens for Department 2 Year Packs

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Price 1</th>
<th>Price 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 2 yr 5 pack</td>
<td></td>
<td>$7,260</td>
<td>$6,389</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 2 yr 25 pack</td>
<td></td>
<td>$32,030</td>
<td>$28,186</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 2 yr 10 pack</td>
<td></td>
<td>$13,665</td>
<td>$12,025</td>
</tr>
</tbody>
</table>

### Enterprise PKI Adobe CDS Tokens for Department 3 Year Packs

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Price 1</th>
<th>Price 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 3 yr 5 pack</td>
<td></td>
<td>$9,920</td>
<td>$8,730</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 3 yr 25 pack</td>
<td></td>
<td>$43,770</td>
<td>$38,518</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 3 yr 10 pack</td>
<td></td>
<td>$18,675</td>
<td>$16,434</td>
</tr>
</tbody>
</table>

### Enterprise PKI Adobe CDS Tokens for Individuals 1 Year Packs

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Price 1</th>
<th>Price 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 1 yr 5 pack</td>
<td></td>
<td>$2,230</td>
<td>$1,962</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 1 yr 10 pack</td>
<td></td>
<td>$4,200</td>
<td>$3,696</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 1 yr 25 pack</td>
<td></td>
<td>$9,845</td>
<td>$8,664</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 1 yr 50 pack</td>
<td></td>
<td>$18,375</td>
<td>$16,170</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 1 yr 100 pack</td>
<td></td>
<td>$34,125</td>
<td>$30,030</td>
</tr>
</tbody>
</table>

### Enterprise PKI Adobe CDS Tokens for Individuals 2 Year Packs

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Price 1</th>
<th>Price 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 2 yr 5 pack</td>
<td></td>
<td>$4,015</td>
<td>$3,533</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 2 yr 10 pack</td>
<td></td>
<td>$7,560</td>
<td>$6,653</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 2 yr 25 pack</td>
<td></td>
<td>$17,720</td>
<td>$15,594</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 1 yr 50 pack</td>
<td></td>
<td>$18,375</td>
<td>$16,170</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 2 yr 100 pack</td>
<td></td>
<td>$61,425</td>
<td>$54,054</td>
</tr>
</tbody>
</table>

### Enterprise PKI Adobe CDS Tokens for Individuals 3 Year Packs

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Price 1</th>
<th>Price 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 3 yr 5 pack</td>
<td></td>
<td>$5,490</td>
<td>$4,831</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 3 yr 10 pack</td>
<td></td>
<td>$10,330</td>
<td>$9,090</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 3 yr 25 pack</td>
<td></td>
<td>$24,215</td>
<td>$21,309</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 3 yr 50 pack</td>
<td></td>
<td>$45,200</td>
<td>$39,776</td>
</tr>
<tr>
<td>Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 3 yr 100 pack</td>
<td></td>
<td>$83,950</td>
<td>$73,876</td>
</tr>
</tbody>
</table>
Certified Document Services (CDS) provides a cost effective PDF digital signing solution.

**How it works...**

Following a thorough verification of both the individual and / or the organization requesting a DocumentSign digital ID, GlobalSign will issue the digital ID in the form of a Digital Certificate, securely stored and protected on a SafeNet® hardware cryptographic device. Authors can digitally certify PDFs (desktop and server-based solutions available) using certificates “chained” up to the trusted Adobe Root. Approval signatures may also be applied at a later stage. Recipients simply need to open the document using the Adobe free reader to instantly verify the authenticity and integrity of the document. Adobe’s simple to interpret “Blue Ribbon, Question Mark, and Red X” trust messaging allows even novice users an easy to understand method to determine if the document is from a legitimate source.

By clicking on the signature properties, recipients can view additional information, such as signing certificate details including information about the certificate policy, signer’s contact information, Certificate Revocation information via embedded Certificate Revocation List (CRL) details and time-stamping information which are the foundation for strong authentication, long term validity, data-integrity and non-repudiation of the signature.

Higher Education providers no longer need to fear their brand and reputation are at risk in the event a legitimately authored PDF is maliciously modified and falsely re-circulated under their name.

**Trends in Higher Education**

Over 22,000 applications were received by Harvard University to the class of 2010 with about 2,100 students being admitted. Imagine the effort to flush through tens of thousands of applications just to locate the top 10% of candidates? Each of the 22,000 applicants will need to be notified of their acceptance or refusal. Now envision the number of notifications that take place every year as thousands of Admission Offices tackle the very same issue of secure and timely document delivery. There is no doubt, that Higher Education is a paper-intensive, high transaction industry that produces vast amounts of highly sensitive documents. Specific examples include:

- Diplomas
- Certifications
- Transcripts
- Admission letters
- Financial aid notifications

**Demand for Transcripts**

Many universities and college registrars’ offices have been inundated with transcript requests creating a mountain of paper work, significant courier expensive, and soaring costs surrounding the labor intensive processing associated with creating authentic transcripts. Often alumni request transcripts in an urgent attempt to meet an employment requirement or to make a graduated school application deadline. With the advent of diploma mills, where schools brand name can be easily harmed via falsified transcripts and diplomas, Registrars are looking for ways to meet the demand for the secure delivery of transcripts in days, not weeks, while at the same time protecting the school brand name. Automating the process is relatively easy, but how can schools automate without compromising both their and alumni security?

**Certified Document Services**

Certified Document Services (CDS) is one of the services enabled by the Adobe root certificate authority and was introduced into the Acrobat product offering with version 6.0. CDS enables document authors to sign Portable Document Format (PDF) files, using standard digital certificates, which automatically validate when authors are using free Adobe® Reader® software. No additional client software or configuration is required. CDS was designed to enable organizations and individuals who publish high-value documents to large and disparate recipient groups to increase the assurance level that the document’s integrity and authenticity are preserved. By adding a CDS signature to a PDF file, document authors can increase this assurance level without requiring recipients to deploy additional software. When a recipient opens a transcript with the free Adobe Acrobat Reader, the Reader displays a visible verification sign. That means the academic institution’s identity was verified by a trusted organization and that the transcript has not been altered.

**Remember!** For the highest assurances of who created a document, look for the Blue Security Bar and Blue Rosette.
DocumentSign™ - Who else benefits?

Digital IDs for the Adobe PDF Platform: Certified Document Services (CDS)

eNotarization:
CDS digital IDs used by Notaries to certify (i.e. Notarize) PDFs are only provided by authorized CDS participants like GlobalSign, and are delivered and controlled under a strict Certificate Policy created by Adobe Systems Inc. In this respect, the authenticity of the signature can be verified automatically by some 700+ Million copies of Adobe’s PDF reader in use around the world. This simple fact removes the myriad of issues created when individual countries, organisations and individuals try to control individual trust models across international boundaries where the recipient’s software cannot be guaranteed.

Healthcare:
The New England Journal of Medicine, 2004, reports “paperwork represent 31% of all health care costs”. CDS can help relieve the burden on physicians surrounding cumbersome processes involving patient paper-work while being part of a CFR 21 Part 11 compliant solution.

Engineering, Architectural, & Construction
(AEC) professionals benefit from CDS with faster design collaboration, more efficient and less expensive electronic document storage, and stronger protection via tamper evident easy to understand trust symbols. Now engineering drawings and product documentation can be exchanged among customers, partners, contractors, and building departments with the assurances both parties require. CDS meets or exceeds most Federal and State electronic signature guidelines with minimal impact to the author as well as an easy to understand and highly trusted experience for the recipient.

Government
CDS supports both local and federal government initiatives including the Government Paperwork elimination Act helping reduce costs, enhance citizen accessibility to government information, and reduce unnecessary environmental waste while at the same time providing high assurances to its citizens that the information is legitimate.

Financial Services
Industry best practices coupled with government imposed regulation like Sarbanes-Oxley make CDS an attractive option as a thorough audit of the signature properties are embedded in the document itself. Well after the Digital ID expires, the signature characteristics are preserved providing relying parties strong authentication of the author, whether the content is still intact, and the exact date and time of the transaction.

The Notarial and Legal professions
CDS provides unequalled support of trusted documents in multiple languages. This alone facilitates increased cross border transactions as both sides are able to interrogate the authenticity of a document in their local language; the ideal solution for e-Notarization.

Other uses:
All sectors can benefit from publishing external facing marketing materials, supplier e-agreements, and internal high stakes documents that have been certified with DocumentSign Digital IDs. The Adobe CDS program protects the organization’s brand name from malicious alteration of company generated e-documents.

© 2009 GlobalSign – The GlobalSign logo is a registered trademark of GlobalSign KK. The Adobe symbol is a registered trademark of Adobe Systems Incorporated. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.
**What is ePKI?**
ePKI is a managed service model that provides Enterprise administrators full control of the digital certificates needed to secure their sensitive e-mail, documents, and networks. Enterprises can usually establish an ePKI service within only five days, allowing one or more administrator the ability to manage the full life-cycle of either Windows or Adobe publically trusted digital IDs. Each ID will display the fully vetted organization name in conjunction with the individual or in some cases, providing legally binding digital signatures displaying your Organization’s legal name.

**What to use ePKI for?**
The ePKI model enables complete management of digital certificates for digital signing, e-mail signatures, encryption, and authentication.

**ePKI Managed Solution**
ePKI administrators may establish one or more certificate profiles providing the flexibility that may be needed to support varying business unit or application needs. All profiles can be centrally managed and provide the following functions:

- Zero footprint application through an easy to use Web browser interface
- Immediate certificate issuance to employees, customers, business partners, and devices.
- Cost Effective – no hidden fees – simply purchase packs of certificates that include 10% free certificates used to cover employee attrition and support.
- Instantly trusted and verified signatures in most popular applications via ubiquitous digital credentials
  - **PersonalSign Pro class 2** - certificates available for Windows publically trusted certificates for secure Microsoft Office Suite documents and Secure E-mail
  - **Documentsign** - for secure Adobe PDF documents - Certified Document Services (CDS)

**Additional Features & Benefits**

1. **One stop PKI-shopping**: ePKI is part of GlobalSign’s Certificate Center (GCC) portal allowing Administrators a single portal to acquire all types of GlobalSign digital IDs including:
   - SSL Certificates
   - Code Signing Certificates
   - Client Certificates

2. **Unlimited Administrators**: allowing the Enterprise to meet the “around the clock” needs of mission critical applications

3. **Robust Reporting**: easy search capabilities provide ePKI administrators a method to review the status of issued certificate and pending requests.

4. **Public ordering URLs**: provides support for “Open enrollments”

5. **Company Branding**: via customized e-mail templates allowing customized messages to your end users.

6. **Revocation and CRL certificates**: ePKI administrators can revoke certificates from their ePKI portal. Revoked certificates will be automatically added to the Certificate Revocation Lists (CRLs).

**Learn More**

**Certificate Types:**
For more information about PersonalSign Digital IDs:

For more information about DocumentSign digital IDs for Adobe PDF:

**Sales@GlobalSign.com**

GlobalSign, Inc.
2 International Drive, Suite 105
Portsmouth, New Hampshire 03801
TEL: 1-877-SSL-GLOBAL FAX: 603-570-7059
http://www.globalsign.com

As e-commerce expands from intercompany electronic exchange to partners, customers, and suppliers, outside of the trusted network, Enterprise’s ability to secure critical data, protect company IP, and meet government and industry regulations must keep pace with the speed of data being exchanged across unsecured networks.
GlobalSign SSL Managed Service™
Manage Multiple Enterprise Level SSL Certificates

Manage the complete lifecycle of enterprise level SSL Certificates through GlobalSign's SSL Managed Service, including issuing, reissuing, renewing, revoking and billing management for multiple SSL Certificates across numerous departments and office locations.

SSL Managed Service provides the ability to quickly; simply and conveniently manage GlobalSign's leading SSL Certificates through a web based management interface designed around enterprise specific security requirements, and will help organizations significantly reduce the budget, time and management costs of using SSL.

The Importance of Security within Today's Economy
As e-commerce transactions increase and organizations bring more services online, security plays an increasingly critical role within organizations of all sizes. SSL, the transaction layer security technology, is now integral to every company's security policy - online transactions, data transfer, network traffic, and digital communications require a secure platform from which to be delivered / processed. From the consumer perspective, digital-age threats such as phishing attacks and identity theft continue to increase and online customers now expect an ever higher level of security as standard. Undeniably, SSL Certificates are now an essential operational requirement for all organizations that have an online presence.

Minimise PKI Costs with GlobalSign’s PKI Service
This growing requirement for increased security can impact an organization's budget, time and management resources. For example, implementing a successful Public Key Infrastructure (PKI) solution requires new investment in software, hardware and will invariably require sufficient IT and administrative capacity to implement the solution effectively. For these reasons, most organizations opt for an outsourced, fully managed Certificate Services provider where costs can be significantly reduced, but control is kept firmly with the organization.

Through global investment in technology, staff and understanding of compliancy and regulation, GlobalSign has built an incredibly robust and comprehensive PKI service designed for effective management of SSL Certificates. GlobalSign’s SSL Managed Service enables control of SSL Certificate issuance and management, without the need to invest in expensive infrastructure and expert staff. It is highly cost-effective, scalable, reliable, immediately deployable, and being a fully managed web based service, incredibly fast and simple to use.

Cost Associated with SSL Certificate Management
Managing multiple SSL Certificates can be costly and time-consuming. For traditionally vetted, high assurance SSL Certificates, organizations need to go through extensive registration and verification processes with the SSL Provider for each and every SSL Certificate purchased. Administrators must also keep track of their Certificate's differing expiration dates. On a yearly basis, administrators can spend many costly man-days just buying and renewing SSL Certificates.

Time and costs associated with managing multiple certs
- No automatic "snapshot" or view exists that details the number of Certificates
- Certificates expire at different times, potentially exposing customers to dangerous "Certificate has expired" messages
- Corporate documents must be submitted over and over again
- Even though numerous SSL Certificates are purchased, no automatic discounts are received
- SSL budgetary requirements become difficult to determine when each department purchases ad hoc

http://www.globalsign.com
Why Choose GlobalSign's Fully Managed SSL Service?
SSL Managed Service from GlobalSign provides the ability to conveniently and quickly purchase GlobalSign's leading SSL Certificates through a web-based management interface. It alleviates costs, simplifies management, and optimizes efficiency of SSL Certificate delivery. This scalable, cost-effective solution can be used by the most distributed of organizations. One-time vetting means once vetted, users simply log into the web-based account (Software as a Service [SaaS]) model (or XML API) and issue, reissue, renew or revoke SSL Certificates on demand. Granular user privileges allow administrators to create roles for users to apply, approve or report on billing and SSL Certificate activity within the account. Plus, immediate discounts mean savings over purchasing SSL Certificates from multiple suppliers or via premium priced retail sites.

Managed SSL Service Benefits:
No Infrastructure or Personnel Overheads - GlobalSign runs the WebTrust certified Certification Authority (CA) and web-based management portal – the Enterprise Certificate Manager – peerless in its ease of use and functionality. Administrators simply log in and manage SSL Certificates online.

Complete Certificate Lifecycle Management – the organization controls the application issuance, reissuance, renewal and revocation of Certificates across many departments using the Enterprise Certificate Manager, plus has ability to customize all Certificates to start and expire within the same time period.

Pre-venting of Domains allows Instant Issuance – the organization no longer has to provide CA with company details for every Certificate issued. By using the Enterprise Certificate Manager, issuances can occur within minutes.

Certificate Discounts – GlobalSign charges no service fees and enables organizations to save considerable budget by purchasing in bulk or Pay As You Go, compared to buying SSL Certificates separately or from a GlobalSign competitor. Flexible options allow bulk (in packs of 10, 50 or 100, or fully customized quantities) and multi-year purchases.

Advanced Delegated Administration and Approval Based Model – administrators have the ability to create additional users within defined roles with appropriate privileges (e.g. IT Manager for Certificate management and Finance Manager for billing). Administrators and users with approval privileges can decide whether applications should be issued (with email alerts sent to approvers).

Public Ordering URL – when activated, the Public Ordering URL allows administrators to share, or post, an application link (e.g. on Intranets). Anybody can place an order for the Certificate via the link and the administrator is alerted to approve new applications.

Full Billing Management – the organization can view and download invoices and automatically create new downloadable “quotes” for internal authorization.

Comprehensive Reporting and Auditing Functions – detailed reports on spend, Certificates issued, upcoming renewals can be created.

XML Based API - allows full integration with the organization’s purchasing systems.

Dedicated Account Manager – provides localized comprehensive support via phone, email and web. The Account Manager can be contacted to discuss account or Certificate lifecycle management issues.

Premier Support Options – if added, organizations have access to a live dedicated support technician 24 hours a day, 7 days a week, 365 days a year, with a maximum response time of 20 minutes. GlobalSign prides itself on providing the industry’s highest level of customer service at all times.

The Benefits of an Industry Leading WebTrust Certified Certification Authority without the need to manage your own software, hardware and expert CA personnel. GlobalSign maintains an industry leading Certification Authority and associated Root Certificates. All the organization has to do is decide when to issue SSL Certificates.

Premier Support Levels
To meet stringent enterprise level SLAs GlobalSign can offer Premier Support, a service that provides around the clock access to a live dedicated support technician 24 hours a day, 7 days a week, 365 days a year with maximum response times of 20 minutes. A support technician is ready to assist with any aspect of account management or Certificate installation issues.

http://wwwglobalsign.com
SSL Certificate Benefits:

**Highly Trusted SSL** - supported by all popular browsers, mobile devices and applications (approx 99% ubiquity). Certificates are issued from GlobalSign's trusted root. A full list of compatible servers, browsers and mobile devices can be downloaded from the GlobalSign website. ([http://www.globalsign.com/resources/ssl_root_compatibility.pdf](http://www.globalsign.com/resources/ssl_root_compatibility.pdf)).

**Free SGC Security** - includes strong 128 bit step-up encryption to force weaker 40 bit browsers to step-up to stronger 128bit browsers or 256 bit enabling technology, improving overall SSL security. SGC from other SSL Providers features at a premium price, but is included free of charge with every GlobalSign SSL Certificate.

**Free SSL Installation Healthcheck** – GlobalSign ensures SSL Certificates are installed and working correctly by checking the server ability, SSL Certificate installation, common error checking and trust enhancing Secure Site Seal installation.

**Free Server Licenses** – 3 server licenses issued with each SSL Certificate to enable organizations to easily secure primary server, secondary or backup server and load balancer without facing additional costs. Other SSL Providers typically issue one license and charge premium prices for additional licenses.

**Custom Options** – add Wildcard SSL, Intranet names / hostnames, IP addresses as premium options. Wildcard SSL provides the ability to secure multiple websites on the same domain name by enabling a variable (rather than fixed) sub domain to be used; saving time, administration and money. If operating an Intranet, Subject Alternative Names (SAN's) can be specified within the Certificate to secure Intranet hostnames. Some organizations may require SSL Certificates to be issued to an IP address – this can be achieved with GlobalSign.

**Secure Both www and non-www Sites with Single Certificate for No Additional Cost** - SSL Certificates are usually issued to a specific Fully Qualified Domain Name (FQDN). To secure both www.domain.com and just domain.com for example, two separate Certificates would usually be required. But not with GlobalSign SSL – the only professional level SSL Certificate to include both forms of the domain name within the Certificate but without additional charges, new IP purchase or server configuration.

**Clickable Site Seal** – enables organizations to show a secure site and enhance trust and credibility of online presence. Easy to install on any web page, the Site Seal can be clicked to deliver a full website profile. The GlobalSign Site Seal will increase visitor trust, convert general visitors into paying customers and reduce the amount of abandoned shopping carts and uncompleted web forms.

**$250k Warranty** – the organization is protected by GlobalSign’s warranty underwritten by insurance.

About GlobalSign

Established in 1996, GlobalSign has been securing identities, websites and transactions as a worldwide digital certificate provider for over 10 years. Now part of the GMO Internet Inc. group (listed on the Tokyo Stock Exchange TSE: 9449), GlobalSign comprizes of considerable expertise and know-how in the online security industry.

As a WebTrust accredited Certificate Authority, GlobalSign offers publicly trusted SSL Certificates, Code Signing Certificates, and Digital IDs, issuing over 1.4 million digital Certificates to individuals, websites and machines. In total over 20 million digital Certificates rely on the security the GlobalSign root, technology and infrastructure provide. GlobalSign is also a member of the CA/B Forum and Anti-Phishing Working Group – a show of its dedication to improving the security for both consumers and businesses.

GlobalSign prides itself on high level customer service, with localized sales and technical support expertise available throughout US, Europe (UK and Belgium) and Asia (Japan and China), available in a number of languages via phone, email and web. As a highly reputable and trusted digital certificate provider, GlobalSign provides Certificates for global enterprises such as BMW, ING Bank, Vodafone, Fortis and Gocompare.com.

LEARN MORE

Contact GlobalSign today to discuss how to manage SSL Certificates more efficiently using GlobalSign's SSL Managed Service. Email: sales@globalsign.com

GlobalSign Inc.
2 International Drive, Suite 330
Portsmouth, New Hampshire 03801
TEL: 1-877-SSLGLOBAL  FAX: 603-570-7059
http://www.globalsign.com
Attachment H

Summary of Negotiations

Request for Proposal 648260
RFP 648260 - - Summary of Negotiations

The following statements are submitted as an attachment to the RFP 648260 proposal submitted by GMO GlobalSign Inc. that may clarify/modify or supersede the RFP 648260 proposal, and shall be part of Contract UCP-.

1) **Contract Participation - Cooperative Use**
   Contract UCP-TS-C01-11 is available for use by Virginia Tech and for cooperative use by only Virginia non-profit agencies, and only if authorized by the Contractor. See Contract Attachment A, RFP Section IV – Contract Participation for details.

2) **Test Period**
   Prior to production implementation both parties shall participate in a 30-day test implementation without incurring financial obligation. Upon written acceptance of testing by both parties production implementation will begin immediately and the Contractor may submit an invoice for implementation (one-time setup/key ceremony fees) and first year annual license fee.
Attachment I

CONFIDENTIAL – Revised Registration Form with Pricing,
for Virginia Tech Only

Request for Proposal 648260
Contract UCP-TS-C01-11, Attachment I intentionally left blank, as the contents are Confidential.