SSL.com Certification Practice Statement

SSL.com
Version 1.0
February 15, 2012
2260 W Holcombe Blvd Ste 700
Houston, Texas, 77019
US

Tel: +1 SSL-CERTIFICATE
(+1-775-237-8434)

Fax: +1 832-201-7706
www.ssl.com

TABLE OF CONTENTS

1.

2. INTRODUCTION

SSL.com Certificate Authority ("SSL.com") is a Certification Authority (CA) that issues digital certificates to various subscribing entities, including private and public companies and individuals. SSL.com performs functions associated with public key operations which include receiving application requests for, issuing, revoking and renewing digital certificates and the maintenance, issuance, and publication of Certificate Revocation Lists ("CRLs") and an Online Certificate Status Protocol ("OCSP").

2.1. Overview

This document is the SSL.com Certification Practice Statement (CPS). The SSL.com CPS outlines the legal, commercial and technical principles and practices that SSL.com employs in approving, issuing, using, and managing certification services. This includes approving, issuing, using and managing Digital Certificates and maintaining a X.509 Certificate based public key infrastructure (PKIX). SSL.com may update and supplement this CPS with amendments in order to provide for additional product offerings and to comply with certain regulatory or industry standards and requirements.

This CPS describes SSL.com's certification processes, business operations, and repository operations. The CPS is only one of many documents that are relevant to SSL.com's certificate issuance practices. Other important documents include the SSL.com subscriber agreement, the relying party agreement, and other ancillary agreements that are posted on the SSL.com repository. These documents obligate parties using or relying on a SSL.com digital certificate to meet a certain minimum criteria prior to their use or reliance on a SSL.com Certificate.

SSL.com's CPS is also a means to notify the public and relevant parties of the roles and responsibilities involved in Certificate based practices within the SSL.com PKI. The CPS is formatted and maintained in accordance with IETF PKIX RFC 3647 and is divided into separate sections that cover the practices and procures for applying for, identifying, issuing, and revoking certificates along with information about SSL.com's security controls and auditing process. To preserve the format of RFC 3647, some section headings do not apply and will contain the text "Not applicable" or "No stipulation". The format is preserved to assist the reader in comparing and contrasting the various CPS documents provided by various CAs.

2.2. Document Name and Identification

This document is the SSL.com CPS version 1.0, which was approved for publication on 2/12/2012 by SSL.com. The CPS is a public statement of the practices of SSL.com and the conditions of issuance, revocation and renewal of a certificate issued under SSL.com's PKI hierarchy. Revisions to this document have been made as follows:

Date	Changes	Version

Revisions not denoted "significant" are those deemed by the CA's Policy Authority to have minimal or no impact on subscribers and relying parties using certificates, the CRLs and the OCSP used by SSL.com. Insignificant revisions may be made without changing the version number of this CPS.

2.3. PKI Participants

2.3.1. Certification Authorities

The term "Certificate Authority (CA)" is a generic term used to describe entities that are allowed to issue public key certificates. The SSL.com CA:

- Conforms its operations to this CPS as may from time to time be modified by amendments published in the SSL.com repository (www.ssl.com/repository/),
- Issues and publishes certificates in a timely manner in accordance with the issuance times set forth in this CPS,
- Revokes certificates upon receipt of a valid revocation request from a person authorized to request revocation,
- Maintains and updates its OCSP on a regular basis and in a timely manner, in accordance with the applicable Certificate Policy and as described in this CPS,
- Publishes CRLs on a regular basis, in accordance with the applicable Certificate Policy and as described in this CPS,
- Distributes issued certificates in accordance with the methods detailed in this CPS,
- Updates CRLs in a timely manner as detailed in this CPS, and
- Notifies subscribers via email of expiring SSL.com issued certificates (for a period disclosed in this CPS).

2.3.2. Registration Authorities

SSL.com does not employ any Registration Authorities.

2.3.3. Subscribers

Subscribers are individuals, companies, or other entities that use SSL.com's PKI services to provide supported transactions and communications. Subscribers are identified in and have the private key corresponding to the public key listed in an issued certificate. Prior to being issued a certificate, an applicant (a potential subscriber) must submit an application accompanied by certain verification information. SSL.com will only issue a Certificate to an applicant after the applicant has been approved and verified by SSL.com.

In certain circumstances, SSL.com may issue a certificate to an individual or entity that is different from the entity which actually applied for the certificate. In such circumstances, the Subject of the certificate will be the entity whose credentials have been submitted, and the term Subscriber shall apply to the entity which contracted with SSL.com for the issuance of the certificate. Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is only used appropriately.

2.3.4. Relying Parties

Relying parties use SSL.com's PKI services to perform certain transactions, communications, or functions and may reasonably rely on issued certificates and/or digital signatures that contain a verifiable reference to a public key that is listed in the subscriber certificate. Not all of SSL.com's certificate products are intended to be used in e-commerce transactions or environments, and parties who rely on such certificates do not qualify as a relying party.

Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be an ethical business operation. Relying Parties should always independently examine each certificate holder to determine whether the certificate owner is ethical and trustworthy.

2.3.5. Other Participants

SSL.com operates a network of resellers that allows authorized agents of SSL.com to integrate SSL.com digital certificates into their own product portfolios. Resellers are responsible for referring digital certificate customers to SSL.com. SSL.com, and not Reseller, maintains full control over the certificate life-cycle process, including application, issuance, renewal and revocation. All Resellers are required to provide proof of organizational status and must enter into

a Reseller agreement with SSL.com that requires them to comply with this CPS prior to being provided with Reseller status and facilities. Unless otherwise noted, all certificates provided by SSL.com are also available through its Reseller program.

2.4. Certificate Usage

A digital certificate is formatted data that cryptographically binds an identified subscriber to a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to the other participants in such transaction. Certificates may be issued for individuals, organizations, government entities, educational institutions, or infrastructure components such as firewalls, routers, or other security devices.

2.4.1. Appropriate Certificate Use

Depending on the certificate type, the certificates issued from SSL.com may only be used for authentication, encryption, access control, and digital signature purposes.

Low assurance (or Domain Validated) certificates are not used for authentication purposes and are ideal for mail servers and server to server communications. Entities purchasing these certificates receive limited validation by SSL.com. These certificates are used to ensure that the data being transmitted from one party to another is secure and are not intended for websites conducting e-commerce or other valued data transactions. A party transmitting data cannot be sure or guaranteed that the receiving party is the party named in the certificate. Due to increased validation speed, the lack of stringent validation, and the intended use of low assurance certificates, the certificates do not carry a warranty.

High assurance certificates are issued to both individuals and organization whose identity has first been verified according to the validation procedures described in section 4.

Code Signing Certificates are designed for commercial software developers to provide assurance regarding the developer's identity, and are designed to represent the level of assurance provided today by retail channels for software. With a Code Signing Certificate, a digital signature can be appended to the executable code itself, thus providing assurance to recipients that the code or software does indeed come from the signer of the software.

Secure Email Certificate, in combination with an S/MIME compliant email application, allow subscribers to digitally sign email for relying parties, or relying parties to encrypt email for the subscriber.

SSL.com uses third party domain name registrars and directories to assist with application validation in order to provide increased speed of issuance. Where possible, SSL.com's or a third party's directories will be used to confirm the right to use the domain name used in the application. If the directory cannot be used to sufficiently validate a certificate applicant, further validation processes may be used which may include an out of bands validation of the applicant's submitted information.

See Appendix B for further information on different Certificates issued by SSL.com.

2.4.2. Prohibited Certificate Use

Certificates may only be used in accordance with their intended purpose and in compliance with all applicable laws and regulations. Certificates may not be used to complete or assist in performing any transaction that is prohibited by law.

Each party using or relying on a certificate shall be bound by and comply with the terms and conditions set forth in the applicable agreement between the party and SSL.com. Low assurance certificates may not be used as proof of identity and may not be held forth as establishing the legitimacy of the certificate holder's business operations. Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be an ethical business operation.

Certificates may not be used for any application requiring fail-safe performance systems such as the operation of nuclear power facilities, air traffic control systems, weapon control systems, or any other system where a failure of the system could cause any form of damage.

2.5. Policy Administration

2.5.1. Organization Administering the Document

This CPS and any related documents, agreements, or policy statements referenced herein are maintained and administered by the SSL.com Policy Authority.

SSL Corp
2260 W Holcombe Blvd Ste 700
Houston, Texas
US

2.5.2. Contact Person

SSL.com Certification Authority
2260 W Holcombe Blvd Ste 700
Houston, Texas
US

2.5.3. Person Determining CPS Suitability for the Policy

The suitability and applicability of SSL.com's CPS is reviewed and approved by both SSL.com's Policy Authority and SSL.com's legal department.

2.5.4. CPS Approval Procedures

SSL.com's CPS and any amendments made to it are reviewed and approved by SSL.com's policy authority and legal department. Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum. The current version of the CPS is always made available to the public through SSL.com's repository which can be accessed online at www.ssl.com/repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 5.4 of this CPS.

2.6. Definitions and Acronyms

Acronyms:

CA	Certificate Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVC	Content Verification Certificate
EPKI	Enterprise Public Key Infrastructure Manager
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MDC	Multiple Domain Certificate

OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SGC	Server Gated Cryptography
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

Definitions:

Applicant:	The Applicant is an entity applying for a Certificate.
Certificate:	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, and contains a serial number.
Subscriber:	The Subscriber is an entity that has been issued a Certificate.
Subscriber Agreement:	The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Digital Certificate product type as presented during the product online order process.
Relying Party:	The Relying Party is an entity that relies upon the information contained within the Certificate.
Relying Party Agreement:	The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at www.ssl.com/repository/ssl_v1_cps.pdf.

3. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CPS is only one of a set of documents relevant to the SSL.com's certification services. The list of documents below is a list of other documents that this CPS will from time to time mention. The list is not exhaustive. The document name, location of, and status, whether public or private, are detailed below. The SSL.com Repository can be found at www.ssl.com/repository.

Document Status Location	Status	Location
SSL.com Certification Practice Statement	Public	SSL.com Repository
SSL Subscriber Agreement	Public	SSL.com Repository
Code Signing Subscriber Agreement	Public	SSL.com Repository
Email Certificate Subscriber Agreement	Public	SSL.com Repository

SSL Relying Party Agreement	Public	SSL.com Repository
SSL Relying Party Warranty	Public	SSL.com Repository
Reseller Agreement	Confidential	Presented to partners accordingly

3.1. Repositories

SSL.com publishes this CPS, its subscriber agreements, and the relying party agreement in the official SSL.com repository at www.ssl.com/repository. The SSL.com Certificate Policy Authority maintains the SSL.com repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in this CPS.

SSL.com makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated, and correct information. However, SSL.com cannot accept any liability beyond the limits set forth in this CPS.

Parties accessing the repository agree with the provisions of this CPS and any other conditions of usage that SSL.com may make available. Parties demonstrate acceptance this CPS and the other terms and conditions that may apply by using a SSL.com issued certificate.

Failure to comply with the conditions herein or posted on the SSL.com website may result in the termination of the relationship between SSL.com and the party.

3.2. Publication of Certificate Information

Certificate information is published by SSL.com's issuance of the Certificate and in accordance with the provisions of this CPS that are relevant to such a certificate. Revoked certificate information is published through SSL.com's OCSP operations.

An updated CRL is published on the SSL.com website every 24 hours; however, under special circumstances the CRL may be published more frequently. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate.

3.3. Time or Frequency of Publication

Updates to the CPS are published in accordance with Section 9.12. Updates to the Subscriber Agreement, Relying Party Agreements, and other agreements posted on the repository are published as often as necessary. Certificates are published upon issuance.

Certificate information is published in accordance with the provisions of the CPS relevant to such a certificate. CRLs are issued every 24 hours and include a monotonically increasing sequence number for each CRL issued. Under special circumstances, SSL.com may publish new CRLs prior to the expiration of the current CRL. Each CRL is valid only for the 24 hours following its publication or until an updated CRL has been published, whichever comes first.

Typically, SSL.com updates its OCSP every 24 hours. Under special circumstances the OCSP may be more frequently. All parties are strongly urged to always consult the OCSP prior to relying on information featured in a certificate.

3.4. Access Controls on Repositories

The information published in the SSL.com repository (www.ssl.com/repository) is public information and may be accessed freely by anyone visiting the site, provided they agree to the site's terms and conditions as posted thereon. Read-only access to the information is unrestricted. SSL.com has implemented logical and physical security measures to prevent unauthorized additions, modification, or deletions of repository entries.

4. IDENTIFICATION AND AUTHENTICATION

4.1. Naming

4.1.1. Types of Names

SSL.com Certificates are issued with an X.501 compliant non-null Distinguished Name (DN) in the Issuer and Subject Fields. Issuer Distinguished Names may consist of a combination of the following Components:

Attribute	Abbr.	Value
Common Name	CN	The CA name or not used
Organization	O	
Organizational Unit	OU	Certificates may be multiple OU attributes. The attributes may include: Copyright information References to the terms and conditions of use Description of the Certificate
Country	C	PT
Locality	L	Not used
State or Province	S	Not Used

Certificate Distinguished Names may consist of a combination of the following Components:

Attribute	Abbr.	Value
Common Name	CN	The Common Name which could be the name of the Subscriber or domain name for which the certificate has been issued
Organization	O	The organization or blank
Organizational Unit	OU	Certificates may be multiple OU attributes. The attributes may include: Organization information or Issuer Information Copyright information References to the terms and conditions of use Description of the Certificate Certificate warranty information Verification or validation information Issuance and/or hosting information Special certificate notes
Country	C	The two letter ISO country code or not used
Locality	L	Subscriber's locality or not used
State or Province	S	State or Providence or not used
Street	STREET	Street address or not used
Postal code	PostalCode	Postal code or not used

Email address	E	Email address for Email certificates

Enhanced naming is the usage of an extended organization field in an X.509v3 certificate. Information contained in the organizational unit field is also included in the Certificate Policy extension that SSL.com may use.

For High assurance certificates, the Common Name (CN) component of the Certificate is verified prior to the Certificate's issuance. The CN is not verified in Low Assurance certificates.

SSL.com certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and any disclaimers of warranty that may apply. The lack of such information does not mean it does not apply to that certificate.

To communicate information SSL.com may use:

- An organizational unit attribute.
- A SSL.com standard resource qualifier to a certificate policy.
- SSL.com' SSL.comed extensions.

4.1.2. Need for Names to be Meaningful

SSL.com uses non-ambiguous designations and commonly used semantics to identify both the Issuer of the Certificate and the Subject of the Certificate.

4.1.3. Anonymity or Pseudonymity of Subscribers

SSL.com does not intentionally issue anonymous or pseudonymous names. However, low assurance and email certificate subscribers are not validated prior to the certificate's issuance and, as a result, may contain an anonymous or pseudonymous name.

4.1.4. Rules for Interpreting Various name Forms

Distinguished Names in Certificates are X.501 compliant. For information on how X.501 Distinguished names are interpreted, please see RFC 2253 and RFC 2616.

4.1.5. Uniqueness of Names

The Distinguished Name of a SSL.com-issued Certificate is unique for each Subscriber. The uniqueness of the Distinguished Name is ensured through an automated process. Also, SSL.com assigns certificate serial numbers that appear in SSL.com certificates. Assigned serial numbers are unique.

4.1.6. Recognition, Authentication, and Role of Trademarks

Through its subscriber agreements, SSL.com prohibits the use of a name or symbol that infringes upon the Intellectual Property Rights of another. However, SSL.com does not verify or check the name appearing in a Certificate for non-infringement. Subscribers are solely responsible for ensuring the legality of any information presented for use in a SSL.com-issued Certificate. SSL.com subscribers represent and warrant that when submitting an application to SSL.com and when using a domain and distinguished name (and all other certificate application information) that they are not interfering with or infringing any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

SSL.com does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property or a domain's use of any infringing material. SSL.com, in its sole discretion and without any liability, may reject an application or revoke a certificate, based on any intellectual property infringement claims or ownership disputes.

4.2. Initial Identity Validation

Upon receipt of an application for a digital certificate and based on the submitted information, SSL.com confirms the following information:

- The certificate applicant is the same person as the person identified in the certificate request.
- The certificate applicant holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate, except for non-verified subscriber information.
- Any agents who apply for a certificate listing the certificate applicant's public key are duly authorized to do so.

Verification of a digital signature is used to determine that:

- the private key corresponding to the public key listed in the signer's certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

In all types of SSL.com certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify SSL.com of any changes that would affect the validity of the certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber. Subscriber shall still be required to pay any applicable charges and fees as specified in the relevant subscriber agreement.

4.2.1. Method to Prove Possession of Private Key

Every Applicant must demonstrate that it holds the private key corresponding to the public key that will be included in the Certificate. To prove possession, the Applicant must submit a digitally signed PKCS#10 to SSL.com or provide another cryptographically equivalent demonstration.

4.2.2. Authentication of Organization Identity

The following elements are critical information elements for a SSL.com certificate issued to an organization. Those elements marked with PUBLIC are present within an issued certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Company / DUNS number (if available)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone

- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber agreement, signed (if applying out of bands)

Documentation requirements for organizational applicants include any / all of the following:

- Articles of Association
- Business License
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorized representative of a government organization
- Official letter from office of Dean or Principal (for Educational Institutions)

SSL.com may accept at its discretion other official organizational documentation supporting an application.

Each certificate is validated according to the level of security required for the issued certificate as explained more fully in Section 4.2

SSL.com may use the services of a third party to confirm information on a business entity that applies for a digital certificate. SSL.com accepts confirmation from third party organizations, other third party databases and government entities.

SSL.com's controls may also include Trade Registry transcripts that confirm the registration of the applicant company and state the members of the board, the management and Directors representing the company.

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

4.2.3. Authentication of Individual Identity

The following elements are critical information elements for a SSL.com certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Contact information including full name, email address and telephone

- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Subscriber agreement, signed (if applying out of bands)

Documentation requirements for Individual applicants shall include identification elements such as:

- Passport
- Driving License
- Bank statement

SSL.com may accept, in its sole s discretion, other official documentation supporting an application.

Each certificate is validated according to the level of security required for the issued certificate as explained more fully in Section 4.2

4.2.4. Non-Verified Subscriber Information

SSL.com does not validate any information not listed as being validated under Section 4.2. Subscriber Information in low assurance certificates is not validated.

4.2.5. Validation of Authority

The authority of an individual's authority to issue a certificate is confirmed with a WHOIS check or by a practical demonstration of the agent's authority to act on behalf of the domain owner.

The Subscriber shall control and be responsible for the data that an agent supplies to SSL.com. The Subscriber must promptly notify SSL.com of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

4.2.6. Criteria for Interoperation

SSL.com does not appoint third party CAs and does not allow other CAs to sign to its root certificates.

4.3. Identification and Authentication for Re-key Requests

4.3.1. Identification and Authentication for Routines Re-key

Renewal application requirements and procedures are the same as those requirements and procedures implemented for the application validation and issuance of new customers.

4.3.2. Identification and Authentication for Re-key After Revocation

Rekey/renewal after revocation is only permitted if the Certificate was not revoked because of (i) a mistake in the party to whom the certificate was issued, (ii) a breach of the subscriber agreement, (iii) a material misrepresentation by the Subscriber, or (iv) any other reason that could potentially cause harm to SSL.com's trusted status.

4.4. Identification and Authentication for Revocation Requests

Prior to revoking a certificate, SSL.com verifies that the revocation was requested by the Certificate Subscriber. The revocation request must be sent by the administrator contact associated with the certificate application. SSL.com may, if necessary, also request that the revocation request be made by either the organizational contact or billing contact. Upon receipt of the revocation request, SSL.com will request confirmation of out of bands contact details by telephone or by fax from the known administrator.

5. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

5.1. Certificate Application

SSL.com certificates are issued to organizations and individuals who submit a certificate application and successfully complete the required validation procedures described herein. Prior to the issuance of a certificate, SSL.com will validate an application in accordance with this CPS. Validation of the application may involve the request by SSL.com for the applicant to provide relevant official documentation supporting the application.

5.1.1. Who Can Submit a Certificate Application

Certificate applications may be submitted by an individual or an authorized representative of an organization or other entity who is the subject of the certificate. An authorized agent of an applicant may submit a certificate on the applicant's behalf.

5.1.2. Enrollment Process and Responsibilities

Generally, applicants will complete the online forms made available by SSL.com through its website in order to apply for a certificate. Under special circumstances, the applicant may submit an application via email. Email applications are under the discretion of SSL.com and may not be accepted.

All Certificate applicants must complete the enrollment process prior to being issued a certificate. The enrollment process may include:

- Generating a RSA key pair and demonstrate to SSL.com ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR)
- Making all reasonable efforts to protect the integrity the private key half of the key pair
- Submitting to SSL.com a certificate application, including application information as detailed in this CPS, a public key half of a key pair, and agree to the terms of the relevant subscriber agreement
- Providing proof of identity through the submission of official documentation as requested by SSL.com during the enrollment process

Additional documentation in support of the application may be required by SSL.com in its sole discretion in order to assist SSL.com in verifying the identity of the subscriber. Upon verification of identity, SSL.com issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify SSL.com of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.

The following steps describe the milestones to issue a Secure Server Certificate:

a) The applicant fills out the online request on SSL.com's web site and the applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organizational information, country code, verification method and billing information.
b) The applicant accepts the on line subscriber agreement.
c) The applicant submits the required information to SSL.com.
d) The applicant pays the certificate fees.
e) SSL.com verifies the submitted information using third party databases and Government records

f) Upon successful validation of the application information, SSL.com may issue the certificate to the applicant. Should the application be rejected, SSL.com will alert the applicant that the application has been unsuccessful.
g) Renewal is conducted as per the procedures outlined in this CPS and the official SSL.com websites.
h) Revocation is conducted as per the procedures outlined in this CPS.

5.2. Certificate Application Processing

Prior to the issuance of a certificate SSL.com will validate an application in accordance with this CPS which may involve the request by SSL.com to the applicant for relevant official documentation supporting the application.

From time to time, SSL.com may modify the requirements related to application information for individuals, to respond to SSL.com's requirements, the business context of the usage of a digital certificate, or as prescribed by law.

5.2.1. Performing Identification and Authentication Functions

Applications for SSL.com certificates are supported by appropriate documentation to establish the identity of an applicant as described in Section 3.2. SSL.com may use any means of communication at its disposal to ascertain the identity of an organizational or individual applicant. SSL.com reserves the right of refusal in its absolute discretion.

Prior to issuing a Certificate, SSL.com employs controls to validate the identity of the subscriber information featured in the certificate application. Such controls are indicative of the product type:

5.2.1.1. Low Assurance Certificates

Low assurance certificates receive limited validation by SSL.com. SSL.com, at its discretion, may establish domain control by utilizing SSL.com or third party domain registrars and directories, by verifying control of the domain by practical demonstration of control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

5.2.1.2. High Assurance Certificates

Validation of high assurance certificates involves validating the organization named in the certificate. This process involves SSL.com, automatically or manually, reviewing the application information provided by the applicant (as per section 4.1 of this CPS) in order to check that:

1. The applicant has the right to use the domain name used in the application.
    - Validated by reviewing domain name ownership records or (for government and educational institutions associated with a .EDU or .GOV domain only) receiving a letter on official departmental letterhead, with the order details and a statement verifying that the signor (which must be a WHOIS contact or senior member of management) is authorized to act on behalf of the organization.
    - Validation may be supplemented through the use of the administrator contact associated with the domain name SSL.com record for communication with SSL.com validation staff or for automated email challenges.
    - Validation may be supplemented through the use of generic emails which ordinarily are only available to the person(s) controlling the domain name administration, for example webmaster@..., postmaster@..., admin@...
2. The applicant is an accountable legal entity, whether an organization or an individual.

- Validated by requesting official company documentation, such as Business License, Articles of Incorporation, Sales License or other relevant documents.
- For non-corporate (including individual, government, and educational entities) applications, documentation such as bank statement, copy of passport, copy of driving license or other relevant documents.

The above assertions are reviewed through an automated process, manual review of supporting documentation and reference to third party official databases.

5.2.1.3. Code Signing

Code Signing Certificates are processed by SSL.com in accordance with the process outlined for high assurance certificates. SSL.com may employ the data held in its domain databases to expedite the validation process. If the application data matches the records held by SSL.com, manual validation intervention is not required.

5.2.1.4. Secure Email/ Client Certificates

Secure Email Certificates and client certificates are *non-validated*. SSL.com only validates the right for the applicant to use the submitted email address. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by SSL.com. The login details are sent via email to the address submitted during the certificate application.

Once logged into the online certificate collection facilities and prior to the installation of the Secure Email Certificate, SSL.com validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application process. If the automated challenge is successful, SSL.com will release the digital certificate to the Subscriber.

5.2.2. Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application, SSL.com will approve an application for a digital certificate and issue the certificate.

If the validation of a certificate application fails, SSL.com will reject the certificate application. SSL.com reserves its right to reject applications to issue a certificate to applicants if, on its own assessment, by issuing a certificate to such parties the good and trusted name of SSL.com might get tarnished, diminished, or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently re-apply.

The private key associated with a public key, which has been submitted as part of a rejected certificate application, may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate. The private key may also not be resubmitted as part of any other certificate application.

5.2.3. Time to Process Certificate Applications

SSL.com makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner. Upon the receipt of the necessary details and / or documentation, SSL.com aims to confirm submitted application data and to complete the validation process and issue / reject a certificate application within two (2) working days.

From time to time, events outside of the control of SSL.com may delay the issuance process. However SSL.com will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

5.3. Certificate Issuance

SSL.com issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 4.4 of this CPS). Issuing a digital certificate means that SSL.com accepts a certificate application. SSL.com certificates are issued to organizations or individuals.

5.3.1. CA Actions During Certificate Issuance

SSL.com issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 4.4 of this CPS). Issuing a digital certificate means that SSL.com accepts a certificate application.

5.3.2. Notification to Subscriber by the CA of Issuance of Certificate

SSL.com notifies the Subscriber of the issuance of a certificate within a reasonable amount of time after the certificate is created. Issued certificates may either be downloaded by the Subscriber or may be installed by SSL.com directly (depending on the certificate type).

5.4. Certificate Acceptance

An issued certificate is either delivered via email or installed on a subscriber's computer / hardware security module through an online collection method.

5.4.1. Conduct Constituting Certificate Acceptance

A subscriber is deemed to have accepted a certificate when:

- the subscriber uses the certificate, or
- 30 days pass from the date of the issuance of a certificate

5.4.2. Publication of the Certificate by the CA

An issued certificate is published solely by delivering the certificate to the Subscriber.

5.4.3. Notification of Certificate Issuance by the CA to Other Entities

Other parties involved in the issuance and approval of the Certificate may receive notification of the issuance of a certificate to their customer or client.

5.5. Key Pair and Certificate Usage

5.5.1. Subscriber Private Key and Certificate Usage

Use of the Private Key is prohibited until the Subscriber has agreed to a Subscriber agreement. Certificates may only be used for lawful and appropriate purposes as set forth in this CPS. Subscribers are responsible for protecting their private keys from unauthorized use and agree to immediately cease using the Certificate following the expiration or revocation of the Certificate.

5.5.2. Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

- the digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate;
- the relying party has checked the revocation status of the certificate by referring to the relevant OCSP and the certificate has not been revoked;

- the relying party understands that a digital certificate is issued to a subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the certificate profile; and
- the digital certificate applied for is appropriate for the application it is used in, e.g. relying parties should not rely on low assurance SSL Certificates for e-commerce uses.

Reliance is accepted as reasonable under the provisions made for the relying party under this CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by SSL.com under the provisions made in this CPS, the relying party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

5.6. Certificate Renewal

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

Renewal fees are detailed on the official SSL.com websites and within communications sent to subscribers approaching the certificate expiration date. SSL.com shall make reasonable efforts to notify subscribers via e-mail of the imminent expiration of a digital certificate. Notice shall ordinarily be provided within a 60-day period prior to the expiration of the certificate.

5.6.1. Circumstances for Certificate Renewal

A Subscriber may renew an existing Certificate prior to or after its expiration by submitting a renewal request on line or in writing to SSL.com.

5.6.2. Who May Request Renewal

The Subscriber of the certificate or an authorized representative must be the party requesting the certificate's renewal.

5.6.3. Processing Certificate Renewal Requests

Renewal applications and requests undergo the same identity check as detailed for new customers.

5.6.4. Notification of New Certificate Issuance to Subscriber

Notification of a new certificate issuance is performed in accordance with Section 4.4.3.

5.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting acceptance of a renewed certificate is the same as specified in Section 4.4.1.

5.6.6. Publication of the Renewal Certificate by the CA

A renewed certificate is published by delivering the certificate to the Subscriber.

5.6.7. Notification of Certificate Issuance by the CA to other Entities

A reseller may receive notification of its customer's certificate renewal.

5.7. Certificate Re-key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

5.7.1. Circumstances for Certificate Re-Key

Sometimes circumstances may dictate that a valid or expired certificate must be rekeyed. Rekeying a certificate prior to tits expiration will prevent an interruption in the certificates usage. A rekey request made more than thirty (30) days from the certificate's date of issuance may be refused.

5.7.2. Who May Request Certificate of a New Public Key

The Subscriber of a Certificate or an authorized representative must be the party requesting a certificate rekey.

5.7.3. Processing Certificate Re-keying Requests

During a 30-day period (beginning when a certificate is first issued) the Subscriber may request a rekey of their certificate and incur no further fees for the reissue. If details other than just the public key require amendment, SSL.com reserves the right to revalidate the application in accordance with the validation processes detailed within this CPS. If the rekey request does not pass the validation process, SSL.com reserves the right to refuse the rekey application. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant.

5.7.4. Notification of New Certificate Issuance to Subscriber

Notification of a rekeyed certificate is provided in accordance with Section 4.3.2.

5.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

Acceptance of a rekeyed certificate is made in the manner specified in Section 4.4.1.

5.7.6. Publication of the Re-keyed Certificate by the CA

A rekeyed certificate is published by its deliver to the Subscriber.

5.7.7. Notification of Certificate Issuance by the CA to Other Entities

A reseller may receive notice of the rekeying of its customer's certificate.

5.8. Certificate Modification

5.8.1. Circumstance for Certificate Modification

Certificate information may change during the life of the certificate. In this case, SSL.com will issue a new certificate based on the new information rather than modifying an existing certificate. Certificate modification is considered and handled the same as an application for a new certificate.

5.8.2. Who May Request Certificate Modification

See 4.1.1.

5.8.3. Processing Certificate Modification Requests

See 4.1.2.

5.8.4. Notification of New Certificate Issuance to Subscriber

See 4.3.2

5.8.5. Conduct Constituting Acceptance of Modified Certificate

See 4.4.1

5.8.6. Publication of the Modified Certificate by the CA

See 4.4.2.

5.8.7. Notification of Certificate Issuance by the CA to Other Entities

See 4.4.3

5.9. Certificate Revocation and Suspension

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the OCSP and remains on the OCSP until some time after the end of the certificate's validity period.

5.9.1. Circumstances for Revocation

Revocation of a certificate is the permanent end of the operational period of the certificate prior to reaching the conclusion of its stated validity period. SSL.com may revoke a digital certificate if any of the following occur:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the certificate;
- The Subscriber or SSL.com has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- Either the Subscriber's or SSL.com's obligations under this CPS or the relevant Subscriber Agreement are 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 pertaining to the Subscriber that is contained within the certificate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way;
- A Subscriber's Digital Certificate has not been issued in accordance with the policies set out in this CPS;
- The subscriber has used the Subscription Service contrary to law, rule or regulation, or SSL.com reasonably believes that the Subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The certificate is being used or is suspected to be used to distribute or sign malware;
- The information contained in the certificate is incorrect or has changed;
- The certificate was issued as a result of fraud or negligence; or
- The certificate, if not revoked, will compromise the trust status of SSL.com.

When considering whether or not the certificate should be revoked, SSL.com will consider:

- The nature and number of complaints received
- The nature of the complaining party
- Relevant legislation and industry standards
- Additional outside input regarding the trust status of the certificate or the nature of the use of the certificate

5.9.2. Who can Request Revocation

The subscriber or other appropriately authorized parties can request revocation of a certificate. Prior to the revocation of a certificate SSL.com will verify that the revocation request has been made by the organization or individual entity that has made the certificate application.

5.9.3. Procedure for Revocation Request

SSL.com employs the following procedure for authenticating a revocation request:

- The revocation request must be sent by the Administrator contact associated with the certificate application. SSL.com may, if necessary, also request that the revocation request be made by either the organizational contact or the billing contact.
- Upon receipt of the revocation request, SSL.com will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- SSL.com validation personnel will then command the revocation of the certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

5.9.4. Revocation Request Grace Period

There is no revocation grace period.

5.9.5. Revocation Checking Requirement for Relying Parties

Relying Parties must always check the status of the Certificate on which they are relying. Relying Parties may check the OCSP and/or CRL or use the applicable web-based repository to confirm that the certificate has not been revoked or expired.

5.9.6. Time Within Which CA Must Process the Revocation Request

SSL.com processes all revocation requests without delay. The amount of time required depends on the nature of the revocation request, the party requesting the revocation, and other factors surrounding the revocation request. SSL.com will revoke the certificate and place the certificate in the OCSP and/or CRL once it has determined, to SSL.com's satisfaction, that the revocation request was proper.

5.9.7. CRL Issuance Frequency

An updated CRL is published on the SSL.com website every 24 hours. Under special circumstances the CRL may be published more frequently.

5.9.8. Maximum Latency for CRLs

CRLs are posted to the online repository within a commercially reasonable time after their generation. Usually, this is within a minute of the CRL's generation.

5.9.9. On-line Revocation/Status Checking Availability

SSL.com manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by SSL.com are X.509v2 CRLs as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. SSL.com updates and publishes a new CRL every 24 hours or more frequently under special circumstances. The CRL for end entity certificates can be accessed via crl.ssl.com.

5.9.10. On-line Revocation Checking Requirements

Relying Parties must confirm the validity of a certificate via the CRL prior to relying on the Certificate.

5.9.11. Other Forms for Revocation Advertisements available

Not applicable.

5.9.12. Special Requirements Re-key Compromise

SSL.com uses commercially reasonable efforts to notify Relying Parties if it believes or has reason to believe that one of its private keys have been compromised.

5.9.13. Circumstances for Suspension

SSL.com does not utilize certificate suspension.

5.9.14. Who can Request Suspension

Not applicable

5.9.15. Procedure for Suspension Request

Not applicable

5.9.16. Limits on Suspension Period

Not applicable

5.10. Certificate Status Services

5.10.1. Operational Characteristics

SSL.com utilizes both CRLS and an OCSP to allow relying parties to verify the validity of a digital signature made using a SSL.com issued digital certificate. Each CRL and the OCSP contain information for all of SSL.com's revoked or un-expired certificates.

Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. SSL.com issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, SSL.com may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 5.5 of this CPS) for a period of 7 years or longer if applicable.

Individual entries into the OCSP can be requested using the SSL.com OCSP responder. Revoked certificates are affected in the OCSP within 24 hours after their revocation.

5.10.2. Service Availability

The OSPC provides access to certificate status information 24x7. CRL's are open to public inspection 24x7.

5.10.3. Optional Features

Not applicable.

5.11. End of Subscription

A Subscriber may terminate a subscription to SSL.com's Certificate services by allowing the Certificate to expire without renewal or by requesting that SSL.com revoke the issued Certificate.

5.12. Key Escrow and Recovery

SSL.com does not escrow subscriber private keys

6. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

6.1. Physical Security Controls

SSL.com makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

6.1.1. Site Location and Construction

SSL.com performs its CA operations in a secure data center located in the United Kingdom. The building is a secure structure. The data center is operated under a secure policy to ensure that no unauthorized logical or physical access is allowed.

Most records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

6.1.2. Physical Access

Access to the secure part of SSL.com facilities is limited using physical access control and is only accessible to appropriately authorized individuals (referred to hereon as Trusted Personnel). Card access systems are in place to control, monitor and log access to all areas of the facility. Access to the SSL.com CA physical machinery within the secure facility is protected with locked cabinets and logical access control.

6.1.3. Power and Air Conditioning

SSL.com secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

6.1.4. Water Exposures

SSL.com has taken commercially reasonable efforts to ensure that its CA system is secure and protected from flood and water damage.

6.1.5. Fire Prevention and Protection

Fire protection and prevention is made in compliance with local fire regulations

6.1.6. Media Storage

All media storing SSL.com data or information, including media containing audit logs, archived records, software, subscriber information, and other information pertinent to the CA's operation is stored in a secure facility that has implemented both logical and physical controls that limit potential harm to the data.

6.1.7. Waste Disposal

Sensitive documents are shredded prior to disposal. Electronic Media is wiped clean by a trusted source upon the expiration of the data. All media is rendered unreadable prior to its disposal and, where possible, is physically destroyed.

6.1.8. Off-site Backup

SSL.com performs routine backups of all sensitive information. Off-site backups are stored in a separate secure location using a third party data center.

6.2. Procedural Controls

6.2.1. Trusted Roles

Trusted roles are parties allowed to access the SSL.com account management system. Persons acted in a trusted role are granted functional permissions to the account management system. All permissions are applied on an individual basis and are decided by senior members of the management team. All signed authorizations are archived. The roles and responsibilities of each personnel are assigned in such a manner that one person alone cannot circumvent SSL.com's security measures.

6.2.2. Number of Persons Required Per Task

Internal policy and operational procedures require multiple trusted personnel to take part in the CA's operations. This provides an added layer of security. All of the CA's most sensitive tasks require the involvement of multiple trusted personnel.

At least two trusted individuals are required to:

- Issue certificates
- Revoke Certificates
- Handle the CA private keys

6.2.3. Identification and Authentication for Each Role

Trusted personnel must identify and authenticate themselves before system access is granted. Identification is via a username, with authentication requiring a password and digital certificate.

6.2.4. Roles Requiring Separation of Duties

Roles requiring the separation of duties include:

- Validation of Certificate Applications, renewals, or rekeys
- Approval or rejection of Certificate Applications
- Certificate Issuance and Revocations
- Management of the CA key, including issuance or destruction of a CA certificate

6.3. Personnel Security Controls

6.3.1. Qualifications, Experience, and Clearance Requirements

SSL.com follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. All SSL.com employees must have the necessary qualifications or experience to fulfill their job descriptions.

6.3.2. Background Check Procedures

Background checks are performed on all trusted personnel before access is granted to SSL.com's systems. These checks include, but are not limited to, credit history, employment history (for references), and a Companies House cross-reference to disqualified directors.

6.3.3. Training Requirements

Personnel training occurs via a mentoring process involving senior members of the team to which the employee is attached. SSL.com periodically reviews and enhances its training programs as necessary.

Training programs are tailored toward each individual's job responsibilities and include training on PKI concepts, job responsibilities, operational policies and procedures, incident handling and reporting, and disaster recovery procedures.

6.3.4. Retraining Frequency and Requirements

SSL.com provides refresher training courses to its personnel in order to ensure that all such personnel can competently and satisfactorily perform their job responsibilities.

6.3.5. Job Rotation Frequency and Sequence

No Stipulation

6.3.6. Sanctions for Unauthorized Actions

Any personnel found violating a SSL.com policy or procedure is subject to disciplinary action. The action taken by SSL.com depends on the circumstances surrounding the action, the severity of the violation, and the personnel's past performance. In some cases, disciplinary action may include the personnel's termination.

6.3.7. Independent Contractor Requirements

If an independent contractor or consultant is used, SSL.com shall first ensure that each such contractor or consultant is first obligated to abide by the same functional and security criteria that are set forth herein. Contractors and consultants are subject to the same sanctions as other personnel as set forth in Section 5.3.6.

6.3.8. Documentation Supplied to Personnel

SSL.com supplies its personnel with the training and documentation needed to perform their job responsibilities. SSL.com personnel understand and are obligated and required to safe guard and protect all private and confidential information to which they might have access.

6.4. Audit Logging Procedures

6.4.1. Types of Events Recoded

For audit purposes, SSL.com maintains electronic or manual logs of the following events for core functions.

CA & Certificate Lifecycle Management

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber certificate life cycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances and certificate renewals
- Subscriber certificate revocation requests, including the reason for the revocation
- Subscriber changes of affiliation that would invalidate the validity of an existing certificate
- Certificate Revocation List updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a private key

Security Related Events

- System downtime, software crashes, and hardware failures
- CA system actions performed by SSL.com personnel, including software updates, hardware replacements, and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service, or repair and retirement
- Successful and unsuccessful SSL.com PKI access attempts
- Secure CA facility visitor entry and exit

Certificate Application Information

- The documentation and other related information presented by the applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

An audit log is maintained of each movement of the removable media.

6.4.2. Frequency of Processing Log

Logs are review on a weekly basis by CA management.

6.4.3. Retention Period of Audit Log

Logs are archived by the system administrator on a weekly basis by the system administrator. Logs are thereafter retain as part of the record archive as set forth in Section 5.5.

6.4.4. Protection of Audit Log

All logs are backed up on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by SSL.com staff on a visit to the data center, and when not in the data center are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

6.4.5. Audit Log Backup Procedures

Logs are archived by the system administrator on a weekly basis by the system administrator. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the certificates of destruction are archived.

6.4.6. Audit Collection System

Audit data is generated both automatically and manually. Automatic logs are computer-generated and are based off of set security protocols, scans, and alerts. Manual audits are recorded and stored by SSL.com personnel.

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

6.4.7. Notification to Event-Causing Subject

Notice of audited events are confidential information and no notice is given to individuals or organizations unless required by law or agreement.

6.4.8. Vulnerability Assessments

Events in the audit process are logged to monitor vulnerabilities. SSL.com periodically reevaluates its security procedures and updates them as may be required.

6.5. Records archival

6.5.1. Types of records archived

The following information may be archived:

- Information or documentation submitted by Subscribers in support of a certificate application.
- Copies of certificates, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that SSL.com may see fit.
- Audit logs
- Other records deemed important and valuable to the SSL.com business operations

6.5.2. Retention period for archive

SSL.com retains the records of SSL.com digital certificates and the associated documentation for a term of than 7 years, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation.

6.5.3. Protection of archive

Records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

6.5.4. Archive backup procedures

SSL.com regularly backs up electronic archives. Copies are maintained of paper files.

6.5.5. Requirements for time-stamping of records

Certificates, CRLs, and other archived information shall contain time and date information that may or may not be cryptographic-based.

6.5.6. Archive collection system

The SSL.com archive collection system is an internal system.

6.5.7. Procedures to obtain and verify archive information

Only authorized trusted personnel are permitted access to the archive. Subscribers may obtain copies of archived information related to their Certificate upon written request and payment of any associated costs.

6.6. Key changeover

Towards the end of each private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in section 6.1 of this CPS.

6.7. Compromise and disaster recovery

6.7.1. Incident and compromise handling procedures

To maintain its CA operations when an incident occurs, SSL.com makes a backup of critical CA software is performed weekly and is stored off-site. SSL.com also performs a backup of critical business information is performed daily and is stored off-site Further, SSL.com operations are distributed across several sites world wide. All sites offer facilities to manage the life-cycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates.

6.7.2. Computing resources, software, and/or data are corrupted

SSL.com operates a fully redundant CA system. The backup CA is readily available in the event that the primary CA should cease operation. All of SSL.com's critical computer equipment is housed in a co-location facility run by a commercial data-center, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows SSL.com to specify a maximum system outage time (in case of critical systems failure) of 1 hour.

As well as a fully redundant CA system, SSL.com maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that SSL.com will endeavor to minimize interruptions to its CA operations.

6.7.3. Business continuity capabilities after a disaster

To maintain the integrity of its services SSL.com implements, documents and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plans are revised and updated as may be required at least once a year.

6.8. CA termination

In the event that it is necessary for SSL.com to cease operation, SSL.com shall make a commercially reasonable effort to notify Participants of such termination in advance of the effective date of the termination. Should SSL.com cease its CA operations, SSL.com shall develop a termination plan to minimize the disruption of services to its customers, Subscribers, and Relying Parties. The plan shall provide for:

- Revocation of Certificates issued to the CA
- Revocation of unexpired and unrevoked Certificates as may be necessary
- Preservation of the CA's archives and records as required by this CPS
- Continuation of customer support services
- Providing to affected parties and how to address the cost of such notice
- Transition of the services to the CA's successor
- Disposition of the CA's private key
- Refunds (if necessary)
- Continuation of revocation services

7. TECHNICAL SECURITY CONTROLS

SSL.com's operational sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities. This section of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

7.1. Key pair generation and installation

7.1.1. Key pair generation

SSL.com securely generates and protects its own private key(s), using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The SSL.com CA Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

The Subscriber is solely responsible for the generation of the private key used in the certificate request. SSL.com does not provide key generation, escrow, recovery or backup facilities.

Upon making a certificate application, the Subscriber is solely responsible for the generation of an RSA key pair appropriate to the certificate type being applied for. During application, the Subscriber will be required to submit a public key and other personal / corporate details in the form of a Certificate Signing Request (CSR).

Secure Server Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software.

Code Signing Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in Microsoft Internet Explorer.

Secure Email Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in popular browsers.

7.1.2. Private key delivery to subscriber

SSL.com provides the full certificate chain to the Subscriber upon issuance and delivery of the Subscriber certificate. SSL.com incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the digital certificate.
- Any other applicable certificate policy as may be stated on an issued SSL.com certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customized elements of the standard X.509v3.
- 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.

Delivery of Subscriber certificates to the associated Subscriber is dependent on the certificate product type:

7.1.2.1. Secure Server Certificate

If SSL.com's domain databases hold sufficient validation information, an automatic validation of the Certificate Application may take place. In the event of such an automated validation the Certificate is delivered to commonly used generic email addresses ordinarily belonging to authorized personnel at the domain name used in the application, such as webmaster@... admin@... postmaster@... Confirmation of the certificate delivery location is provided to the administrator contact provided during the application process. If the Certificate is validated outside of SSL.com's databases, then the secure server certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

7.1.2.2. Code Signing Certificates

Code Signing Certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

7.1.2.3. Delivery of other Certificates

Unless otherwise specified through an amendment to this CPS, all other Certificates shall be delivered to the relevant party through email using a Subscriber-provided email address.

7.1.2.4. Secure Email Certificate

Upon issuance of a Secure Email Certificate, the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original certificate request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the private key corresponding to the public key submitted during application. Pending a successful challenge, the issued certificate is installed automatically onto the Subscriber's computer.

7.1.3. Public key delivery to certificate issuer

Secure Server Certificate requests are generated using the Subscriber's webserver software and the request is submitted to SSL.com in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the SSL.com website or through a SSL.com approved RA.

Secure Email Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted to SSL.com in the form of a PKCS#10 Certificate Signing Request (CSR). The Subscriber's browser generally makes submission automatically.

Code Signing Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted automatically to SSL.com in the form of a PKCS#10 Certificate Signing Request (CSR).

The private key may either be allowed to remain in the cryptographic service provider, or may be exported to the subscriber's hard drive.

7.1.4. CA public key delivery to relying parties

SSL.com makes all its CA Root Certificates available in online repositories at www.ssl.com/repository.

The UTN USERFirst Hardware certificate is present in Explorer 5.01 and above, Netscape 8.1 and above, Opera 8.0 and above, Mozilla 1.76 and above, Konqueror 3.5.2 and above, Safari 1.2 and above, FireFox 1.02 and above, Camino and SeaMonkey and is made available through these browsers.

The AddTrust External CA Root certificate is present in Netscape 4.x and above, Opera 8.00 and above, Mozilla .06 and above, Konqueror, Safari 1.0 and above, Camino and SeaMonkey and is made available to relying parties through these browsers.

7.1.5. Key sizes

Key pairs are of sufficient length to prevent unauthorized determination or reverse engineering of the private key. Most keys are 2048 bit keys, however some 1024 bit intermediate keys exist. See Appendix A for the size of each issued key.

7.1.6. Public key parameters generation and quality checking

SSL.com securely generates and protects its own private key(s), using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The SSL.com CA Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

7.1.7. Key usage purposes (as per X.509 v3 key usage field)

The key usage field extension in SSL.com Certificates specifies the purpose for which the Certificate may be used. Enforcement of the limitations of use found in this field are beyond SSL.com's control as its correct use is highly dependent on having the correct software.

7.2. Private Key Protection and Cryptographic Module Engineering Controls

SSL.com protects its CA Root key pairs in accordance with this CPS.

7.2.1. Cryptographic module standards and controls

Comodo CA Limited protects the UTN and AddTrust CA Root key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo's WebTrust compliance are available at its official website (www.comodogroup.com).

SSL.com private keys are generated and store on an IBM 4758 accredited to FIPS PUB 140-1 level 4.

7.2.2. Private key (n out of m) multi-person control

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across **m** removable media and requires **n** of **m** to reconstruct the decryption key. Custodians in the form of two or more authorized SSL.com officers are required to physically retrieve the removable media from the distributed physically secure locations.

7.2.3. Private key escrow

SSL.com does not escrow private keys.

7.2.4. Private key backup

SSL.com's CA keys are generated and stored inside cryptographic hardware. The keys are backed up and transferred in an encrypted form.

The Subscriber is solely responsible for protection of their private keys. SSL.com maintains no involvement in the generation, protection or distribution of such keys.

SSL.com strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber private key.

7.2.5. Private key archival

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration.

7.2.6. Private key transfer into or from a cryptographic module

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

7.2.7. Private key storage on cryptographic module

SSL.com private keys are generated and store on an IBM 4758 accredited to FIPS PUB 140-1 level 4.

7.2.8. Method of activating private key

SSL.com's private keys are activated according to the specifications of the cryptographic hardware manufacturer. Subscriber's are responsible for protecting their own private keys and should take commercially reasonable steps to prevent physical or logical unauthorized access to a private key. This might include using a windows logon or screensaver password.

7.2.9. Method of deactivating private key

All deactivated private keys should be kept in an encrypted form only. Keys are deactivated by logging off their system. Root keys are further deactivated by removing them from their storage partition.

7.2.10. Method of destroying private key

Private keys are destroyed by deleting them from all known storage partitions and then by zeroing or by physically destroying the hardware on which they were stored. All CA key destruction activities are logged.

7.2.11. Cryptographic Module Rating

See Section 6.2.1.

7.3. Other aspects of key pair management

SSL.com conducts the overall certification management within the SSL.com PKI. SSL.com is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

7.3.1. Public key archival

SSL.com retains copies of all Public Keys in its archive via its routine backup procedures and as described in Section 5.5.

7.3.2. Certificate operational periods and key pair usage periods

The operational period of each Certificate generated ends upon its revocation of expiration. The operational period of each CA key is set forth in Appendix A.

The validity period of SSL.com certificates varies dependent on the certificate type, but typically, a certificate will be valid for 1 to 5 years. SSL.com reserves the right to, at its discretion, issues certificates that may fall outside of these set periods.

7.4. Activation data

7.4.1. Activation data generation and installation

SSL.com activates the cryptographic module containing its private keys according the specifications set forth by the hardware manufacture and meets the requirements of FIPS 140-2 Level 4. All cryptographic hardware is under two-personnel control.

All SSL.com personnel are required to use strong passwords (non-dictionary alphanumeric passwords with a minimum length that are changed on a regular basis) to protect sensitive information.

7.4.2. Activation data protection

Data is protected using strong passwords as described in 6.4.1.

7.4.3. Other aspects of activation data

All activation is transmitted, stored, and destroyed using methods and procedures that protect against loss, theft, modification, or any other unauthorized access, loss, or use.

7.5. Computer security controls

The SSL.com CA Infrastructure uses trustworthy systems to provide certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

7.5.1. Specific computer security technical requirements

SSL.com computer systems are set up and maintained in a secure manner that prevents unauthorized access. SSL.com uses software and hardware that constitute the industry's best practice in security measures.

Computers are password protected and require a strong password for access. All passwords are changed on a regular basis. Computers are fire walled and scanned regularly for viruses, spyware, Trojans, and other malware.

7.5.2. Computer security rating

No Stipulation.

7.6. Life cycle technical controls

7.6.1. System development controls

SSL.com closely controls and monitors its CA systems and software development. All systems and software are developed and implemented in accordance with industry standards. All systems and software are routinely checked for malware and security issues.

7.6.2. Security management controls

SSL.com controls and monitors the configuration and operation of its CA systems. Changes in Security-related changes are logged and processed. SSL.com periodically reviews and updates its security policy and controls to ensure that no unauthorized access is allowed.

7.6.3. Life cycle security controls

No Stipulation.

7.7. Network security controls

SSL.com performs all of its CA functions on secured networks to prevent unauthorized access and other malicious activity.

7.8. Time-stamping

Certificates, CRLs, and OCSP entries shall contain time and date information about the Certificate, CRL, or OCSP information. Such information may not be cryptographic based.

8. CERTIFICATE, CRL, AND OCSP PROFILES

SSL.com currently offers a portfolio of digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications.

SSL.com offers a range of distinct certificate types. The different certificate types have differing intended usages and differing policies. Pricing and subscriber fees for the certificates are made available on the relevant official SSL.com websites. The maximum warranty associated with each certificate is set forth in Appendix E of this CPS.

As the suggested usage for a digital certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific certificate.

SSL.com may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of SSL.com products creates no claims by any third party. If necessary, SSL.com shall amend this CPS upon the inclusion of a new certificate product in the SSL.com hierarchy. The CPS shall usually be made public on the official SSL.com websites at least seven (7) days prior to the offering such new product.

Suspended or revoked certificates are appropriately referenced in the CRL and/or OCSP.

8.1. Certificate profile

SSL.com certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on a SSL.com certificate, the relying party must use X.509v3 compliant software.

8.1.1. Version number(s)

All SSL.com certificates are X.509 version 3 certificates.

8.1.2. Certificate extensions

SSL.com uses the standard X.509, version 3 to construct digital certificates for use within the SSL.com PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. SSL.com uses a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for digital certificates.

8.1.2.1. Key Usage Extension field

SSL.com certificates include key usage extension fields to specify the purposes for which the certificate may be used and to technically limit the functionality of the certificate when used with

X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of SSL.com. SSL.com assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. SSL.com cannot warrant that any such user software will support and enforce the controls required by SSL.com. All software use is left to the user's sole discretion.

The possible key purposes identified by the X.509v3 standard are the following:

a) Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity
b) Non-repudiation, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below)
c) Key encipherment, for enciphering keys or other security information, e.g. for key transport
d) Data encipherment, for enciphering user data, but not keys or other security information as in c) above
e) Key agreement, for use as a public key agreement key
f) Key certificate signing, for verifying a CA's signature on certificates, used in CA certificates only
g) Encipher only, public key agreement key for use only in enciphering data when used with key agreement
h) Decipher only, public key agreement key for use only in deciphering data when used with key agreement

8.1.2.2. Extension Criticality Field

The Extension Criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

8.1.2.3. Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-entity. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of SSL.com.

8.1.3. Algorithm object identifiers

SSL.com uses the UTN-USERFIRST-Hardware and AddTrust External CA Root for its Root CA Certificates. This allows SSL.com to issue highly trusted digital certificates by inheriting the trust level associated with the UTN root certificate (named "UTN-USERFIRST-Hardware") and the AddTrust root certificate (named "AddTrust External CA Root"). The high-level representation of the SSL.com PKI set forth in Appendix C is used to illustrate the hierarchy utilized.

8.1.4. Name forms

SSL.com Certificates following the naming policy set forth in Section 3.1.1.

8.1.5. Name constraints

No Stipulation

8.1.6. Certificate policy object identifier

Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy.

Specific SSL.com certificate profiles are provided in Appendix D.

8.1.7. Usage of Policy Constraints extension

No Stipulation

8.1.8. Policy qualifiers syntax and semantics

SSL.com usually includes information in the Policy Qualifier field of the Certificate Policy extension that puts Relying Parties on notice of the location of its CPS. This field usually includes a URL that points the Relying Party to the CPS where they can find out more about the limitations on liability and other terms and conditions governing the use of the Certificate.

8.1.9. Processing semantics for the critical Certificate Policies extension

No Stipulation.

8.2. CRL profile

SSL.com manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by SSL.com are X.509v2 CRLs, in particular as profiled in RFC3280.

8.2.1. Version number(s)

CRLs conform to RFC 3280 and contain the basic fields listed below:

Version	[Version 1]	
Issuer Name	CountryName = [Root Certificate Country Name], OrganizationName=[Root Certificate Organization], CommonName=[Root Certificate Common Name] [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 24 hours]	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

8.2.2. CRL and CRL entry extensions

No Stipulation.

8.3. OCSP profile

OCSP is way for users to obtain information about the revocation status of a SSL.com issued Certificate. SSL.com uses OCSP to provide information about all of its certificates. OCSP responders conform to RFC 2560.

8.3.1. Version Number(s)

SSL.com uses Version 1 of the OCSP specification as defined by RFC2560.

8.3.2. OCSP Extensions

SSL.com's uses timestamp and validity periods to establish the accuracy of each OCSP response. SSL.com does not use a cryptographic nonce in connection with its OCSP services. Instead, local time should be used by participants to ensure the freshness of the OCSP response.

9. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

9.1. Frequency or Circumstances of Assessment

An annual audit is performed by an independent external auditor to assess SSL.com's compliance with the AICPA/CICA WebTrust program for Certification Authorities.

9.2. Identity/Qualifications of Assessor

SSL.com's audits are performed by a public accounting firm that:

- Is a highly reputable accredited accounting firm that is a member of the American Institute of Certified Public Accountants (AICPA)
- Has significant quality assurance mechanisms, including peer review, competency testing, and other measures.
- Abides by and conforms with the applicable standards and best practices as set forth by the relevant standards committees.
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology, data centers, personnel controls, and other relevant fields of interest.
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology.

9.3. Assessor's Relationship to Assessed Entity

The Assessor is independent of SSL.com and does not have any financial interest or course of dealings with SSL.com that could foreseeably create a significant bias in the Assessor's evaluation.

9.4. Topics Covered by Assessment

Topics covered by the annual audit include but are not limited to the following:

- CA business practices disclosure
- Service integrity
- CA environmental controls

9.5. Actions Taken as a Result of Deficiency

If any material noncompliance or deficiencies are discovered during an audit, then SSL.com shall create and implement a plan to cure such deficiencies or noncompliance. The plan shall be created by SSL.com management with input from the auditing agent. In the event that the deficiency cannot be resolved, SSL.com may revoke any certificates affected by deficiency or noncompliance.

9.6. Communication of Results

The results of each audit are reported directly to SSL.com management and any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement. Audit results may also be published by SSL.com in SSL.com's sole and absolute discretion.

10. OTHER BUSINESS AND LEGAL MATTERS

This part of the CPS describes the business matters of SSL.com and legal representations, warranties and limitations associated with SSL.com digital certificates.

10.1. Fees

10.1.1. Certificate Issuance or Renewal Fees

SSL.com charges Subscriber fees for some of the certificate services it offers, including issuance, and renewal. Such fees are detailed on the official SSL.com websites (www.ssl.com). SSL.com retains its right to affect changes to such fees.

10.1.2. Certificate Access Fees

Currently, SSL.com does not charge a fee for Certificate Access, but reserves the right to establish and charge a reasonable fee for access to its database of certificates. Charges may be incurred for extensive or time consuming searches. Fees for such extensive used are negotiated on an individual basis.

10.1.3. Revocation or Status Information Access Fees

SSL.com does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a SSL.com issued certificate using its OCSP.

10.1.4. Fees for Other Services

Fees for other services offered by SSL.com are set either within the individual agreements with the parties or are detailed on the official SSL.com websites (www.ssl.com) depending on the Services required. Fees may be discussed for other services by contacting SSL.com at:

SSL.com Certification Authority
2260 W Holcombe Blvd Ste 700
Houston, Texas
US

or by using the contact telephone numbers and addresses listed on any one of the websites listed.

10.1.5. Refund Policy

SSL.com offers a 30-day refund policy. During a 30-day period (beginning when a certificate is first issued), the Subscriber may request a full refund for their certificate. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant. SSL.com is not obliged to refund a certificate after the 30-day reissue policy period has expired.

10.2. Financial Responsibility

10.2.1. Insurance Coverage

SSL.com maintains errors and omissions insurance coverage.

10.2.2. Other Assets

No Stipulation

10.2.3. Insurance or Warranty Coverage for End-Entities

If SSL.com was negligent in issuing a digital certificate that resulted in a loss to a Relying Party, Relying Party may be eligible under SSL.com's certificate warranty to receive reimbursement for any damages caused, subject to the limitations of SSL.com's insurance policy. Except to the extent of willful misconduct, the liability of SSL.com is limited to the negligent issuance of certificates. The cumulative maximum liability of SSL.com to all applicants, subscribers and relying parties for each certificate is set forth in the table in Appendix E.

Under SSL.com's warranty a covered person may only receive the maximum payment per online transaction listed in Schedule E ("Incident Limit") for which the Covered Person claims there was a breach of the SSL.com Warranty (each an "Incident"). If multiple Covered Persons are affiliated as to a common entity, then those multiple Covered Persons collectively are eligible to receive the maximum amount per Incident. Any payments to Covered Persons shall decrease by an amount equal to the sum of such payments the relevant Aggregate Limit available to any party for future payments for any claims relating to that Digital Certificate. For example, if a Digital Certificate carries a Payment Limit of $10,000 and a per incident limit of $1,000, then Covered Persons can receive payments in accordance with this warranty for up to $1,000 per Incident until a total of $10,000 has been paid in the aggregate for all claims by all parties related to that Digital Certificate. Upon renewal of any Digital Certificate, the total claims paid for such Digital Certificate shall be reset to zero dollars.

SSL.com certificates may only be used in connection with data transfer and transactions having a US dollar (US$) value no greater than the max transaction value associated with the certificate and detailed in the table in Appendix E of this CPS.

10.3. Confidentiality of Business Information

SSL.com observes applicable rules on the protection of personal data deemed by law or the SSL.com privacy policy to be confidential.

10.3.1. Scope of Confidential Information

SSL.com keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Executed Subscriber agreements.
- Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports, except for WebTrust audit reports that may be published at the discretion of SSL.com.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of SSL.com infrastructure, certificate management and enrollment services and data.

10.3.2. Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all certificates issued by the SSL.com CA is public information. Subscriber application data marked as "Public" in the relevant subscriber agreement and submitted as part of a certificate application is published within an issued digital certificate in accordance with this CPS.

10.3.3. Responsibility to Protect Confidential Information

All personnel in trusted positions handle all information in strict confidence. SSL.com is not required to and does not release any confidential information, unless otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom SSL.com owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

10.4. Privacy of Personal Information

10.4.1. Privacy Plan

SSL.com has implemented a privacy policy, which complies with this CPS. The SSL.com privacy policy is published at the SSL.com repository at www.ssl.com/repository.

10.4.2. Information Treated as Private

Any information about Subscribers that is not publicly accessible or available through the content of the issued certificate, a CRL, or the OCSP is treated as private information.

10.4.3. Information Not Deemed Private

Certificates, CRLs, the OCSP, and the information appearing in them are not considered private.

10.4.4. Responsibility to Protect Private Information

All SSL.com employees receiving private information are responsible to protect such information from compromise and disclosure to third parties. Each party shall use the same degree of care that it exercises with respect to its own information of like importance, but in no event shall the degree of care be less than a reasonable degree of care.

10.4.5. Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, the applicable privacy policy, or by agreement, a party will not use private information without the subject's express written consent.

10.4.6. Disclosure Pursuant to Judicial or Administrative Process

SSL.com shall be entitled to disclose any confidential or private information, if SSL.com believes, in good faith, that the disclosure is necessary in response to subpoenas and search warrants or if disclosure is necessary in response to a pending legal proceeding.

10.4.7. Other Information Disclosure Circumstances

No Stipulation.

10.5. Intellectual Property Rights

SSL.com or its partners or associates own all intellectual property rights associated with its databases, web sites, SSL.com digital certificates and any other publication originating from SSL.com including this CPS.

10.5.1. Certificates

Certificates are the property of SSL.com. SSL.com gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. SSL.com reserves the right to revoke the certificate at any time. Private and public keys are property of the subscribers who rightfully issue and hold them. All secret shares (distributed elements) of the SSL.com private key remain the property of SSL.com.

Subscribers represent and warrant that when submitting to SSL.com and using a domain and distinguished name (and all other certificate application information), they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to the third party's trademarks, service marks, trade names, company names, or any other intellectual property right, and that the subscriber is not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective

business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

10.5.2. Copyright

This CPS is copyrighted by SSL Corp. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of SSL.com. Requests for any other permission to reproduce this SSL.com document (as well as requests for copies from SSL.com) must be addressed to:

SSL.com Certification Authority
2260 W Holcombe Blvd Ste 700
Houston, Texas
US

10.5.3. Trademarks

“SSL.com” and other terms in this CPS are trademarks of SSL.com and may only be used by permission.

10.5.4. Infringement

Although SSL.com will provide all reasonable assistance, certificate subscribers shall defend, indemnify, and hold SSL.com harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of SSL.com.

10.6. Representations and Warranties

Subscribers, relying parties and any other parties shall not interfere with or reverse engineer the technical implementation of SSL.com PKI services, including, but not limited to, the key generation process, the public web site, and the SSL.com repositories except as explicitly permitted by this CPS or upon prior written approval of SSL.com. Failure to comply with this as a subscriber will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber, and the Subscriber shall pay any Charges payable but that have not yet been paid under this Agreement. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the SSL.com repository and any Digital Certificate or Service provided by SSL.com.

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

10.6.1. CA Representations and Warranties

To the extent specified in the relevant sections of the CPS, SSL.com promises to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the SSL.com Repository and web site for the operation of PKI 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 private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this CPS and fulfill its obligations presented herein.
- Publish accepted certificates in accordance with this CPS.
- Provide support to subscribers and relying parties as described in this CPS.
- Revoke certificates according to this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.
- Warrant the accuracy of information published on a Qualified Certificate issued pursuant to the requirements of the European Directive 99/93.
- Warrant that the signatory held the private key at the time of issuance of a certificate issued pursuant to the requirements for Qualified Certificates as in the European Directive 99/93.

The subscriber also acknowledges that SSL.com has no further obligations under this CPS.

10.6.2. RA Representations and Warranties

SSL.com does not employ the use of RAs.

10.6.3. Subscriber Representations and Warranties

Upon accepting a certificate, the subscriber represents to SSL.com and to relying parties that at the time of acceptance and until further notice:

- Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the subscriber and the certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorized person has ever had access to the subscriber's private key.
- All representations made by the subscriber to SSL.com regarding the information contained in the certificate are accurate and true.
- All information contained in the certificate is accurate and true to the best of the subscriber's knowledge or to the extent that the subscriber had notice of such information whilst the subscriber shall act promptly to notify SSL.com of any material inaccuracies in such information.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use a SSL.com certificate only in conjunction with the entity named in the organization field of a digital certificate (if applicable).
- The subscriber retains control of her private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The subscriber is an end-user subscriber and not a CA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise, unless expressly agreed in writing between subscriber and SSL.com.

- The subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of SSL.com.
- The subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

Unless otherwise stated in this CPS, subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own private / public key pair to be used in association with the certificate request submitted to SSL.com.
- Ensure that the public key submitted to SSL.com corresponds with the private key used.
- Ensure that the public key submitted to SSL.com is the correct one.
- Provide correct and accurate information in its communications with SSL.com.
- Alert SSL.com if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to SSL.com.
- Generate a new, secure key pair to be used in association with a certificate that it requests from SSL.com.
- Read, understand and agree with all terms and conditions in this SSL.com CPS and associated policies published in the SSL.com Repository at www.ssl.com/repository.
- Refrain from tampering with a SSL.com certificate.
- Use SSL.com certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- Cease using a SSL.com certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a SSL.com certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the subscriber's private key corresponding to the public key in a SSL.com issued certificate to issue end-entity digital certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a SSL.com certificate.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a SSL.com certificate.
- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their private keys.

10.6.4. Relying Party Representations and Warranties

A party relying on a SSL.com certificate accepts that in order to reasonably rely on a SSL.com certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; the relying party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.
- Study the limitations to the usage of digital certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a SSL.com digital certificate.
- Read and agree with the terms of the SSL.com CPS and relying party agreement.
- Verify a SSL.com certificate by examining the information available through SSL.com's OCSP.
- Trust a SSL.com certificate only if it is valid and has not been revoked or has expired.
- Rely on a SSL.com certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

10.6.5. Representations and Warranties of Other Participants

Partners of the SSL.com network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the SSL.com products and services. SSL.com partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the relying party, the removal of permission to use or access the SSL.com repository and any Digital Certificate or Service provided by SSL.com.

10.7. Disclaimers of Warranties

SSL.com disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law.

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93 SSL.com does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of SSL.com except as it may be stated in the relevant product description below in this CPS and in the SSL.com insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in SSL.com Personal certificates class 1, free, trial or demo certificates.
- In addition, shall not incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although SSL.com is responsible for the revocation of a certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless specifically stated by SSL.com.

Notwithstanding limitation warranties under the product section of this CPS, SSL.com shall not be responsible for non-verified subscriber information submitted to SSL.com, or the SSL.com directory or otherwise submitted with the intention to be included in a certificate, except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93.

In no event (except for fraud or willful misconduct) shall SSL.com be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS or the intended use of the ordered certificate as described on the SSL.com website or elsewhere.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a subscriber uses.
- Any liability that arises from compromise of a subscriber's private key.

10.8. Limitations of Liability

In no event (except for fraud or willful misconduct) will the aggregate liability of SSL.com to all parties including without any limitation a subscriber, an applicant, a recipient, or a relying party for all digital signatures and transactions related to such certificate exceed the cumulative maximum liability for such certificate as stated in the SSL.com insurance plan detailed in section 9.2.3 and Appendix E of this CPS.

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate through the OCSP services provided by SSL.com. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the subscriber.

Relying on an unverifiable digital signature may result in risks that the relying party, and not SSL.com, assumes in whole.

By means of this CPS, SSL.com has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at www.ssl.com/repository or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

SSL.com reserves its right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. SSL.com reserves the right not to disclose reasons for such a refusal.

SSL.com does not limit or exclude liability for death or personal injury.

10.9. Indemnities

10.9.1. Subscriber Indemnity to SSL.com

By accepting a certificate, the subscriber agrees to indemnify and hold SSL.com, as well as its agent(s) and contractors 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 SSL.com, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- Any false or misrepresented data supplied by the subscriber or agent(s).
- Any failure of the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, SSL.com, or any person receiving or relying on the certificate.
- Failure to protect the subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

For certificates issued at the request of a subscriber's agent, both the agent and the subscriber shall jointly and severally indemnify SSL.com, and its agents and contractors.

10.9.2. Subscriber Indemnity to Relying Parties

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

10.10. Term and Termination

10.10.1. Term

This CPS and any amendments hereto shall become effective seven days after being published to the Repository and shall remain effective until terminate in accordance with this Section 9.10.

10.10.2. Termination

This CPS and any amendments hereto shall remain effective until replaced with a newer version.

10.10.3. Effect of Termination and Survival

In case of termination of CA operations for any reason whatsoever, SSL.com will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, SSL.com will take the following steps, where possible:

- Providing subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoking all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Giving timely notice of revocation to each affected subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as SSL.com's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

10.11. Individual notices and Communications with Participants

SSL.com 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 SSL.com, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or SSL.comed sent mail, postage prepaid, return receipt requested, addressed as follows:

SSL.com Certification Authority
2260 W Holcombe Blvd Ste 700
Houston, Texas
US

10.12. Amendments

The SSL.com Certificate Policy Authority is responsible for determining the suitability of certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

10.12.1. Procedure for Amendment

Amendments to this CPS may be made from time to time by SSL.com. Amendments shall either be in the form of an amended form of the CPS or made available as a supplemental document on SSL.com's repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS and shall be indicated through appropriate revision numbers and publication dates. Revisions that are not deemed significant by SSL.com (those amendments or additions that have minimal or no impact on Subscribers or Relying Parties), shall be made without notice and without changing the version number of this CPS.

Controls are in place to reasonably ensure that the SSL.com CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

10.12.2. Notification Mechanism and Period

Upon the Certificate Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the SSL.com repository (available at www.ssl.com/repository), with seven (7) days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

10.12.3. Circumstances Under Which OID Must be Changed

If SSL.com decides that a change in SSL.com's Certificate Policy of Certificate Practices warrants a change in the currently specified OID for a particular Certificate type, then the revised CPS or amendment thereto will contain a revised OID for that type of certificate.

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 SSL.com of the dispute with a view to seek dispute resolution.

10.14. Governing Law

This CPS is governed by, and construed in accordance with the laws of the United States. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of SSL.com digital certificates or other products and services. U.S. law

applies in all SSL.com commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to SSL.com products and services where SSL.com acts as a provider, supplier, beneficiary receiver or otherwise.

10.15. Compliance with Applicable Law

Each party, including SSL.com partners, subscribers and relying parties, irrevocably agrees that the courts of the United States have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of SSL.com PKI services.

10.16. Miscellaneous Provisions

10.16.1. Entire Agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services and products of SSL.com and its international network of Registration Authorities as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS. When this CPS conflicts with other rules, guidelines, or contracts, this CPS shall prevail and bind the subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this CPS.
- Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

10.16.2. Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. 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.

10.16.3. Severability

If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

10.16.4. Enforcement

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision. Agreements between SSL.com and the parties detailed in this CPS may contain additional provisions governing enforcement and shall be enforced according to the terms and conditions set forth within each respective agreement.

SSL.com may seek indemnification and attorneys' fees from any party that violates their individual agreements with SSL.com or whose conduct is in violation of this CPS. Except where an express time frame is set forth in this CPS any delay or omission by any party shall not impair or be construed as a waiver of such right, remedy or power.

10.16.5. Force Majeure

SSL.com shall not be liable for any breach of its obligations, representations, warranties, or for its failure to perform where such failure or breach is as a result of a Force Majeure Event., including, but not limited to, fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, blockage, embargo, labor dispute, strike, lockout or interruption or failure of electricity or telephone service or any other system operated by any other party over which SSL.com has no control, or other similar causes beyond SSL.com's reasonable control where SSL.com is without fault or negligence.

10.17. Other Provisions

No Stipulation

APPENDIX A

CA KEYS

CA Number	Description	Usage	Lifetime	Size

APPENDIX B

CERTIFICATE TYPES

SSL.com Certificate offerings may include the following types of certificates:

1. Low Assurance Certificates

Low assurance (or Domain Validated) certificates are not used for authentication purposes and are ideal for mail servers and server to server communications. Entities purchasing these certificates receive limited validation by SSL.com. These certificates are used to ensure that the data being transmitted from one party to another is secure and are not intended for websites conducting e-commerce or other valued data transactions. A party transmitting data cannot be sure or guaranteed that the receiving party is the party named in the certificate. Due to increased validation speed, the lack of stringent validation, and the intended use of low assurance certificates, the certificates do not carry a warranty.

2. High Assurance Certificates

High assurance certificates are issued to both individuals and organization whose identity has first been verified according to the validation procedures described in section 4. High assurance certificates are intended for ecommerce use and may be used to conduct transactions of value.

3. SGC SSL Certificates

SGC SSL Certificates are professional level Server Gated Cryptography (SGC) enabled certificates designed to upgrade the encryption capabilities of older browsers from 40-bit encryption into full 128/256 bit encryption. SGC are high assurance certificates.

4. Trial Certificates

Trial certificates are designed to help customers use SSL in a test environment prior to the roll out of a full SSL solution. Trial Certificates may be used in an external environment and ultimately may contain information relied upon by Relying Party. Trial Certificates are free of charge but may only be used for testing purposes and do not come with a warranty. All Trial Certificates are validated in accordance with Section 4.2.1 prior to issuance.

5. Wildcard Certificates

Wildcard Certificates are used to secure multiple sub-domains with a single Certificate. Wildcard Certificates may be low assurance certificates or high assurance certificates.

6. MDCs

Multi Domain Certificates (MDCs) are Secure Server Certificates issued by SSL.com as a means of validation of domain control for the domains jointly hosted on a single server and named within the MDC. MDCs may be high assurance or low assurance certificates, but do not carry any warranty.

7. Code Signing Certificates

Code Signing Certificates are designed for commercial software developers to provide assurance regarding the developer's identity, and are designed to represent the level of assurance provided today by retail channels for software. With a Code Signing Certificate, a digital signature can be appended to the executable code itself, thus providing assurance to recipients that the code or software does indeed come from the signer of the software.

8. Secure Email Certificates

Secure Email Certificates, in combination with an S/MIME compliant email application, allow subscribers to digitally sign email for relying parties, or relying parties to encrypt email for the subscriber.

Secure Email Certificates are *non-validated*. SSL.com only validates the right for the applicant to use the submitted email address. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by SSL.com. The login details are sent via email to the address submitted during the certificate application.

Once logged into the online certificate collection facilities and prior to the installation of the Secure Email Certificate, SSL.com validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application process. If the automated challenge is successful, SSL.com will release the digital certificate to the subscriber.

APPENDIX C

PKI HEIRARCHY

1. Trial and Short Term Certificates

Visible on IE compatible browsers:

UTN-USERFIRST-Hardware (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd, expiry = 09 July 2019 19:19:22*)

- ↳ End Entity SSL/End Entity Secure Email (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

- ↳ UTN-USERFirst-Hardware (serial number = 48 4b ac f1 aa c7 d7 13 43 d1 a2 74 35 49 97 25, expiry = 30 May 2020 11:48:38)
  - ↳ End Entity SSL/End Entity Secure Email (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

2. 1-5 year SSL certificates

Visible on IE compatible browsers as follows:

UTN-USERFIRST-Hardware (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd, expiry = 09 July 2019 19:19:22*)

- ↳ End Entity SSL/End Entity Secure Email (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

- ↳ UTN-USERFirst-Hardware (serial number = 48 4b ac f1 aa c7 d7 13 43 d1 a2 74 35 49 97 25, expiry = 30 May 2020 11:48:38)
  - ↳ End Entity SSL/End Entity Secure Email (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

3. SGC / Platinum SGC / Multi-Domain certificates

Visible on IE compatible browsers as follows:

UTN - DATACorp SGC (*serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 20:06:40*)

- ↳ End Entity SSL (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

- ↳ UTN - DATACorp SGC (serial number = 53 7b 76 56 4f 29 7f 14 dc 69 43 e9 22 ad 2c 79, expiry = 30 May 2020 11:48:38)
  - ↳ End Entity SSL (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

4. Code Signing certificates

UTN-USERFirst-Object (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2d e0 b3 5f 1b, expiry = 09 July 2019 19:40:36*)

- End Entity (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

5. Secure Email / Client certificates

Visible on IE compatible browsers as follows:

UTN-USERFirst-Client Authentication and Email (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89, expiry = 09 July 2019 18:36:58*)

↳ End Entity (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN-USERFirst-Client Authentication and Email (serial number = 27 f4 ea 11 f4 7a 86 c4 6e 9d bb 6e a9 17 07 07, expiry = 30 May 2020 11:48:38)

↳ End Entity (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

APPENDIX D

CERTIFICATE POLICIES

SSL.com Server Certificates- Trial, High Assurance, Low Assurance, SGC		
Signature Algorithm	Sha1	
Issuer (non-SGC)	CN	SSL.com Free SSL CA / SSL.com High Assurance CA
	OU	(c)
	OU	Terms and Conditions of use: https://www.ssl.com/repository
	O	SSL.com
	C	US
Issuer (SGC)	CN	SSL.com Free SSL CA / SSL.com High Assurance CA
	OU	(c)
	OU	Terms and Conditions of use: https://www.ssl.com/repository
	O	SSL.com
	C	US
Validity	1-5 years	
Subject	CN	Common Name
	OU	SSL.com Free SSL / SSL.com High Assurance / SSL.com SGC
	OU (for Trial SSL only)	TEST USE ONLY - NO WARRANTY ATTACHED
	O	Organization
	OU	Organization Unit
	L	Locality
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Authority Key Identifier	KeyID only is specified.	
Key Usage (NonCritical)	Digital Signature, Key Encipherment(A0)	
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	

(Additional usages for SGC types only)	Microsoft SGC (1.3.6.1.4.1.311.10.3.3) Netscape SGC (2.16.840.1.113730.4.1)
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication(c0)
Basic Constraint	Subject Type = End Entity Path Length Constraint = None
Certificate Policies	[1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.38064.1.2.1.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: https://www.ssl.com/repository/ssl_v1_cps.pdf
CRL Distribution Policies	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<Primary CDP URL> [2]CRL Distribution Point Distribution Point Name: Full Name: URL=<Secondary CDP URL>
OCSP Distribution Policies	
Thumbprint Algorithm	SHA1
Thumbprint	

SSL.com Email Certificate		
Signature Algorithm	Sha1	
Issuer	CN	SSL.com Client Authentication and Email CA
	OU	(c)
	OU	Terms and Conditions of use: www.ssl.com/repository
	O	SSL.com
	C	US
Validity	1-5 years	

Subject (for Personal Emails)	E	*Email address*
	CN	*Common Name (name of subscriber)*
	OU	(c) 2008
	OU	*Terms and Conditions of use: www.ssl.com/repository/*
	OU	PERSONA NOT VALIDATED
Subject (for Corporate Emails)	E	Email address
	CN	Common Name (name of subscriber)
	OU	Corporate Secure Email
	O	Organization
	OU	Organization Unit
	L	Locality
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Authority Key Identifier	KeyID only is specified.	
Key Usage (NonCritical)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Netscape Certificate Type(	SMIME(20)	
Basic Constraint	Subject Type = End Entity Path Length Constraint = None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.38064.1.2.1.3.5 [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: https://www.ssl.com/repository/ssl_v1_cps.pdf	

CRL Distribution Policies	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<Primary CDP URL> [2]CRL Distribution Point Distribution Point Name: Full Name: URL=<Secondary CDP URL>
Thumbprint Algorithm	SHA1
Thumbprint	

SSL.com MDC		
Signature Algorithm	Sha1	
Issuer	CN	SSL.com High Assurance CA
	OU	
	O	SSL.com
	C	US
Validity	1-5 Years	
Subject	CN	Common Name [Name Windows displays as “Issued To” – Typically Entity Name like O field]
	O	*Organization*
	OU	*Organization Unit*
	L	*Locality*
	S	*Street*
	C	*Country*
	CN	*Domain Name 1*
	CN	*Domain Name 2*
	CN	*Domain Name 3 (etc to Domain Name 100)*
	CN	Common Name [Name Windows displays as “Issued To” – Typically Entity Name like O field]
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Microsoft SGC (1.3.6.1.4.1.311.10.3.3) Netscape SGC (2.16.840.1.113730.4.1)	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	

Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication(c0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.38064.1.2.1.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.ssl.com/repository/ssl_v1_cps.pdf
OCSP Distribution Points	
Authority Information Access	*[1]Authority Info Access* *Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)* *Alternative Name:* *URL=<Primary AIA URL>* *[2]Authority Info Access* *Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)* *Alternative Name:* *URL=<Secondary AIA URL>*
Subject Alternate Name	*DNS Name=Domain Name 1* *DNS Name=Domain Name 2* *DNS Name=Domain Name 3* *….up to* *DNS Name=Domain Name 100*
Thumbprint Algorithm	SHA1
Thumbprint	

Code Signing Certificate		
Signature Algorithm	Sha1	
Issuer	CN	SSL.com Object CA
	OU	http://www.ssl.com.
	O	SSL.com
	C	US
Validity	12-63 months	
Subject	CN	Common Name (name of subscriber)
	O	Organization

	OU	Organization Unit
	L	Locality
	STREET	Street
	S	State
	PostalCode	Zip or Postal Code
	C	Country
Authority Key Identifier	KeyID only.	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
Netscape Certificate Type	Signature (10)	
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.38064.1.2.1.3.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.ssl.com/repository/ssl_v1_cps.pdf	
OCSP Distribution Policies		
Subject Alternative Name	RFC822 Name = <Email Address>	
Thumbprint Algorithm	SHA1	
Thumbprint		

APPENDIX E

INSURANCE LIMITS

SSL.com Certificate Type	Max Transaction Value	Cumulative Max Liability
Low Assurance Certificates	$0	$0
High Assurance Certificates	$10,000	$100,000
Code Signing Certificate	$0	$50,000
Secure Email Certificate	$0	$0