AlphaSSL CA
Certification Practice Statement

Date: May 9 2007

Version: v.1.1

Table of Contents

Document History

Document Change Control

Version	Release Date	Author	Status + Description
V1.0	1 May 2007	Johan Sys	Initial Version
V1.1	9 May 2007	Johan Sys	Administrative update

Acknowledgments

This AlphaSSL CA CPS endorses in whole or in part the following industry standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- The ISO 1-7799 standard on security and infrastructure

1. Introduction

This Certification Practice Statement (CPS) of the AlphaSSL Certification Authority (hereinafter, AlphaSSL CA) applies to the services of the AlphaSSL CA that are associated with the issuance of and management of digital certificates. This CPS can be found on the AlphaSSL CA repository at: http://www.AlphaSSL.com/repository. This CPS may be updated from time to time.

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 AlphaSSL CA.

1.1 Overview

This CPS applies to the specific domain of the AlphaSSL CA. The purpose of this CPS is to present the AlphaSSL practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to AlphaSSL's own and industry requirements pursuant to the standards set out above. The certificate type addressed in this CPS is the following : AlphaSSL certificate. This certificate can be used to authenticate web resources, such as servers and other devices.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of AlphaSSL certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved including the AlphaSSL CA, AlphaSSL 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 AlphaSSL CA under a managed Brand Root.
A subscriber or relying party of a AlphaSSL CA certificate must refer to the AlphaSSL CPS in order to establish Trust. It is also essential to establish the trustworthiness of the entire certificate chain of the AlphaSSL certificate hierarchy, including the Brand Root.

A full list of accreditation and recognition of service is available upon request.

This CPS is made available on-line under https://www.alphassl.com/repository.

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

1.2 AlphaSSL Certificate types

This part describes the public AlphaSSL products.

1.2.1 Server Certificates

AlphaSSL certificates can be used for web based transactions. It 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 AlphaSSL CA, only the ownership of the domain or the right of the requester to apply for a domain as represented in the Domain Name System.

1.2.2 Acceptable Subscriber Names

For publication in its certificates AlphaSSL CA accepts subscriber names that are meaningful and can be authenticated as required.

1.2.2.1 Pseudonyms

AlphaSSL CA 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.

1.2.3 Registration procedures

AlphaSSL CA reserves the right to update registration procedures and subscriber submitted data to improve the identification and registration process.

1.3 AlphaSSL certificates

1.3.1 General

AlphaSSL certificates are meant for secure communication with for example a web-site through an SSL or TLS link.

The applicant is an individual or organization that has an Internet Server such as a website. AlphaSSL certificates are used to assure a confidential communication with the Internet Server.

AlphaSSL certificates validity period is between one and five years.
AlphaSSL certificates are issued to entities and individuals who own a domain name, or have the right to request a AlphaSSL certificate for a specific domain.

1.3.2 Certificate Request

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 AlphaSSL CA. Additional documentation in support of the application may be required so that AlphaSSL CA 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 AlphaSSL CA the additional documentation. Upon verification of ownership or right to use of the domain name, AlphaSSL CA issues the certificate and sends a notice to the

applicant. The applicant downloads and installs the certificate on the server. The applicant must notify AlphaSSL CA 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.

1.3.3 Content

Typical information published on a AlphaSSL certificate includes the following elements

- Applicant's domain name
- Applicant's public key
- Issuing certification authority (AlphaSSL CA)
- AlphaSSL electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.3.4 Information Submitted to verify ownership or right to use of the Domain name

The applicant must provide contact details to AlphaSSL CA and underwrite those by click-through process. AlphaSSL CA has the right to request a signed registration form or a signed subscriber agreement. AlphaSSL CA has the right to request proof of the ownership of the domain name or can ask the owner of the domain name to validate the request of the applicant.

1.3.5 Time to Confirm Submitted Data

AlphaSSL CA makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. While AlphaSSL certificates are typically issued within minutes, up to 1 to 3 working days might be required for proper verification.

1.3.6 Issuing Procedure

The issuing procedure for a AlphaSSL 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 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 AlphaSSL CA automatically.
6 AlphaSSL CA 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 and independent verification through telephone.
7 AlphaSSL CA may positively verify the applicant.
8 AlphaSSL CA may issue the certificate to the applicant.
9 AlphaSSL CA publishes the issued certificate in online database
10 Renewal: allowed

11 Revocation: allowed

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

1.3.7 Limited Warranty

AlphaSSL accepts liability up to USD 1000 per loss due to a false domain name (lack of ownership or lack of right to use domain) in a certificate issued following the CPS.

1.3.8 Relevant AlphaSSL Documents

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

1 AlphaSSL CPS
2 Subscriber Agreement

1.4 Certificate usages

Certain limitations apply to the use of AlphaSSL certificates. An AlphaSSL certificate can only be used for authentication of a remote domain name and webservice and encryption (confidentiality) of the communication channel.

Other uses of AlphaSSL certificates are not supported by this CPS.

1.5 Document Name and Identification

AlphaSSL ensures compliance of its certificates with the requirements and assertions of this CPS.

1.6 PKI participants

The AlphaSSL CA makes its services available to AlphaSSL certificate subscribers. These subscribers include without limitation entities that uses the AlphaSSL certificates for the purposes of:

- Authentication (digital signature)
- Encryption

1.6.1 AlphaSSL Certification Authority

A Certification Authority, such as AlphaSSL CA, 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 AlphaSSL CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates.

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

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

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

- Issuance
- Revocation
- Renewal
- Status validation

1.6.1.1 AlphaSSL CA outsource agent

Through an outsource agent, AlphaSSL CA operates a secure facility in order to deliver CA services including the issuance, revocation, renewal and status validation of AlphaSSL CA certificates. The AlphaSSL outsource agent operates a service to AlphaSSL CA on the basis of a service agreement. The scope of the service is the support in certificate management. The AlphaSSL outsource agent warrants designated services and service levels that meet those required by AlphaSSL CA. The AlphaSSL outsource agent carries out tasks associated with the administration of services and certificates on behalf of AlphaSSL CA.

1.6.1.2 Role of AlphaSSL CA

AlphaSSL CA operates 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 that operate under agreement with and within the conditions laid out by AlphaSSL CA.

1.6.2 Subscribers

Subscribers of AlphaSSL services are natural persons that successfully apply for a certificate. Subscribers are parties that have ultimate authority over the private key corresponding to the public key that is listed in a subject certificate.

Natural persons that are subscribers typically hold a valid identification document, such as an identity card, passport or equivalent, which might be used as credential in order to issue AlphaSSL certificates.

Additional credentials are required as explained on the online process for the application for a certificate.

1.6.3 Relying Parties

Relying parties are natural 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.

To verify the validity of a digital certificate, relying parties must always refer to AlphaSSL CA revocation information, currently a Certificate Revocation List (CRL). Certificate validation takes place prior to relying on information featured in a certificate. Relying parties meet specific obligations as described in this CPS.

1.7 Certificate use

Certain limitations apply to the use of AlphaSSL CA certificates.

1.7.1 Appropriate certificate usage

AlphaSSL certificates can be used for public domain transactions that require:

- Authentication and
- Confidentiality

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

1.7.2 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.

1.7.3 Certificate extensions

AlphaSSL CA issues certificates that might contain extensions defined by the X.509 v3 standard as well as any other formats including those used by Microsoft and Netscape.

AlphaSSL CA 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.

1.7.4 Critical Extensions

AlphaSSL CA 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.

1.8 Policy Administration

The Policy Managing Authority of the AlphaSSL CA manages this AlphaSSL CPS. The AlphaSSL CA registers, observes the maintenance, and interprets this CPS. The AlphaSSL CA makes available the operational conditions prevailing in the life-cycle management of AlphaSSL certificates.

1.8.1 Scope

AlphaSSL 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 CPS.

1.8.2 AlphaSSL Policy Management Authority

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

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

1.8.3 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the AlphaSSL Policy Management Authority, that CPS is published in the AlphaSSL online Repository at https://www.alphassl.com/repository.

AlphaSSL CA publishes a notice of such updates on its public web site at http://www.alphassl.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 AlphaSSL CPS.

AlphaSSL CA publishes on its web site at least the two latest versions of its CPS.

1.8.4 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

1.9 Definitions and acronyms

A list of definitions can be found at the end of this CPS.

2. Publication and Repository Responsibilities

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

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

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

AlphaSSL CA 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 AlphaSSL CA adheres to, such as Web Trust for CAs..

3. Identification and Authentication

AlphaSSL CA maintain appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

AlphaSSL CA authenticate the requests of parties wishing to revoke certificates under this policy.

3.1 Initial Identity Validation

The identification of the applicant for a certificate is carried out according to a documented procedure.

For the identification and authentication procedures of the initial subscriber registration, AlphaSSL CA might rely on such resources as third party databases.

3.2 Subscriber registration process

AlphaSSL CA ensures that:

- Subscribers of certificates are properly identified and authenticated
- Subscriber certificate requests are complete, accurate and duly authorized.

In particular:

- AlphaSSL CA provides notice to the applicant through its web site at www.alphassl.com and the dedicated policy framework published on its repository at www.alphassl.com/repository.
- Before entering any contractual relationship with the subscriber, AlphaSSL CA makes available a subscriber agreement, which the applicant must approve prior to placing a request with AlphaSSL CA. This agreement can also be consulted in advance on AlphaSSL CA's repository at www.alphassl.com/repository.
- AlphaSSL CA maintains documented contractual relationships with all third party outsourced agents it uses to deliver certificates.

3.2.1 Documents used for subscriber registration

AlphaSSL CA typically verifies certificate request by appropriate means and on the basis of a documented procedure: the applicant must submit to AlphaSSL CA a registration form and a Subscriber Agreement, both accepted and agreed to through a click-through acceptance process.

AlphaSSL CA may prescribe additional identification proof in support of the verification of the applicant ownership or right to use of the domain.

3.2.2 Records for subscriber registration

AlphaSSL CA maintains records of the executed subscriber agreement and any material or documents that support the application which also include but are not limited to:

- AlphaSSL CA subscriber agreement as approved of, and executed by, the applicant.
- Consent to the keeping of a record by AlphaSSL 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.
- A specifically designed attribute that uniquely identifies the applicant within the context of the AlphaSSL CA.

The records identified above shall be kept for a period of no less than 2 years following the expiration of a certificate.

3.2.3 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests, AlphaSSL CA requires using an online authentication mechanism and/or a request addressed to the AlphaSSL CA.

4. Certificate Life-Cycle Operational Requirements

The following operational requirements apply to Certificate Life-Cycle.

All entities within the AlphaSSL domain including subscribers or other participants have a continuous duty to inform the AlphaSSL 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.

To carry out its tasks AlphaSSL may use third party agents for which AlphaSSL CA assumes responsibility.

Subscribers undergo an enrolment process that requires:
a. Filling out an application form.
b. Generating a key pair.
c. Delivering the generated public key corresponding to a private key to AlphaSSL CA.
d. Accepting the subscriber agreement.

The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the AlphaSSL CA. The subscriber agreement incorporates by reference this CPS.

In general, an online enrolment process will be sufficient, only as explicitly permitted by AlphaSSL CA.

4.1 Certificate Application Processing and issuance

AlphaSSL CA acts upon a AlphaSSL certificate application to validate the submitted domain. Subsequently, the application is either approved or rejected. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

For rejected applications of certificate requests, AlphaSSL CA notes the reason for rejecting the application.

Following issuance of the approved certificate, the AlphaSSL CA delivers the issued certificate to the subscriber directly or through an agent.

4.2 Certificate generation

With reference to the issuance and renewal of certificates, AlphaSSL CA 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..

- Certificate requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.

4.3 Certificate Acceptance

An issued AlphaSSL certificate is deemed accepted by the subscriber when no objection is received by AlphaSSL from the subscriber within 1 working day after receival. Any objection to accepting an issued certificate must explicitly be notified to the AlphaSSL CA. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

The AlphaSSL CA might posts the issued certificate on a repository (X.500 or LDAP). The AlphaSSL CA also reserves its right to notify the certificate issuance by the AlphaSSL CA to other entities.

4.4 Key Pair and Certificate Usage

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

4.4.1 Subscriber

The obligations of the subscriber include the following ones:

4.4.1.1Subscriber 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 AlphaSSL CA published in the AlphaSSL Repository.
2. Notifying the AlphaSSL CA of any changes in the information submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a AlphaSSL certificate when it becomes invalid.
4. Using a AlphaSSL 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.
7. Refraining from submitting to AlphaSSL CA or any AlphaSSL directory any material that contains statements that violate any law or the rights of any party.
8. Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a AlphaSSL certificate.
9. Refraining from tampering with a certificate.
10. Only using certificates for legal and authorised purposes in accordance with the CPS.
11. Refrain from using a certificate outside possible license restrictions imposed by AlphaSSL CA.

The Subscriber has all above stated duties towards the CA at all times.

4.4.1.2Subscriber 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.

4.4.1.3Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the AlphaSSL 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 AlphaSSL 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 AlphaSSL CA Repositories and web site may result in terminating the relationship between the AlphaSSL CA and the party.

4.4.2 Relying party

The duties of a relying party are as follows:

4.4.2.1Relying party duties

A party relying on a AlphaSSL certificate will:

- Validate a AlphaSSL certificate by using certificate status information (e.g. CRL) published by AlphaSSL CA.
- Trust a AlphaSSL 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 AlphaSSL certificate, only as it may be reasonable under the circumstances.
- Trust a certificate only if it has not been revoked.

4.4.2.2AlphaSSL CA Repository and Web site Conditions

Parties, including subscribers and relying parties, accessing the AlphaSSL CA Repository and web site agree with the provisions of this CPS and any other conditions of use that the AlphaSSL 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.
- Validating the status of a digital certificate before encrypting data using the public key included in a certificate
- Obtaining information published on the AlphaSSL CA web site.

4.5 Certificate Renewal

Subscribers may request the renewal of AlphaSSL certificates. To request the renewal of a AlphaSSL 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.

4.6 Certificate Revocation

AlphaSSL CA 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 or suspension 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.

The AlphaSSL CA revokes an AlphaSSL 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 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.

4.7 Certificate Status Services

The AlphaSSL CA makes available certificate status checking services including CRLs, and appropriate Web interfaces.

CRL
A CRL lists all revoked and suspended certificates during the application period. CRLs for the different products are available from http://crl.alphassl.com.

A CRL is issued each 3 hours.

4.8 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

4.9 Certificates Problem Reporting and Response Capability

In addition to certificate revocation, AlphaSSL CA provides Subscribers, Relying Parties, 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. AlphaSSL CA shall use reasonable efforts to provide a 24x7 capability to accept and acknowledge and respond to such reports.

5. Management, Operational, And Physical Controls

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

5.1 Physical Security Controls

The AlphaSSL CA implements physical controls on its own, leased or rented premises.

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

The AlphaSSL 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 AlphaSSL 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 AlphaSSL CA implements a partial off-site backup.

The sites of the AlphaSSL CA host the infrastructure to provide the AlphaSSL CA services. The AlphaSSL 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 AlphaSSL 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 AlphaSSL 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 AlphaSSL 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 AlphaSSL CA staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

The AlphaSSL CA ensures that all actions with respect to the AlphaSSL CA can be attributed to the system and the person of the CA that has performed the action.

The AlphaSSL CA implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

The AlphaSSL 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 AlphaSSL 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 AlphaSSL 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

AlphaSSL 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 AlphaSSL CA personnel.

5.3.8 Documentation for initial training and retraining

The AlphaSSL CA 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.

AlphaSSL CA implements the following controls:

AlphaSSL 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.

AlphaSSL 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 AlphaSSL CA 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

AlphaSSL CA keeps archives in a retrievable format.

AlphaSSL 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 AlphaSSL CA as appropriate.

The AlphaSSL 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 1 years after expiration of a certificate. Support documents can be electronically stored.

5.5.1 Types of records

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

5.5.2 Retention period

AlphaSSL 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 AlphaSSL CA archive collection system is internal.

5.5.5 Procedures to obtain and verify archive information

To obtain and verify archive information AlphaSSL CA maintains records under clear hierarchical control.

The AlphaSSL CA retains records in electronic or in paper-based format. The AlphaSSL CA may require 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 AlphaSSL CA may see fit.

The AlphaSSL CA may revise record retention terms as it might be required in order to comply with accreditation schemes including WebTrust for CAs.

5.6 Compromise and Disaster Recovery

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

The AlphaSSL 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.

Before terminating its CA activities, the AlphaSSL CA will take steps to transfer to a designated organization the following information at the AlphaSSL CA's own costs:

- All information, data, documents, repositories, archives and audit trails pertaining to the AlphaSSL CA.

6. Technical Security Controls

The security measures taken by the AlphaSSL CA to protect its cryptographic keys and activation data is outlined in the Certificate Policy of the AlphaSSL Managed Brand root.

7. Certificate and CRL Profiles

This section specifies the certificate format and CRL formats.

7.1 Certificate Profile

AlphaSSL certificate profiles are available upon request.

7.2 CRL Profile

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

8. Compliance Audit And Other Assessment

AlphaSSL CA accepts under condition the auditing of practices and procedures it does not publicly disclose. AlphaSSL 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, AlphaSSL 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

AlphaSSL CA currently meets the requirements of the accreditation scheme known as WebTrust for CAs.

AlphaSSL CA shall also seek accreditation by Qualified Auditors and seek accreditation under the WebTrust for CAs scheme on a recurrent basis.

Information on AlphaSSL CA's conformance with the requirements of any other accreditation scheme can be sought by the organization of such accreditation scheme directly.

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 AlphaSSL CA, 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 AlphaSSL CA 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 trials, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

With regard to conformance audits, AlphaSSL CA 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, AlphaSSL CA may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration. AlphaSSL CA 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, AlphaSSL CA remains ultimately in charge of the whole process. AlphaSSL CA will ensure that compliance audits are also applied to such outsourced services. AlphaSSL CA limits its responsibility thereof according to the conditions in this CPS.

9. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of the AlphaSSL certificates under this CPS as described in this section.

9.1 Fees

The issuance and management of AlphaSSL certificates is subject to fees announced on the AlphaSSL CA web site www.alphassl.com or through requested quotes.

9.1.1 Refund policy

AlphaSSL CA accepts requests for refund in writing. Refund requests must be duly justified and addressed to the Legal Services of AlphaSSL CA. AlphaSSL CA reserves its right to endorse or grant and refunds.

9.2 Financial Responsibility

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

9.3 Confidentiality of Business Information

AlphaSSL CA observes personal data privacy rules and confidentiality rules as described in the AlphaSSL 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.

AlphaSSLCA 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 AlphaSSL CA owes a duty to keep information confidential is the party requesting such information.
- A court order.

AlphaSSL CA 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. AlphaSSL CA properly manages the disclosure of information to the CA personnel.

To incorporate information by reference, AlphaSSL CA might use computer-based and text-based pointers that include URLs, etc.

9.4 Privacy of Personal Information

AlphaSSL CA has an internal policy for the protection of personal data of the applicant applying for an AlphaSSL certificate.

9.5 Intellectual Property Rights

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

The Distinguished names in use across AlphaSSL CA, remain the sole property of AlphaSSL CA, which enforces these rights.

Certificates are and remain property of AlphaSSL CA. AlphaSSL 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 AlphaSSL 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.

AlphaSSL 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

AlphaSSL CA uses this CPS and a subscriber agreement to convey legal conditions of usage of AlphaSSL certificates to subscribers and relying parties.

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

All parties of the AlphaSSL domain, including the AlphaSSL CA 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 AlphaSSL CA.

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 AlphaSSL CA.
- Ensuring that the public key submitted to AlphaSSL CA correctly corresponds to the private key used.
- Accepting all terms and conditions in the AlphaSSL CA CPS and associated policies published in the AlphaSSL CA Repository.
- Refraining from tampering with an AlphaSSL certificate.
- Using AlphaSSL certificates for legal and authorised purposes in accordance with this CPS.
- Notifying AlphaSSL CA or an AlphaSSL RA of any changes in the information submitted.
- Ceasing to use an AlphaSSL certificate if any featured information becomes invalid.
- Ceasing to use an AlphaSSL certificate when it becomes invalid.
- Removing an AlphaSSL certificate when invalid from any applications and/or devices they have been installed on.
- Using an AlphaSSL 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 AlphaSSL CA or any AlphaSSL 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 AlphaSSL CA certificate.
- Notifying AlphaSSL CA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.

AlphaSSL CA makes available a subscriber agreement in order to ensure that the subscriber is bound under the following terms:

a) Submit accurate and complete information to AlphaSSL CA in accordance with the requirements of this CPS particularly with regards to registration.

b) Only use the key pair in accordance with this CPS.
c) Exercise reasonable care to avoid unauthorized use of its private key.
   - Under the AlphaSSL CA model the subscriber always generates its own keys, in which case the following terms also apply : use a key length and algorithm, which is recognized as being fit for the purposes of electronic signatures.
d) Notify AlphaSSL CA 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 subscribers 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 an AlphaSSL certificate must:

- Have the technical capability to use digital certificates.
- Receive notice of the AlphaSSL CA and associated conditions for relying parties.
- Validate an AlphaSSL certificate by using certificate status information (e.g. a CRL) published by AlphaSSL CA.
- Trust an AlphaSSL certificate only if all information featured on such certificate can be verified as being correct and up to date.
- Rely on an AlphaSSL certificate, only as it may be reasonable under the circumstances.
- Notify AlphaSSL CA 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 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, AlphaSSL 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.

Relying parties are hereby notified that the conditions prevailing in this CPS are binding upon them each time they consult an AlphaSSL CA 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 AlphaSSL CA Repository and Web site Conditions

Parties (including subscribers and relying parties) accessing the AlphaSSL CA Repository and web site agree with the provisions of this CPS and any other conditions of usage that AlphaSSL 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 AlphaSSL CA Repositories include or contain:

- Information provided as a result of the search for a digital certificate.
- Information to verify the status of an AlphaSSL certificate.
- Information published on the AlphaSSL CA web site.
- Any other services that AlphaSSL 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 AlphaSSL CA.

The AlphaSSL CA maintains a certificate repository during the application period and for a maximum of five years after the expiration or revocation of a certificate.

9.6.4.1Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the AlphaSSL 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. AlphaSSL 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 AlphaSSL Repositories and web site may result in terminating the relationship between the AlphaSSL CA and the party.

9.6.4.2Accuracy of Information

AlphaSSL CA makes every effort to ensure that parties accessing its repositories receive accurate, updated and correct information. AlphaSSL CA, however, cannot accept any liability beyond the limits set in this CPS and the AlphaSSL CA insurance policy.

9.6.5 AlphaSSL CA Obligations

AlphaSSL CA promises to:

- Comply with this CPS and its amendments as published under https://www. alphassl.com/repository
- Provide infrastructure and certification services, including the establishment and operation of the AlphaSSL 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.
- 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 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 AlphaSSL CA repository.

The liability of AlphaSSL CA under the above stated article for proven damages is limited to 1 Dollar for any individual certificate, directly caused by the occurrences listed above. This limit might be reviewed by AlphaSSL CA. AlphaSSL CA 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 AlphaSSL 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, including identification data, serial numbers and public key values
- Erroneous or incomplete requests for operations on certificates
- 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.

AlphaSSL CA acknowledges it has no further obligations under this CPS.

9.6.6 Information incorporated by reference into a digital certificate

AlphaSSL CA incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the AlphaSSL CA CPS.
- Any other applicable certificate policy as may be stated on an issued AlphaSSL 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.

9.6.7 Pointers to incorporate by reference

To incorporate information by reference AlphaSSL uses computer-based and text-based pointers. AlphaSSL may use URLs, OIDs etc.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

AlphaSSL CA does not warrant:

- The accuracy of any unverifiable piece of information contained in certificates.
- 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 is AlphaSSL 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 AlphaSSL certificates is limited to a maximum of USD 1000 toward the subscriber.:

9.9 Indemnities

This section contains the applicable indemnities.

To the extent permitted by law, the subscriber agrees to indemnify and hold AlphaSSL 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 AlphaSSL 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 managed Branded Root.

9.10 Term and Termination

This CPS remains in force until notice of the opposite is communicated by AlphaSSL 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

AlphaSSL 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 AlphaSSL 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 AlphaSSL CA must be addressed to legal@alphassl.com or by post to the AlphaSSL in the address mentioned in the introduction of this document.

9.12 Ownership

AlphaSSL CA is operated and owned by GlobalSign nv/sa and should be regarded as a separate brand of GlobalSign. The Brand Root is the GlobalSign Root CA (which is managed according to practises described in the GlobalSign Certificate Policy published under www.globalsign.net/repository. This CPS does not address the Brand Root policies, but rely exclusively on the practises described in the GlobalSign Certificate Policy.

Request for information on the compliance of t AlphaSSL CA with accreditation schemes as well as any other inquiry associated with this CPS can be addressed to:
GlobalSign
attn. AlphaSSL,
Ubicenter,
Philipssite 5
B-3001 Leuven,
Belgium.

This CPS is final and binding between GlobalSign NV/SA (operating and owning the AlphaSSL CA), a company under public law, with registered office at Ubicenter, Philipssite 5, B-3001 Leuven, VAT Registration Number BE 459.134.256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (Hereinafter referred to as "AlphaSSL")

and

the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the AlphaSSL 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 AlphaSSL certificate to a AlphaSSL directory. The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CPS.

9.13 Amendments

Changes to this CPS are indicated by appropriate numbering.

9.14 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 AlphaSSL CA of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, AlphaSSL CA convenes a Dispute Committee that advises AlphaSSL 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 member of AlphaSSL CA 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 AlphaSSL CA executive management. AlphaSSL CA executive management may subsequently communicate the proposed settlement to the resting party.

9.15 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 AlphaSSL certificates or other products and services. The law of Belgium apply to all AlphaSSL CA commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to AlphaSSL CA products and services where AlphaSSL CA acts as a provider, supplier, beneficiary receiver or otherwise.

9.16 Compliance with Applicable Law

AlphaSSL CA complies with applicable laws of Belgium..

9.17 Miscellaneous Provisions

9.17.1 Survival

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

9.17.2 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.
.

10. 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 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.
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.
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.
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 AlphaSSL CA.
CERTIFICATION PRACTICE STATEMENT OR **CPS**
A statement of the practices in the management of certificates during all life phases.
CERTIFICATE CHAIN
A hierarchical list certificates containing a 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, and suspension of certificates.
CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked and suspended 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 AlphaSSL CA that issues, suspends, or revokes a digital certificate.
CERTIFICATE POLICY (CP)

A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a CA certificate.

CERTIFICATE ISSUANCE
Delivery of X.509 v3 digital certificates.

CERTIFICATE SUSPENSION
Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period

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 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.

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.

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.
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.
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.
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.
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
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, suspension, 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.

ALPHASSL CA PUBLIC CERTIFICATION SERVICES

A digital certification system made available by AlphaSSL CA as well as the entities that belong to the AlphaSSL CA domain as described in this CPS.

ALPHASSL CA PROCEDURES

A document describing the AlphaSSL CA's internal procedures with regard to registration of end users, security etc.

WEBTRUST PROGRAM FOR CAS: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities, available at http://www.webtrust.org/certauth fin.htm.

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. List of acronyms

CA: Certification Authority
RA: Registration Authority
LRA: Local Registration Authority
CP: Certificate Policy
CPS: Certification Practice Statement
ETSI: European Telecommunications Standards Institute
IETF: Internet Engineering Task Force
ISO: International Standards organization
ITU: International Telecommunications Union
PKI: Public Key Infrastructure
RFC: Request for Comments
SSCD: Secure Signature Creation Device
VAT: Value Added Tax