

SSLGenie Certification Practice Statement

SSLGenie Certificate Services
MindGenies

Version 1.0
23 August 2007

www.sslgenie.com

1	General	6
1.1	SSLGenie	6
1.2	SSLGenie CPS	6
1.3	CPS Suitability, Amendments and Publication	6
1.4	Other Practice Statements & Agreements	6
1.5	Liability of SSLGenie	7
1.6	Compliance with applicable standards	7
1.7	Digital Certificate Policy Overview	7
1.8	SSLGenie PKI Hierarchy	8
1.8.1	High Assurance SSL Certificates	9
1.8.2	Code Signing / Time Stamping certificates	9
1.8.3	Client certificates	9
1.9	SSLGenie Certification Authority	9
1.10	SSLGenie Registration Authorities	10
1.10.1	SSLGenie Partners	10
1.10.2	EPKI Manager Account Holders	10
1.11	Subscribers	10
1.12	Relying Parties	11
2	Technology	12
2.1	SSLGenie CA Infrastructure	12
2.1.1	Root CA Signing Key Protection & Recovery	12
2.1.2	CA Root Signing Key Generation Process	12
2.1.3	CA Root Signing Key Archival	12
2.1.4	Procedures employed for CA Root Signing Key Changeover	12
2.1.5	CA Root Public Key Delivery to Subscribers	13
2.1.6	Physical CA Operations	13
2.2	Digital Certificate Management	13
2.3	SSLGenie Directories, Repository and Certificate Revocation Lists	13
2.4	Types of SSLGenie Certificates	14
2.4.1	SSLGenie Secure Server Certificates	14
2.4.2	SSLGenie Code Signing Certificates	15
2.4.3	SSLGenie Secure Email Certificates	16
2.5	Extensions and Naming	16
2.5.1	Digital Certificate Extensions	16
2.5.2	Incorporation by Reference for Extensions and Enhanced Naming	16
2.6	Subscriber Private Key Generation Process	16
2.7	Subscriber Private Key Protection and Backup	16
2.8	Subscriber Public Key Delivery to SSLGenie	17
2.9	Delivery of Issued Subscriber Certificate to Subscriber	17
2.9.1	Secure Server Certificate: Flash SSLGenie and wildcard	17
2.9.2	Secure Server Certificate: Premium SSLGenie, Premium SGC SSLGenie	17
2.9.3	Secure Email Certificate	17
2.10	Delivery of Issued Subscriber Certificate to Web Host SSLGenie Partner	17
2.11	Delivery of Issued Subscriber Certificate to EPKI Manager Account Holder	17
2.12	SSLGenie Certificates Profile	17
2.12.1	Key Usage extension field	17
2.12.2	Extension Criticality Field	18
2.12.3	Basic Constraints Extension	18
2.12.4	Certificate Policy (CP)	18
2.13	SSLGenie Certificate Revocation List Profile	21
3	Organisation	22
3.1	Conformance to this CPS	22
3.2	Termination of CA Operations	22

3.3	<i>Form of Records</i>	22
3.4	<i>Records Retention Period</i>	22
3.5	<i>Logs for Core Functions</i>	22
3.5.1	CA & Certificate Lifecycle Management	23
3.5.2	Security Related Events	23
3.5.3	Certificate Application Information	23
3.5.4	Log Retention Period	23
3.6	<i>Business Continuity Plans and Disaster Recovery</i>	23
3.7	<i>Availability of Revocation Data</i>	23
3.8	<i>Publication of Critical Information</i>	24
3.9	<i>Confidential Information</i>	24
3.9.1	Types of Information deemed as Confidential	24
3.9.2	Types of Information not deemed as Confidential	24
3.9.3	Access to Confidential Information	24
3.9.4	Release of Confidential Information	24
3.10	<i>Personnel Management and Practices</i>	24
3.10.1	Trusted roles.....	24
3.10.2	Personnel controls	24
3.11	<i>Privacy Policy</i>	24
3.12	<i>Publication of information</i>	25
4	Practices and Procedures	26
4.1	<i>Certificate Application Requirements</i>	26
4.1.1	SSLGenie Partner Certificate Applications.....	26
4.1.2	EPKI Manager Account Holder Certificate Applications	26
4.1.3	Methods of application.....	26
4.2	<i>Application Validation</i>	26
4.2.1	Secure Server Certificate – Premium SSLGenie and Premium SGC SSLGenie Application Four Step Validation Process	26
4.2.2	Secure Server Certificate – Flash SSLGenie Application One Step Validation Process	27
4.2.3	Code Signing Certificate Application Four Step Validation Process	27
4.2.4	Secure Email Certificate	28
4.3	<i>Validation Information for Certificate Applications</i>	28
4.3.1	Application Information for Organisational Applicants.....	28
4.3.2	Supporting Documentation for Organisational Applicants	28
4.3.3	Application Information for Individual Applicants.....	29
4.3.4	Supporting Documentation for Individual Applicants	29
4.4	<i>Validation Requirements for Certificate Applications</i>	29
4.4.1	Third-Party Confirmation of Business Entity Information	29
4.4.2	Serial Number Assignment	30
4.5	<i>Time to Confirm Submitted Data</i>	30
4.6	<i>Approval and Rejection of Certificate Applications</i>	30
4.7	<i>Certificate Issuance and Subscriber Consent</i>	30
4.8	<i>Certificate Validity</i>	30
4.9	<i>Certificate Acceptance by Subscribers</i>	30
4.10	<i>Verification of Digital Signatures</i>	30
4.11	<i>Reliance on Digital Signatures</i>	30
4.12	<i>Certificate Suspension</i>	31
4.13	<i>Certificate Revocation</i>	31
4.13.1	Request for Revocation	31
4.13.2	Effect of Revocation	31
4.14	<i>Renewal</i>	31
4.15	<i>Notice Prior to Expiration</i>	32
5	Conditions of Issuance	33
5.1	<i>SSLGenie Representations</i>	33
5.2	<i>Information Incorporated by Reference into a SSLGenie Digital Certificate</i>	33
5.3	<i>Displaying Liability Limitations, and Warranty Disclaimers</i>	33
5.4	<i>Publication of Certificate Revocation Data</i>	33

5.5	<i>Duty to Monitor the Accuracy of Submitted Information</i>	33
5.6	<i>Publication of Information</i>	33
5.7	<i>Interference with SSLGenie Implementation</i>	33
5.8	<i>Standards</i>	33
5.9	<i>SSLGenie Partnerships Limitations</i>	33
5.10	<i>SSLGenie Limitation of Liability for a SSLGenie Partner</i>	34
5.11	<i>Choice of Cryptographic Methods</i>	34
5.12	<i>Reliance on Unverified Digital Signatures</i>	34
5.13	<i>Rejected Certificate Applications</i>	34
5.14	<i>Refusal to Issue a Certificate</i>	34
5.15	<i>Subscriber Obligations</i>	34
5.16	<i>Representations by Subscriber upon Acceptance</i>	35
5.17	<i>Indemnity by Subscriber</i>	35
5.18	<i>Obligations of SSLGenie Registration Authorities</i>	35
5.19	<i>Obligations of a Relying Party</i>	35
5.20	<i>Legality of Information</i>	36
5.21	<i>Subscriber Liability to Relying Parties</i>	36
5.22	<i>Duty to Monitor Agents</i>	36
5.23	<i>Use of Agents</i>	36
5.24	<i>Conditions of usage of the SSLGenie Repository and Web site</i>	36
5.25	<i>Accuracy of Information</i>	36
5.26	<i>Obligations of SSLGenie</i>	36
5.27	<i>Fitness for a Particular Purpose</i>	37
5.28	<i>Other Warranties</i>	37
5.29	<i>Non-Verified Subscriber Information</i>	37
5.30	<i>Exclusion of Certain Elements of Damages</i>	37
5.31	<i>Certificate Insurance Plan</i>	38
5.31.1	Flash SSLGenie Certificate.....	38
5.31.2	Premium SSLGenie Certificate.....	38
5.31.3	Premium SGC SSLGenie Certificate	38
5.31.4	Code Signing Certificate.....	38
5.31.5	Secure Email Certificate	38
5.32	<i>Financial Limitations on Certificate Usage</i>	38
5.33	<i>Damage and Loss Limitations</i>	38
5.34	<i>Conflict of Rules</i>	38
5.35	<i>SSLGenie Intellectual Property Rights</i>	38
5.36	<i>Infringement and Other Damaging Material</i>	39
5.37	<i>Ownership</i>	39
5.38	<i>Governing Law</i>	39
5.39	<i>Jurisdiction</i>	39
5.40	<i>Dispute Resolution</i>	39
5.41	<i>Successors and Assigns</i>	39
5.42	<i>Severability</i>	39
5.43	<i>Interpretation</i>	39
5.44	<i>No Waiver</i>	40
5.45	<i>Notice</i>	40
5.46	<i>Fees</i>	40
5.47	<i>SSLGenie Reissue Policy</i>	40
5.48	<i>SSLGenie Refund Policy</i>	40
6	General Issuance Procedure	41

6.1	<i>General - SSLGenie</i>	41
6.2	<i>Certificates issued to Individuals and Organisations</i>	41
6.3	<i>Content</i>	41
6.3.1	Secure Server Certificates – Premium SSLGenie and Premium SGC SSLGenie	41
6.3.2	Secure Server Certificates – Flash SSLGenie	41
6.3.3	Code Signing Certificates	41
6.3.4	Secure Email Certificates.....	41
6.4	<i>Time to Confirm Submitted Data</i>	42
6.5	<i>Issuing Procedure</i>	42
Document Control		43

Terms and Acronyms Used in the CPS

Acronyms:

CA	Certificate Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
EPKI	Enterprise Public Key Infrastructure Manager
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
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

Terms:

Applicant:	The Applicant is an entity applying for a Certificate.
Subscriber:	The Subscriber is an entity that has been issued a certificate.
Relying Party:	The Relying Party is an entity that relies upon the information contained within the 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 and is available for reference at www.sslgenie.com/repository .
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.sslgenie.com/repository .
Certificate Policy:	The Certificate Policy is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context.

1 General

This document is the SSLGenie Certification Practice Statement (CPS) and outlines the legal, commercial and technical principles and practices that SSLGenie employ in providing certification services that include, but are not limited to, approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate based public key infrastructure (PKIX) in accordance with the Certificate Policies determined by SSLGenie. It also defines the underlying certification processes for Subscribers and describes SSLGenie's repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the SSLGenie PKI.

1.1 SSLGenie

SSLGenie is a Chain Certification Authority (CA) that issues high quality and highly trusted digital certificates to entities including private and public companies and individuals in accordance with this CPS. In its role as a CA, SSLGenie performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital certificate and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the SSLGenie PKI. In delivering its PKI services SSLGenie complies in all material respects with high-level international standards including those on Qualified Certificates pursuant to the European Directive 99/93 and the relevant law on electronic signatures and all other relevant legislation and regulation.

SSLGenie extends, under agreement, membership of its PKI to approved third parties known as Registration Authorities. The international network of SSLGenie RAs share SSLGenie's policies, practices, and CA infrastructure to issue SSLGenie digital certificates.

1.2 SSLGenie CPS

The SSLGenie CPS is a public statement of the practices of SSLGenie and the conditions of issuance, revocation and renewal of a certificate issued under SSLGenie's own hierarchy. Pursuant to the division of the tasks of a CA, this CPS is largely divided in the following sections: Technical, Organisational, Practices and Legal.

The SSLGenie Certificate Policy Authority maintains this CPS, related agreements and Certificate policies referenced within this document. The Certificate Policy Authority may be contacted at email: legal@sslgenie.com or by mail at:

MindGenies
C-22/28, Sector-57
Noida,Up
India-201301

This CPS, related agreements and Certificate policies referenced within this document are available online at www.sslgenie.com/repository.

1.3 CPS Suitability, Amendments and Publication

The SSLGenie 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. 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 SSLGenie repository (available at www.sslgenie.com/repository), with 7 days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

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 and CRLs issued by CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS.

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

1.4 Other Practice Statements & Agreements

The CPS is only one of a set of documents relevant to the provision of Certification Services by SSLGenie and that the list of documents contained in this clause are other documents that this CPS will from time to time mention, although this is not an exhaustive list. The document name, location of and status, whether public or private, are detailed below:

Document	Status	Location
SSLGenie Certification Practice Statement	Public	SSLGenie Repository: www.sslgenie.com/repository
Digital Certificate Terms & Conditions	Public	SSLGenie Repository: www.sslgenie.com/repository

Relying Party Agreement	Public	SSLGenie Repository: www.sslgenie.com/repository
Flash SSLGenie Certificate Subscriber Agreement	Public	SSLGenie Repository: www.sslgenie.com/repository
Premium SSLGenie Certificate Subscriber Agreement	Public	SSLGenie Repository: www.sslgenie.com/repository
Premium SGC SSLGenie Certificate Subscriber Agreement	Public	SSLGenie Repository: www.sslgenie.com/repository
Code Signing Certificate Subscriber Agreement	Public	SSLGenie Repository: www.sslgenie.com/repository
Secure Email Certificate Subscriber Agreement	Public	SSLGenie Repository: www.sslgenie.com/repository
Enterprise Public Key Infrastructure Manager Agreement	Confidential	Presented to partners accordingly
SSLGenie Agreement	Confidential	Presented to partners accordingly
Enterprise Public Key Infrastructure Manager Guide	Confidential	Presented to partners accordingly
SSLGenie Guide	Confidential	Presented to partners accordingly

1.5 Liability of SSLGenie

For legal liability of SSLGenie under the provisions made in this CPS, please refer to Section 4.

1.6 Compliance with applicable standards

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.

A regular audit is performed by an independent external auditor, to assess SSLGenie's compliancy with the AICPA/CICA WebTrust program for Certification Authorities. Topics covered by the annual audit include but are not limited to the following:

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

1.7 Digital Certificate Policy Overview

A digital certificate is formatted data that cryptographically binds an identified subscriber with a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

As detailed in this CPS, SSLGenie offer a range of distinct certificate types. The different certificate types have differing intended usages and differing policies.

Applicant	Certificate Type	Channels Available	Validation Levels ¹	Suggested Usage
Company or Organization	Secure Server Certificate: <i>FlashSSLGenie</i>	- SSLGenie Website - SSLGenie Network - EPKI Manager	1. Right to use the domain name used in the application. Approval email sent to domain name administrator's email. 2. The Whois database is used in the first instance, however if insufficient validation details are held, the application is manually validated.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session. Non-E-commerce website
Company or Organization	Secure Server Certificate: <i>Premium SSLGenie</i>	- SSLGenie Website - SSLGenie Network - EPKI Manager	1. Confirmation of right to use the business name used in the application using third party databases and / or business documentation plus right to use the domain name used in the application. 2. The application is manually validated. The applicant's name should be same with the name in Subscriber agreement that have its company seal, business license and the wire transfer payer's bank account	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session. E-commerce website.

¹ Validation levels: SSLGenie or a SSLGenie Registration Authority (if the application is made through a SSLGenie) conducts validation under strict guidelines provided to the Registration Authority. Section 1.10 of this CPS identifies the Registration Authorities and outlines the roles and responsibilities of such entities.

			information. 3. If the applicant's proof document is in Chinese, its organization name in the Certificate should be in Chinese, or it should be the normal English word translation name, or Pinyin name.	
Company or Organization	Secure Server Certificate: <i>Premium SGC SSLGenie</i>	- SSLGenie Website - SSLGenie Network - EPKI Manager	1. Confirmation of right to use the business name used in the application using third party databases and / or business documentation plus right to use the domain name used in the application. 2. The application is manually validated. The applicant's name should be same with the name in Subscriber agreement that have its company seal, business license and the wire transfer payer's bank account information. 3. If the applicant's proof document is in Chinese, its organization name in the Certificate should be in Chinese, or it should be the normal English word translation name, or Pinyin name.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session. E-commerce website. Financial Website
Company or Organization	Code Signing Certificate: <i>Code Signing Certificate</i>	- SSLGenie Website - SSLGenie Network - EPKI Manager	1. Confirmation of right to use the business name used in the application using third party databases and / or business documentation. 2. The application is manually validated. The applicant's name should be same with the name in Subscriber agreement that have its company seal, business license and the wire transfer payer's bank account information. 3. If the applicant's proof document is in Chinese, its organization name in the Certificate should be in Chinese, or it should be the normal English word translation name, or Pinyin name.	Recommended for any publisher who plans to distribute code or content over the Internet or corporate extranets and needs to assure the integrity and authorship of that code.
Individual, corporate representative, corporate	Secure Email Certificate: <i>Personal Version & Corporate Version</i>	- SSLGenie Website - SSLGenie Network - EPKI Manager	Email address search to ensure it is distinguished within the SSLGenie PKI. Email ownership automated challenge is conducted as part of the collection process. When opening an EPKI Account, applicant must provide confirmation of right to use the business name used in the application using third party databases and / or business documentation. Email address search to ensure it is distinguished within the EPKI Manager account. Company administering the EPKI Manager account must submit domain names for right to use validation prior to issuance of a Corporate Secure Email Certificate.	Allows certificate owner to digitally sign email to prove corporate authorship, and for relying parties to verify a digitally signed email and to encrypt email for the certificate owner. May also be used for web based access control where prior validation of the certificate owner is deemed necessary.

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.

1.8 SSLGenie PKI Hierarchy

SSLGenie uses Comodo CA (AICPA/CICA WebTrust Program for Certification Authorities approved security provider) for its Root CA Certificate. The partnership allows SSLGenie to issue highly trusted digital certificates by inheriting the trust level associated with Comodo's UTN (named "UTN-USERFIRST-Hardware") and AddTrust (named "AddTrust External CA Root") root certificates. The following high-level representation of the SSLGenie PKI is used to illustrate the hierarchy utilised.

1.8.1 High Assurance SSL Certificates

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*)

↳ Premium SSLGenie (*serial number = 30 72 b8 04 e0 85 d6 fe 1c 2e fc d6 ee a6 2d 9b, expiry = 30 May 2020 11:48:38*)

↳ End Entity SSL (*serial number = x, expiry = 1, 2, 3, 4, 5 years from issuance*)

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*)

↳ Premium SSLGenie (*serial number = 30 72 b8 04 e0 85 d6 fe 1c 2e fc d6 ee a6 2d 9b, expiry = 30 May 2020 11:48:38*)

↳ End Entity SSL (*serial number = x, expiry = 1, 2, 3, 4, 5 years from issuance*)

1.8.2 Low Assurance SSL Certificates

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*)

↳ Flash SSLGenie (*serial number = 18 ea c3 63 27 06 a1 d4 3e 00 1b 22 c0 2b 55 06, expiry = 30 May 2020 11:48:38*)

↳ End Entity SSL (*serial number = x, expiry = 1, 2, 3, 4, 5 years from issuance*)

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*)

↳ Flash SSLGenie (*serial number = 18 ea c3 63 27 06 a1 d4 3e 00 1b 22 c0 2b 55 06, expiry = 30 May 2020 11:48:38*)

↳ End Entity SSL (*serial number = x, expiry = 1, 2, 3, 4, 5 years from issuance*)

1.8.3 Code Signing / Time Stamping 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*)

↳ SecuriCode SSLGenie (*serial number = 47 33 ba 0b 7e 1f 0c b5 e1 32 3c 41 4d 72 4c 84 expiry = 30 May 2020 11:48:38*)

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

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*)

↳ SecuriCode SSLGenie (*serial number = 47 33 ba 0b 7e 1f 0c b5 e1 32 3c 41 4d 72 4c 84 expiry = 30 May 2020 11:48:38*)

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

1.8.4 Client certificates

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*)

↳ SecuriMail SSLGenie (*serial number = 7f b8 ef f3 86 cd 72 6c dd c7 93 4e ea a4 e9 09, expiry = 30 May 2020 11:48:38*)

↳ End Entity certificate (*serial number = x, expiry = 1, 2, 3, 4, 5 years from issuance*)

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*)

↳ SecuriMail SSLGenie (*serial number = 7f b8 ef f3 86 cd 72 6c dd c7 93 4e ea a4 e9 09, expiry = 30 May 2020 11:48:38*)

↳ End Entity certificate (*serial number = x, expiry = 1, 2, 3, 4, 5 years from issuance*)

1.9 SSLGenie Certification Authority

In its role as a Certification Authority (CA) SSLGenie provides certificate services within the SSLGenie PKI. The SSLGenie CA will:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the SSLGenie repository (www.SSLGenie.com/repository).

- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CPS.
- Upon receipt of a valid request to revoke the certificate from a person authorised to request revocation using the revocation methods detailed in this CPS, revoke a certificate issued for use within the SSLGenie PKI.
- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CPS.
- Distribute issued certificates in accordance with the methods detailed in this CPS.
- Update CRLs in a timely manner as detailed in this CPS.
- Notify subscribers via email of the imminent expiry of their SSLGenie issued certificate (for a period disclosed in this CPS).

1.10 SSLGenie Registration Authorities

SSLGenie has established the necessary secure infrastructure to fully manage the lifecycle of digital certificates within its PKI. Through a network of Registration Authorities (RA), SSLGenie also makes its certification authority services available to its subscribers. SSLGenie RAs:

- Accept, evaluate, approve or reject the registration of certificate applications.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of application as specified in the SSLGenie validation guidelines documentation.
- Use official, notarized or otherwise indicated document to evaluate a subscriber application.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of reissue or renewal as specified in the SSLGenie validation guidelines documentation.

A SSLGenie RA acts locally within their own context of geographical or business partnerships on approval and authorisation by SSLGenie in accordance with SSLGenie practices and procedures.

SSLGenie extends the use of Registration Authorities for its Web Enterprise Public Key Infrastructure (EPKI) Manager program. Upon successful approval to join the respective programs the EPKI Manager Subscriber or are permitted to act as an RA on behalf of SSLGenie. RAs are restricted to operating within the set validation guidelines published by SSLGenie to the RA upon joining the programs. Certificates issued through an RA contain an amended Certificate Profile within an issued certificate to represent the involvement of the RA in the issuance process to the Relying Party.

1.10.1 SSLGenie Partners

SSLGenie operates a SSLGenie Partner network that allows authorised partners to integrate SSLGenie digital certificates into their own product portfolios. SSLGenie Partners are responsible for referring digital certificate customers to SSLGenie, who maintain full control over the certificate lifecycle process, including application, issuance, renewal and revocation. Due to the nature of the SSLGenie program, the SSLGenie must authorise a pending customer order made through its SSLGenie account prior to SSLGenie instigating the validation of such certificate orders. All SSLGenie Partners are required to provide proof of organisational status (refer to section 4.3 for examples of documentation required) and must enter into a SSLGenie Partner agreement prior to being provided with SSLGenie Partner facilities.

1.10.2 EPKI Manager Account Holders

SSLGenie EPKI Manager is a fully outsourced enterprise public key infrastructure service that allows authorised EPKI Manager account holders to control the entire certificate lifecycle process, including application, issuance, renewal and revocation, for certificates designated to company servers, intranets, extranets, partners, employees and hardware devices.

Through a “front-end” referred to as the “Management Area”, the EPKI Manager Account Holder has access to the RA functionality including but not limited to the issuance of Secure Server Certificates and Corporate Secure Email Certificates.

The EPKI Manager Account Holder is obliged to issue certificates only to legitimate company resources, including domain names (servers), intranets, extranets, partners, employees and hardware devices.

1.11 Subscribers

Subscribers of SSLGenie services are individuals or companies that use PKI in relation with SSLGenie supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the private key corresponding to the public key listed in the certificate. Prior to verification of identity and issuance of a certificate, a subscriber is an applicant for the services of SSLGenie. Each Subscriber should sign the Subscriber Agreement with SSLGenie, and the Subscriber should sign and seal the agreement and fax to SSLGenie.

1.12 Relying Parties

Relying parties use PKI services in relation with SSLGenie certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a subscriber certificate. Because not all SSLGenie certificate products are intended to be used in an e-commerce transaction or environment, parties who rely on certificates not intended for e-commerce do not qualify as a relying party. Please refer to Section 2.4 to determine whether a particular product is intended for use in e-commerce transactions.

To verify the validity of a digital certificate they receive, relying parties must refer to the Certificate Revocation List (CRL) prior to relying on information featured in a certificate to ensure that SSLGenie has not revoked the certificate. The CRL location is detailed within the certificate.

2 Technology

This section addresses certain technological aspects of the SSLGenie infrastructure and PKI services.

2.1 SSLGenie CA Infrastructure

The SSLGenie 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.

2.1.1 Root CA Signing Key Protection & Recovery

Protection of the CA Root signing key pairs is ensured with the use of IBM 4578 cryptographic coprocessor devices, which are certified to FIPS 140-1 Level 4, for key generation, storage and use. The CA Root signing key pairs are 2048 bit and were generated within the IBM 4578 device.

CA Number	Description	Usage	Lifetime	Size
1	Premium SSLGenie Server CA	Intermediate certificate for SSL certificates, Class 3	To 10-July-2019	2048
2	Flash SSLGenie Server CA	Intermediate certificate for SSL certificates, Class 2	To 10-July-2019	2048
3	Premium SGC SSLGenie Server CA	Intermediate certificate for SGC-enable SSL certificates, Class 3	To 25-June-2019	2048
4	SecuriCode SSLGenie Code Signing CA	Intermediate certificate for code signing, Class 3	To 10-July-2019	2048
5	SecuriMail SSLGenie Client CA	Intermediate certificate for Client authentication and Email, Class 3	To 10-July-2019	2048

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 authorised SSLGenie officers are required to physically retrieve the removable media from the distributed physically secure locations.

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

Comodo CA ensures the protection of its CA Root signing key pair in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo CA's WebTrust compliancy are available at its official website (www.comodogroup.com).

2.1.2 CA Root Signing Key Generation Process

SSLGenie 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 unauthorised usage of it.

The SSLGenie 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.

2.1.3 CA Root Signing 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, as detailed in section 2.1.1 of this CPS.

2.1.4 Procedures employed for CA Root Signing Key Changeover

The lifetime of our CA keys is set out in the table in 2.1.1. Towards the end of each private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates and CRLs 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 2.1.5 of this CPS.

2.1.5 CA Root Public Key Delivery to Subscribers

SSLGenie makes all its CA Root Certificates available in online repositories at www.SSLGenie.com/repository. The UTN-USERFirst Hardware certificate is present in Internet Explorer 5.01 and above, Netscape 8.1 and above and 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 to relying parties 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

SSLGenie provides the full certificate chain (see section 1.8 of this CPS) to the Subscriber upon issuance and delivery of the Subscriber certificate.

2.1.6 Physical CA Operations

2.1.6.1 SSLGenie

Access to the secure part of SSLGenie facilities is limited using physical access control and is only accessible to appropriately authorised 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 SSLGenie CA physical machinery within the secure facility is protected with locked cabinets and logical access control.

SSLGenie has made reasonable efforts to ensure its secure facilities are protected from:

- Fire and smoke damage (fire protection is made in compliance with local fire regulations).
- Flood and water damage.

SSLGenie 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.

SSLGenie asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

2.2 Digital Certificate Management

SSLGenie certificate management refers to functions that include but are not limited to the following:

- Verification of the identity of an applicant of a certificate.
- Authorising the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.
- Storing certificates.
- Retrieving certificates in accordance with their particular intended use.
- Verification of the domain of an applicant of a certificate.

SSLGenie conducts the overall certification management within the SSLGenie PKI; either directly or through a SSLGenie approved RA. SSLGenie is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

2.3 SSLGenie Directories, Repository and Certificate Revocation Lists

SSLGenie manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by SSLGenie are X.509v2 CRLs, in particular 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. SSLGenie 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 the following URLs:

<http://crl.sslgenie.com/FlashSSLGenie.crl>
<http://crl.sslgenie.com/PremiumSSLGenie.crl>□
<http://crl.sslgenie.com/SecuriMailSSLGenie.crl>□
<http://crl.sslgenie.com/SecuriCodeSSLGenie.crl>
<http://crl.sslgenie.com/PremiumSSLGenieSGC.crl>

Revoked intermediate and higher level certificates are published in the CRL accessed via:

<http://crl.usertrust.com/UTN-USERFirst-Hardware.crl>
<http://crl.usertrust.com/UTN-DATACorpSGC.crl>
<http://crl.usertrust.com/UTN-USERFirst-Object.crl>
<http://crl.usertrust.com/UTN-USERFirst-ClientAuthenticationandEmail.crl>

SSLGenie also publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices, references within this CPS as well as any other information it considers essential to its services. The SSLGenie legal repository may be accessed at www.sslgenie.com/repository.

2.4 Types of SSLGenie Certificates

SSLGenie 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, including but not limited to secure email, protection of online transactions and identification of persons, whether legal or physical, or devices on a network or within a community.

SSLGenie 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 SSLGenie products creates no claims by any third party. Upon the inclusion of a new certificate product in the SSLGenie hierarchy, an amended version of this CPS will be made public within seven (7) days on the official SSLGenie websites.

Suspended or revoked certificates are appropriately referenced in CRLs and published in SSLGenie directories. SSLGenie does not perform escrow of subscriber private keys. SSLGenie does not perform escrow of subscriber private keys.

As detailed in this CPS, SSLGenie 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 SSLGenie websites. The maximum warranty associated with each certificate is set forth in detail in section 5.31

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.

2.4.1 SSLGenie Secure Server Certificates

SSLGenie makes available Secure Server Certificates that in combination with a Secure Socket Layer (SSL) web server attest the public server's identity, providing full authentication and enabling secure communication with customers and business partners. SSLGenie Secure Server Certificates are offered in six variants; Flash SSLGenie, Flash SSLGenie Wildcard, Premium SSLGenie, Premium SSLGenie Wildcard, Premium SGC SSLGenie, Premium SGC SSLGenie Wildcard. Pricing for the certificates are made available on the relevant official SSLGenie websites.

a) Flash SSLGenie and Wildcard

Flash SSLGenie Certificates are the entry level Secure Server Certificate from SSLGenie that issued to registered domain. Their intended usage is for websites conducting non-e-commerce or transferring data of low value and for within internal networks.

Flash SSLGenie wildcard used to secure multiple sub-domains with a single Flash SSLGenie Certificate, it support *.domain.com that hosted in one same physical server.

Flash SSLGenie-MDC support multi-domain that hosted in one same physical server, the minimum domain is 5 domains, the maximum is 100 domains.

In accordance with section 4.2.1(Validation Practices) of this CPS, Flash SSLGenie Certificates validate domain name only. SSLGenie utilises whois database to validate the applicant's identity that it is this domain name's administrator. An approval email is sent to the domain's admin email for the applicant to approve this order.

Due to the increased validation speed and the nature of how SSLGenie intends Flash SSLGenie certificates to be used, the certificates carry a reduced warranty. The maximum warranty associated with a Flash SSLGenie certificate is \$50.

Subscriber fees for a Flash SSLGenie Certificate are available from the official SSLGenie website.

b) Premium SSLGenie and Wildcard

Premium SSLGenie Certificates are the professional level high assurance Secure Server Certificates from SSLGenie with stringent 4 step authentication. Their intended usage is

for websites conducting high value e-commerce or transferring data in Internet or Intranet.

Premium SSLGenie wildcard used to secure multiple sub-domains with a single Premium SSLGenie Certificate, it support *.domain.com that hosted in one same physical server.

In accordance with section 4.2.1 (Validation Practices) of this CPS, Premium SSLGenie Certificates validate the applicant's true identity by four methods: (1) The applicant should sign a contract with SSLGenie to buy the certificate with company seal; (2) The applicant should provide business license or other government authority document; (3) The applicant should transfer money from its own bank to SSLGenie. SSLGenie's bank can provide the payer's company name to SSLGenie, then SSLGenie compare the name with its proof document; (4) SSLGenie also check if the domain's registrant name is same as the proof document.

If the applicant proof document's organization name is in Chinese, then the applicant's certificate's O field should be in Chinese name, or its English translation name that used normal English word to translate its Chinese name into English, the translation should get the approval by SSLGenie's verifier.

The maximum warranty associated with a Premium SSLGenie certificate is \$100,000.

Subscriber fees for a Premium SSLGenie Certificate are available from the official SSLGenie website.

c) Premium SGC SSLGenie and Wildcard

Premium SGC SSLGenie Certificates are the high assurance premium Secure Server Certificates from SSLGenie that support Server Gated Cryptography technology with stringent 4 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption. Their intended usage is for websites conducting high value e-commerce or transferring data in Internet or Intranet for financial-related industry.

Premium SGC SSLGenie wildcard used to secure multiple sub-domains with a single Premium SGC SSLGenie Certificate, it support *.domain.com that hosted in one same physical server.

In accordance with section 4.2.1 (Validation Practices) of this CPS, Premium SSLGenie Certificates validate the applicant's true identity by four methods: (1) The applicant should sign a contract with SSLGenie to buy the certificate with company seal; (2) The applicant should provide business license or other government authority document; (3) The applicant should transfer money from its own bank to SSLGenie. SSLGenie's bank can provide the payer's company name to SSLGenie, then SSLGenie compare the name with its proof document; (4)SSLGenie also check if the domain's registrant name is same as the proof document.

If the applicant proof document's organization name is in Chinese, then the applicant's certificate's O field should be in Chinese name, or its English translation name that used normal English word to translate its Chinese name into English, the translation should get the approval by SSLGenie's verifier.

The maximum warranty associated with a Premium SGC SSLGenie certificate is \$250,000.

Subscriber fees for a Premium SSLGenie Certificate are available from the official SSLGenie website.

2.4.2 SSLGenie Code Signing Certificates

SSLGenie 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.

In accordance with section 4.2.3 (Validation Practices) of this CPS, SSLGenie employs a four-step validation process to confirm the identity of a Code Signing Certificate applicant.

The maximum warranty associated with a Code Signing certificate is \$100,000.

Subscriber fees for a Code Signing certificate are available from the official SSLGenie website.

2.4.3 SSLGenie Secure Email Certificates

SSLGenie makes available Secure Email Certificates that 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. Pricing for the certificates is made available on the relevant official SSLGenie websites. From time to time SSLGenie reserves the right to make available promotional offers that may affect the standard price card.

a) Free Secure Email Certificate

Free Secure Email Certificates are issued to natural persons only via the Tier2 Reseller interface and to ordering URL's. The certificates may be used by an individual as a means of representation for a company named within the certificate.

b) Secure Email Certificate

Secure Email Certificates are issued to natural persons only and may be used by an individual as a means of representation for a company named within the certificate.

Secure Email Certificates are available to holders of a SSLGenie EPKI Manager account. The EPKI Manager account may be used to apply for SSLGenie certificates (SSL and Secure Email) and will contain the corporate details (name, address, country) of the account holding company.

EPKI Manager authorised administrators may log into the EPKI Manager online account and apply for Corporate Secure Email Certificates for employees or authorised representatives of the company only.

In accordance with section 4.2.4 (Validation Practices) of this CPS, SSLGenie validates the right of name that displays in the Secure Email Certificate. For personal applicant, it should provide Identity Card, and for corporate applicant, it should provide legal proof document and SSLGenie will validate its true identity prior to the issuance of the Secure Email Certificate.

There is no warranty associated with a Secure Email Certificate.

Subscriber fees for a Corporate Secure Email Certificate are available from the official SSLGenie website.

2.5 Extensions and Naming

2.5.1 Digital Certificate Extensions

SSLGenie uses the standard X.509, version 3 to construct digital certificates for use within the SSLGenie PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. SSLGenie 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.

2.5.2 Incorporation by Reference for Extensions and Enhanced Naming

Enhanced naming is the usage of an extended organisation field in an X.509v3 certificate. Information contained in the organisational unit field is also included in the Certificate Policy extension that SSLGenie may use.

2.6 Subscriber Private Key Generation Process

The Subscriber is solely responsible for the generation of the private key used in the certificate request. SSLGenie 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 web server software. Secure Email Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in popular browsers. Code Signing Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in Microsoft Internet Explorer.

2.7 Subscriber Private Key Protection and Backup

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

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

2.8 Subscriber Public Key Delivery to SSLGenie

Secure Server Certificate requests are generated using the Subscriber's web server software and the request is submitted to SSLGenie in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the SSLGenie website or through a SSLGenie 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 SSLGenie in the form of a PKCS#10 Certificate Signing Request (CSR). The Subscriber's browser generally makes submission automatically. Code Signing requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted automatically to SSLGenie 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.

2.9 Delivery of Issued Subscriber Certificate to Subscriber

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

2.9.1 Secure Server Certificate: Flash SSLGenie and wildcard

If the whois database holds sufficient validation information, an automatic validation of the Flash SSLGenie certificate application may take place. In the event of such an automated validation the Flash SSLGenie certificate is delivered to the contact email address provided during the certificate ordering process. Confirmation of the certificate delivery location is provided to the administrator contact provided during the validation process.

2.9.2 Secure Server Certificate: Premium SSLGenie, Premium SGC SSLGenie

Premium SSLGenie, Premium SSLGenie Wildcard, Premium SGC SSLGenie, Premium SGC SSLGenie wildcard certificates are delivered via email to the Subscriber using the contact email address provided during the application process.

2.9.3 Code Signing Certificates

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

2.9.3 Secure Email Certificate

Upon issuance of the 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.

2.10 Delivery of Issued Subscriber Certificate to Web Host SSLGenie Partner

Issued Subscriber Secure Server Certificates applied for through a Web Host SSLGenie Partner on behalf of the Subscriber are emailed to the administrator contact of the Web Host SSLGenie Partner account. For Web Host SSLGenie Partners using the "auto-apply" interface, Web Host SSLGenies have the added option of collecting an issued certificate from a Web Host SSLGenie account specific URL.

2.11 Delivery of Issued Subscriber Certificate to EPKI Manager Account Holder

Issued Subscriber Secure Server Certificates applied for through an EPKI Manager Account are emailed to the administrator contact of the account.

Issued Secure Email Certificates are delivered as per section 2.9.3 of this CPS.

2.12 SSLGenie Certificates Profile

A Certificate profile contains fields as specified below:

2.12.1 Key Usage extension field

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

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) CRL signing, for verifying a CA's signature on CRLs
- h) Encipher only, public key agreement key for use only in enciphering data when used with key agreement
- i) Decipher only, public key agreement key for use only in deciphering data when used with key agreement

2.12.2 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.

2.12.3 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 SSLGenie.

2.12.4 Certificate Policy (CP)

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 SSLGenie certificate profiles are as per the tables below:

SSLGenie Secure Server Certificate – Flash SSLGenie / Flash SSLGenie Wildcard	
Signature Algorithm	Sha1
Issuer	CN Flash SSLGenie Server Authority
	O MindGenies.com.
	C India
Validity	1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10 year(s)
Subject	CN Common Name
	OU Flash SSLGenie / FlashSSLGenie Wildcard
	OU Domain Control Validated
Authority Key Identifier	KeyID= d0 4a b5 27 93 1b 46 eb ab 38 46 7c 90 55 e1 16 61 1f 6f d5
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)
Netscape Certificate Type	SSL Server Authentication(40)
Basic Constraint	Subject Type=End Entity
	Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.15 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.SSLGenie.com/repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.SSLGenie.com/SSLGenieServer.crl

	[2]CRL Distribution Point Distribution Point Name: Full Name:
Subject Alternate Name	<i>DNS Name</i>
NetscapeSSLServerName	
Thumbprint Algorithm	SHA1
Thumbprint	

SSLGenie Secure Server Certificate – Premium SSLGenie	
Signature Algorithm	Sha1
Issuer	CN Premium SSLGenie Server Authority
	O MindGenies.com
	C India
Validity	1 Year / 2 Year / 3 Year / 4 Year / 5 Year
Subject	CN <i>Common Name</i>
	O <i>Organisation</i>
	OU <i>Organisation Unit</i>
	L <i>Locality</i>
	S <i>Street</i>
	C <i>Country</i>
Authority Key Identifier	KeyID= d9 ad ac 9c 5e ab 97 fb b4 c6 bb 11 34 a9 fb fe f2 af 7d e8
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)
Netscape Certificate Type	SSL Server Authentication(40)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.15 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.SSLGenie.com/repository
CRL Distribution Points	[[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.SSLGenie.com/SSLGeniePremiumServer.crl [2]CRL Distribution Point Distribution Point Name: Full Name:
Subject Alternate Name	<i>DNS Name</i>
NetscapeSSLServerName	
Thumbprint Algorithm	SHA1
Thumbprint	

SSLGenie Secure Server Certificate – Premium SGC SSLGenie	
Signature Algorithm	Sha1
Issuer	CN Premium SGC SSLGenie Server Authority
	O MindGenies.com
	C India
Validity	1 Year / 2 Year / 3 Year
Subject	CN <i>Common Name</i>
	O <i>Organisation</i>
	OU <i>Organisation Unit</i>

	L	<i>Locality</i>
	S	<i>Street</i>
	C	<i>Country</i>
Authority Key Identifier	KeyID= ca 34 b5 12 b9 ba 8c 45 b1 f9 ac fd e7 b4 a4 86 b2 ec ca 21	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
Enhanced Key Usage	Server Authentication(1.3.6.1.5.5.7.3.1) Unknown Key Usage(1.3.6.1.4.1.311.10.3.3) Unknown Key Usage(2.16.840.1.113730.4.1)	
Netscape Certificate Type	SSL Server Authentication(40)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.15 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.SSLGenie.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.SSLGenie.com/SSLGenieSGCServer.crl [2]CRL Distribution Point Distribution Point Name: Full Name:	
Subject Alternate Name	<i>DNS Name</i>	
NetscapeSSLServerName		
Thumbprint Algorithm	SHA1	
Thumbprint		

SSLGenie Code Signing Certificate		
Signature Algorithm	Sha1	
Issuer	CN	SSLGenie Code Signing Authority
	O	MindGenies.com.
	C	India
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	<i>Organisation</i>
	O	<i>Organisation</i>
	OU	<i>Organisation Unit</i>
	L	<i>Locality</i>
	S	<i>Street</i>
	C	<i>Country</i>
Authority Key Identifier	KeyID= a4 13 6a 3f 10 0b d7 21 87 d4 8b 05 ca bc b1 02 cd 54 e2 8a	
Key Usage (NonCritical)	Code Signing (1.3.6.1.5.5.7.3.3) Unknown Key Usage (1.3.6.1.4.1.311.2.1.22)	
Netscape Certificate Type	Code Signing	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.15 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.SSLGenie.com/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: [2]CRL Distribution Point	

	Distribution Point Name: Full Name: URL=http://crl.SSLGenie.com/SSLGenieCodesigning.crl
Subject Alternate Name	DNS Name
Thumbprint Algorithm	SHA1
Thumbprint	

SSLGenie Secure Email Certificate	
Signature Algorithm	Sha1
Issuer	CN SSLGenie Client Authority
	O MindGenies.com.
	C India
Validity	1 Year / 2 Year / 3 Year / 4 Year / 5 Year
Subject	E <i>Email address</i>
	CN <i>Common Name (name of subscriber)</i>
Authority Key Identifier	KeyID= e4 d0 9b d3 9a e7 4f ee 25 a4 d8 22 bd 36 e5 a6 b0 42 f4 2a
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) Smart Card Logon(1.3.6.1.4.1.311.20.2.2) Unknown Key Usage(1.3.6.1.4.1.6449.1.3.5.2) ²
Netscape Certificate Type	SSL Client Authentication , SMIME(A0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.15 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.SSLGenie.com/repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.SSLGenie.com/SSLGenieClient.crl
Subject Alternate Name	DNS Name
Thumbprint Algorithm	SHA1
Thumbprint	

2.13 SSLGenie Certificate Revocation List Profile

The profile of the SSLGenie Certificate Revocation List is as per the table below:

Version	[Version 1]	
Issuer Name	countryName=[Root Certificate Country Name], organisationName=[Root Certificate Organisation], commonName=[Root Certificate Common Name] [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 2 hours]	
Revoked Certificates	<i>CRL Entries</i>	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

² Used for the SSLGenie Certified Delivery Service receive facility. Certified Delivery Service is not covered in this CPS.

3 Organisation

SSLGenie operates within India, with separate operations, research & development and server operation sites. All sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorised 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.

3.1 Conformance to this CPS

SSLGenie conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

3.2 Termination of CA Operations

In case of termination of CA operations for any reason whatsoever, SSLGenie will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, SSLGenie 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 SSLGenie's.

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

3.3 Form of Records

SSLGenie retains records in electronic or in paper-based format for a period detailed in section 3.4 of this CPS. SSLGenie may require subscribers to submit appropriate documentation in support of a certificate application.

SSLGenie Registration Authorities are required to submit appropriate documentation as detailed in the SSLGenie Partner agreements, EPKI Manager Account Holder agreement, and prior to being validated and successfully accepted as an approved SSLGenie Registration Authority.

In its role as a SSLGenie Registration Authority, RAs may require documentation from subscribers to support certificate applications. In such circumstances, RAs are obliged to retain such records in line with the practices of record retention and protection as used by SSLGenie and as stated in this CPS.

3.4 Records Retention Period

SSLGenie retains the records of SSLGenie digital certificates and the associated documentation for a term of no less than 7 years. The retention term begins on the date of expiration or revocation. Copies of certificates are held, 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 SSLGenie may see fit.

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

3.5 Logs for Core Functions

For audit purposes, SSLGenie maintain electronic or manual logs of the following events for core functions. 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 SSLGenie staff on a visit to the data centre, and when not in the data centre are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

An audit log is maintained of each movement of the removable media. Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management. Both current and archived logs are maintained in a form that prevents unauthorised 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.

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

3.5.1 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 revocation reason
- 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

3.5.2 Security Related Events

- System downtime, software crashes and hardware failures
- CA system actions performed by SSLGenie 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 SSLGenie PKI access attempts
- Secure CA facility visitor entry and exit

3.5.3 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

3.5.4 Log Retention Period

SSLGenie maintains logs for a period of 3 years, or as necessary to comply with applicable laws.

3.6 Business Continuity Plans and Disaster Recovery

To maintain the integrity of its services SSLGenie 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.

- SSLGenie operates a fully redundant CA system. The backup CA is readily available in the event that the primary CA should cease operation. All of our critical computer equipment is housed in a co-location facility run by a commercial data-centre, 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 us to specify a maximum system outage time (in case of critical systems failure) of 1 hour.
- Backup of critical CA software is performed weekly and is stored offsite.
- Backup of critical business information is performed daily and is stored offsite.
- SSLGenie operations are distributed across several sites world wide. All sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates.

As well as a fully redundant CA system, SSLGenie 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 SSLGenie will endeavour to minimise interruptions to its CA operations.

3.7 Availability of Revocation Data

SSLGenie publishes Certificate Revocation Lists (CRLs) to allow relying parties to verify a digital signature made using a SSLGenie issued digital certificate. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. SSLGenie issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, SSLGenie may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this CPS) for a period of 7 years or longer if applicable. SSLGenie does not support OCSP (Online Certificate Status Protocol).

3.8 Publication of Critical Information

SSLGenie publishes this CPS, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements in the official SSLGenie repository at www.SSLGenie.com/repository. The SSLGenie Certificate Policy Authority maintains the SSLGenie repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 3.5 of this CPS.

3.9 Confidential Information

SSLGenie observes applicable rules on the protection of personal data deemed by law or the SSLGenie privacy policy (see section 3.11 of this CPS) to be confidential.

3.9.1 Types of Information deemed as Confidential

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

- 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 SSLGenie.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of SSLGenie infrastructure, certificate management and enrolment services and data.

3.9.2 Types of Information not deemed as Confidential

Subscribers acknowledge that revocation data of all certificates issued by the SSLGenie CA is public information is published every 24 hours. 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 section 2.12.4 of this CPS.

3.9.3 Access to Confidential Information

All personnel in trusted positions handle all information in strict confidence. Personnel of RA/LRAs especially must comply with the requirements of the English law on the protection of personal data.

3.9.4 Release of Confidential Information

SSLGenie is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorised party specifying:

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

3.10 Personnel Management and Practices

Consistent with this CPS SSLGenie 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.

3.10.1 Trusted roles

Trusted roles relate to access to the SSLGenie account management system, with functional permissions applied on an individual basis. Senior members of the management team decide permissions, with signed authorisations being archived.

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

3.10.2 Personnel controls

All trusted personnel have background checks before access is granted to SSLGenie’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. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

3.11 Privacy Policy

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

3.12 Publication of information

The SSLGenie certificate services and the SSLGenie repository are accessible through several means of communication:

- On the web: www.sslgenie.com
- By email from legal@sslgenie.com
By mail from:

MG Infocom Pvt Ltd
C-22/28,Sector-57
Noida,Up
India-201301

4 Practices and Procedures

This section describes the certificate application process, including the information required to make and support a successful application.

4.1 Certificate Application Requirements

All Certificate applicants must complete the enrolment process, which includes:

- Generate a RSA key pair and demonstrate to SSLGenie ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to SSLGenie 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
- Provide proof of identity through the submission of official documentation as requested by SSLGenie during the enrolment process

Certificate applications are submitted to either SSLGenie or a SSLGenie approved RA. The following table details the entity(s) involved in the processing of certificate applications. SSLGenie issues all certificates regardless of the processing entity.

Certificate Type	Enrolment Entity	Processing Entity	Issuing Authority
Secure Server Certificate – <i>all types as per section 2.4.1 of this CPS</i>	End Entity Subscriber SSLGenie Partner	SSLGenie	SSLGenie
Code Signing Certificate – <i>all types as per section 2.4.1 of this CPS</i>	End Entity Subscriber SSLGenie Partner	SSLGenie	SSLGenie
Secure Email Certificate – <i>Corporate version as per 2.4.2 of this CPS</i>	End Entity Subscriber SSLGenie Partner	SSLGenie	SSLGenie

4.1.1 SSLGenie Partner Certificate Applications

SSLGenie Partners may act as RAs under the practices and policies stated within this CPS. The RA may make the application on behalf of the applicant pursuant to the SSLGenie program.

Under such circumstances, the RA is responsible for all the functions on behalf of the applicant detailed in section 4.1 of this CPS. Such responsibilities are detailed and maintained within the Web Host SSLGenie agreement and guidelines.

4.1.2 EPKI Manager Account Holder Certificate Applications

EPKI Manager Account Holders act as RAs under the practices and policies stated within this CPS. The RA makes the application for a secure server certificate to be used by a named server, or a secure email certificate to be used by a named employee, partner or extranet user under a domain name that SSLGenie has validated either belongs to, or may legally be used by the EPKI Manager Account holding organisation.

4.1.3 Methods of application

Generally, applicants will complete the online forms made available by SSLGenie or by approved RAs at the respective official websites. Under special circumstances, the applicant may submit an application via email; however, this process is available at the discretion of SSLGenie or its RAs.

EPKI Manager Account Holder applications are made through the EPKI Manager Management Console – a web based console hosted and supported by SSLGenie.

4.2 Application Validation

Prior to issuing a certificate SSLGenie employs controls to validate the identity of the subscriber information featured in the certificate application. The product type indicates such controls:

4.2.1 Secure Server Certificate – Premium SSLGenie and Premium SGC SSLGenie Application Four Step Validation Process

SSLGenie utilises a four-step validation process prior to the issuance of a secure server certificate – Premium SSLGenie and Premium SGC SSLGenie.

This process involves SSLGenie, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 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 available publicly through Internet or approved global domain name registrars.
 - Validation may be supplemented through the use of the administrator contact associated with the domain name register record for communication with SSLGenie 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 (individual or organisation).
 - If the applicant is an organization, this step demands an official government documentation providing you the right to do business
 - We can request for official company documentation such as certificate of Formation, Business License, Articles of Incorporation, Sales License or other relevant documents.
 - If the applicant is an individual he can submit a proof of identity such a s driving licence, passport
3. The applicant has a physical existence
 - We would require a telephone bill as an address proof. We would also make a call on the telephone number specified and verify
 - We can request for additional document such as electricity bill

Optional Step – The applicant’s management responsibility for the organization

- We can request for an authorization letter from the domain owner, appointment letter with the organization
- This step will be executed only if the case is suspicious and we feel that we need addition verification before we can issue a certificate.

Note:

The applicant in India should wire transfer the certificate fee to SSLGenie’s bank account from its own bank account.

- Validated by checking the bank transfer records available from SSLGenie’s bank to check if the payer’s name is same as its proof document.

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

4.2.2 Secure Server Certificate – Flash SSLGenie Application One Step Validation Process

SSLGenie utilises a one step validation process prior to the issuance of a secure server certificate – Flash SSLGenie.

This process involves SSLGenie, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 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 available publicly through Internet or approved global domain name registrars.
 - Validation may be supplemented through the use of the administrator contact associated with the domain name register record for communication with SSLGenie 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@...

4.2.3 Code Signing Certificate Application Four Step Validation Process

SSLGenie utilises a four-step validation process prior to the issuance of a code signing certificate.

This process involves SSLGenie, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) in order to check that:

1. The applicant is an accountable legal entity (individual or organisation).
 - If the applicant is an organization, this step demands an official government documentation providing you the right to do business
 - We can request for official company documentation such as certificate of Formation, Business License, Articles of Incorporation, Sales License or other relevant documents.
 - If the applicant is an individual he can submit a proof of identity such a s driving licence, passport

2. The applicant has a physical existence
 - We would require a telephone bill as an address proof. We would also make a call on the telephone number specified and verify
 - We can request for additional document such as electricity bill
3. Optional Step – The applicant's management responsibility for the organization
 - We can request for an authorization letter from the domain owner, appointment letter with the organization
 - This step will be executed only if the case is suspicious and we feel that we need addition verification before we can issue a certificate.

Note:

The applicant in India should wire transfer the certificate fee to SSLGenie's bank account from its own bank account.

- Validated by checking the bank transfer records available from SSLGenie's bank to check if the payer's name is same as its proof document.

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

4.2.4 Secure Email Certificate

Secure Email Certificates are available through the EPKI Manager and will only be issued to email addresses within approved domain names. The EPKI Manager Account Holder must first submit a domain name to SSLGenie and appropriate domain name ownership, or right to use a domain name, validation takes place in accordance with 4.2.1 of this CPS. Upon successful validation of a submitted domain name SSLGenie allows the EPKI Manager Account Holder to utilise email addresses within the domain name.

The EPKI Manager nominated administrator applies for corporate versions of the Secure Email Certificate. The administrator will submit the secure email certificate end-entity information on behalf of the end-entity. An email is then delivered to the end-entity containing unique login details to online certificate generation and collection facilities hosted by SSLGenie.

Once logged into the online certificate generation and collection facilities, the end-entity's browser creates a public and private key pair. The public key is submitted to SSLGenie who will issue a Corporate version Secure Email Certificate containing the public key. SSLGenie then validate using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during this automated application process. If the automated challenge is successful, SSLGenie will release the digital certificate to the end-entity subscriber.

4.3 Validation Information for Certificate Applications

Applications for SSLGenie certificates are supported by appropriate documentation to establish the identity of an applicant.

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

4.3.1 Application Information for Organisational Applicants

The following elements are critical information elements for a SSLGenie certificate issued to an Organisation. 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 Organisation (PUBLIC)
- Organisational 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 organisational 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 organisational status of the Organisation
- Subscriber agreement, signed (if applying out of bands)

4.3.2 Supporting Documentation for Organisational Applicants

Documentation requirements for Organisational 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 authorised representative of a government organisation
- Official letter from office of Dean or Principal (for Educational Institutions)

SSLGenie may accept at its discretion other official organisational documentation supporting an application.

4.3.3 Application Information for Individual Applicants

The following elements are critical information elements for a SSLGenie certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)
- Organisational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organisational 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 organisational status of the Organisation
- Subscriber agreement, signed (if applying out of bands)

4.3.4 Supporting Documentation for Individual Applicants

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

- Passport
- Driving License
- Bank statement

SSLGenie may accept at its discretion other official documentation supporting an application.

4.4 Validation Requirements for Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information, SSLGenie 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 authorised to do so.

In all types of SSLGenie certificates, the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify SSLGenie 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 and the Subscriber shall pay any Charges payable but that have not yet been paid under the Agreement.

4.4.1 Third-Party Confirmation of Business Entity Information

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

SSLGenie'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.

SSLGenie may use any means of communication at its disposal to ascertain the identity of an organisational or individual applicant. SSLGenie reserves right of refusal in its absolute discretion.

4.4.2 Serial Number Assignment

SSLGenie assigns certificate serial numbers that appear in SSLGenie certificates. Assigned serial numbers are unique.

4.5 Time to Confirm Submitted Data

SSLGenie makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

SSLGenie assures that all certificates will be issued within 2 working days after the receipt of all required validation information as per this CPS.

4.6 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application SSLGenie approves an application for a digital certificate.

If the validation of a certificate application fails, SSLGenie rejects the certificate application. SSLGenie 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 SSLGenie 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.

4.7 Certificate Issuance and Subscriber Consent

SSLGenie 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 4.9 of this CPS). Issuing a digital certificate means that SSLGenie accepts a certificate application.

4.8 Certificate Validity

Certificates are valid upon issuance by SSLGenie and acceptance by the subscriber. Generally, the certificate validity period will be 1, 2 or 3 years, however SSLGenie reserves the right to offer validity periods outside of this standard validity period.

4.9 Certificate Acceptance by Subscribers

An issued certificate is either delivered via email or installed on a subscriber's computer / hardware security module through an online collection method. A subscriber is deemed to have accepted a certificate when:

- The subscriber uses the certificate.
- 30 days pass from the date of the issuance of a certificate.

4.10 Verification of Digital Signatures

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.
- The signed data associated with this digital signature has not been altered since the digital signature was created.

4.11 Reliance on Digital Signatures

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 Certificate Revocation Lists 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.
- the digital certificate applied for is appropriate for the application it is used in,

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 SSLGenie 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.

4.12 Certificate Suspension

SSLGenie does not utilise certificate suspension.

4.13 Certificate Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. SSLGenie will revoke a digital certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key associated with the certificate.
- The Subscriber or SSLGenie has breached a material obligation under this CPS or the relevant Subscriber Agreement.
- Either the Subscriber's or SSLGenie's obligations under this CPS 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 SSLGenie 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 was issued as a result of fraud or negligence; or
 - The certificate, if not revoked, will compromise the trust status of SSLGenie.

4.13.1 Request for Revocation

The subscriber or other appropriately authorised parties such as RAs can request revocation of a certificate. Prior to the revocation of a certificate SSLGenie will verify that the revocation request has been:

- Made by the organisation or individual entity that has made the certificate application.
- Made by the RA on behalf of the organisation or individual entity that used the RA to make the certificate application

SSLGenie employs the following procedure for authenticating a revocation request:

- The revocation request must be sent by the Administrator contact associated with the certificate application. SSLGenie may if necessary also request that the revocation request be made by either / or the organisational contact and billing contact.
- Upon receipt of the revocation request SSLGenie will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- SSLGenie 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.

4.13.2 Effect of Revocation

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 Certificate Revocation List (CRL) and remains on the CRL until some time after the end of the certificate's validity period. An updated CRL is published on the SSLGenie website every 24 hours; however, under special circumstances the CRL may be published more frequently.

4.14 Renewal

Depending on the option selected during application, the validity period of SSLGenie certificates is one year (365 days), two years (730 days) or three years (1095 days) from the date of issuance and is detailed in the relevant field within the certificate.

Renewal fees are detailed on the official SSLGenie websites and within communications sent to subscribers approaching the certificate expiration date.

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

4.15 Notice Prior to Expiration

SSLGenie 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 90-day period prior to the expiry of the certificate.

5 Conditions of Issuance

5.1 SSLGenie Representations

SSLGenie makes to all subscribers and relying parties certain representations regarding its public service, as described below. SSLGenie reserves its right to modify such representations as it sees fit or required by law.

5.2 Information Incorporated by Reference into a SSLGenie Digital Certificate

SSLGenie 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 SSLGenie certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customised 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.

5.3 Displaying Liability Limitations, and Warranty Disclaimers

SSLGenie 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 disclaimers of warranty that may apply. Subscribers must agree to SSLGenie Terms & Conditions before signing-up for a certificate. To communicate information SSLGenie may use:

- An organisational unit attribute.
- A SSLGenie standard resource qualifier to a certificate policy.
- Proprietary or other vendors' registered extensions.

5.4 Publication of Certificate Revocation Data

SSLGenie reserves its right to publish a CRL (Certificate Revocation List) as may be indicated.

5.5 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of SSLGenie certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify SSLGenie of any such changes.

5.6 Publication of Information

Published critical information may be updated from time to time as prescribed in this CPS. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

5.7 Interference with SSLGenie Implementation

Subscribers, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of SSLGenie PKI services including the key generation process, the public web site and the SSLGenie repositories except as explicitly permitted by this CPS or upon prior written approval of SSLGenie. 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 SSLGenie repository and any Digital Certificate or Service provided by SSLGenie.

5.8 Standards

SSLGenie 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. SSLGenie cannot warrant that such user software will support and enforce controls required by SSLGenie, whilst the user should seek appropriate advice.

5.9 SSLGenie Partnerships Limitations

Partners of the SSLGenie network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the SSLGenie products and services. SSLGenie 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 SSLGenie repository and any Digital Certificate or Service provided by SSLGenie.

5.10 SSLGenie Limitation of Liability for a SSLGenie Partner

As the SSLGenie network includes RAs that operate under SSLGenie practices and procedures SSLGenie warrants the integrity of any certificate issued under its own root within the limits of the SSLGenie insurance policy and in accordance with this CPS.

5.11 Choice of Cryptographic Methods

Parties are solely responsible for having exercised independent judgement 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.

5.12 Reliance on Unverified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by SSLGenie. 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 SSLGenie, assume in whole.

By means of this CPS, SSLGenie 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.sslgenie.com/repository or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

5.13 Rejected Certificate Applications

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.

5.14 Refusal to Issue a Certificate

SSLGenie 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. SSLGenie reserves the right not to disclose reasons for such a refusal.

5.15 Subscriber Obligations

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

- To minimise 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 SSLGenie or a SSLGenie RA.
- Ensure that the public key submitted to SSLGenie or a SSLGenie RA corresponds with the private key used.
- Ensure that the public key submitted to SSLGenie or a SSLGenie RA is the correct one.
- Provide correct and accurate information in its communications with SSLGenie or a SSLGenie RA.
- Alert SSLGenie or a SSLGenie RA if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to SSLGenie.
- Generate a new, secure key pair to be used in association with a certificate that it requests from SSLGenie or a SSLGenie RA.
- Read, understand and agree with all terms and conditions in this SSLGenie CPS and associated policies published in the SSLGenie Repository at www.sslgenie.com/repository.
- Refrain from tampering with a SSLGenie certificate.
- Use SSLGenie certificates for legal and authorised purposes in accordance with the suggested usages and practices in this CPS.
- Cease using a SSLGenie certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a SSLGenie 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 SSLGenie issued certificate to issue end-entity digital certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorised use of the private key corresponding to the public key published in a SSLGenie certificate.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a SSLGenie certificate.

- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their private keys.

5.16 Representations by Subscriber upon Acceptance

Upon accepting a certificate, the subscriber represents to SSLGenie 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 unauthorised person has ever had access to the subscriber's private key.
- All representations made by the subscriber to SSLGenie 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 SSLGenie of any material inaccuracies in such information.
- The certificate is used exclusively for authorised and legal purposes, consistent with this CPS.
- It will use a SSLGenie certificate only in conjunction with the entity named in the organisation field of a digital certificate (if applicable).
- The subscriber retains control of her private key, use a trustworthy system, and take reasonable precautions to prevent its loss, disclosure, modification, or unauthorised 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 SSLGenie.
- The subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of SSLGenie.
- 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.

5.17 Indemnity by Subscriber

By accepting a certificate, the subscriber agrees to indemnify and hold SSLGenie, 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 SSLGenie, 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, SSLGenie, 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 unauthorised 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.

5.18 Obligations of SSLGenie Registration Authorities

A SSLGenie RA operates under the policies and practices detailed in this CPS and also the associated Web Host SSLGenie agreement, Powered SSL agreement and EPKI Manager Account agreement. The RA is bound under contract to:

- Receive applications for SSLGenie certificates in accordance with this CPS.
- Perform all verification actions prescribed by the SSLGenie validation procedures and this CPS.
- Receive, verify and relay to SSLGenie all requests for revocation of a SSLGenie certificate in accordance with the SSLGenie revocation procedures and the CPS.
- Act according to relevant Law and regulations.

5.19 Obligations of a Relying Party

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

- Minimise 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 SSLGenie digital certificate.
- Read and agree with the terms of the SSLGenie CPS and relying party agreement.
- Verify a SSLGenie certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA.
- Trust a SSLGenie certificate only if it is valid and has not been revoked or has expired.
- Rely on a SSLGenie certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

5.20 Legality of Information

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.

5.21 Subscriber Liability 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.

5.22 Duty to Monitor Agents

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

5.23 Use of Agents

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

5.24 Conditions of usage of the SSLGenie Repository and Web site

Parties (including subscribers and relying parties) accessing the SSLGenie Repository (www.sslgenie.com/repository) and official web site(s) agree with the provisions of this CPS and any other conditions of usage that SSLGenie may make available.

Parties demonstrate acceptance of the conditions of usage of the CPS by using a SSLGenie issued certificate.

Failure to comply with the conditions of usage of the SSLGenie Repositories and web site may result in terminating the relationship between SSLGenie and the party.

5.25 Accuracy of Information

SSLGenie, recognising its trusted position, makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated and correct information. SSLGenie, however, cannot accept any liability beyond the limits set in this CPS and the SSLGenie insurance policy.

Failure to comply with the conditions of usage of the SSLGenie Repositories and web site may result in terminating the relationship between SSLGenie and the party.

5.26 Obligations of SSLGenie

To the extent specified in the relevant sections of the CPS, SSLGenie 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 SSLGenie 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 fulfil its obligations presented herein.
- Upon receipt of a request from an RA operating within the SSLGenie network; act promptly to issue a SSLGenie certificate in accordance with this SSLGenie CPS.

- Upon receipt of a request for revocation from an RA operating within the SSLGenie network; act promptly to revoke a SSLGenie certificate in accordance with this SSLGenie CPS.
- 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 SSLGenie has no further obligations under this CPS.

5.27 Fitness for a Particular Purpose

SSLGenie 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.

5.28 Other Warranties

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93 SSLGenie 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 SSLGenie except as it may be stated in the relevant product description below in this CPS and in the SSLGenie insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in SSLGenie 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 SSLGenie 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 SSLGenie.

5.29 Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this CPS, SSLGenie shall not be responsible for non-verified subscriber information submitted to SSLGenie, or the SSLGenie 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.

5.30 Exclusion of Certain Elements of Damages

In no event (except for fraud or wilful misconduct) shall SSLGenie 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 wilful 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.
- 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.
- eband software a subscriber uses.
- Any liability that arises from compromise of a subscriber's private key.

SSLGenie does not limit or exclude liability for death or personal injury.

5.31 Certificate Insurance Plan

In the event SSLGenies was found to be negligent in the issuance of a digital certificate which resulted in a loss to a Relying Party, the Relying Party may be eligible under SSLGenies's certificate warranty to receive up to US\$1,000 per incident. The eligibility is subject to the cumulative maximum limits explained below for all claims related to that digital certificate. Except to the extent of wilful misconduct, the liability of SSLGenies is limited to the negligent issuance of certificates. The cumulative maximum liability of SSLGenies to all applicants, subscribers and relying parties for each certificate is set forth in the table below.

Under SSLGenies's warranty a covered person may only receive a maximum payment of \$1,000 per online transaction ("Incident Limit") for which the Covered Person claims there was a breach of the SSLGenies 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 a maximum amount of \$1,000 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, 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.

5.31.1 Flash SSLGenie Certificate

The maximums and cumulative liability of SSLGenie to applicants, subscribers and relying parties in respect of each Flash SSLGenie Certificate shall not exceed \$50.00 (fifty US dollars).

5.31.2 Premium SSLGenie Certificate

The maximum cumulative liability of SSLGenie to applicants, subscribers and relying parties in respect of each Premium SSLGenie Certificate shall not exceed \$100,000.00 (one hundred thousand US dollars). The maximum transaction value is \$10,000.

5.31.3 Premium SGC SSLGenie Certificate

The maximum cumulative liability of SSLGenie to applicants, subscribers and relying parties in respect of each Premium SGC SSLGenie Certificate shall not exceed \$250,000.00 (two hundred and fifty thousand US dollars). The maximum transaction value is \$10,000.

5.31.4 Code Signing Certificate

The maximum cumulative liability of SSLGenie to applicants, subscribers and relying parties in respect of each Code Signing Certificate shall not exceed \$50,000.00 (Fifty thousand US dollars).

5.31.5 Secure Email Certificate

There is no liability of SSLGenie to applicants, subscribers and relying parties.

5.32 Financial Limitations on Certificate Usage

SSLGenie certificates may only be used in connection with data transfer and transactions having a US dollar (US\$) value no greater than the level of warranty associated with the certificate and detailed in section 5.31 of this CPS.

5.33 Damage and Loss Limitations

In no event (except for fraud or wilful misconduct) will the aggregate liability of SSLGenie 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 exceeds the applicable liability cap for such certificate as stated in the SSLGenie insurance plan detailed section 5.31 of this CPS.

5.34 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this CPS, dated 23 August 2007, 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.

5.35 SSLGenie Intellectual Property Rights

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

5.36 Infringement and Other Damaging Material

SSLGenie subscribers represent and warrant that when submitting to SSLGenie 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 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.

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

5.37 Ownership

Certificates are the property of SSLGenie. SSLGenie gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. SSLGenie 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 SSLGenie private key remain the property of SSLGenie.

5.38 Governing Law

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

5.39 Jurisdiction

Each party, including SSLGenie partners, subscribers and relying parties, irrevocably agrees that the courts of the Republic of India 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 SSLGenie PKI services.

5.40 Dispute Resolution

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 SSLGenie of the dispute with a view to seek dispute resolution.

5.41 Successors and Assigns

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.

5.42 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.

5.43 Interpretation

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 SSLGenie 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.

5.44 No Waiver

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.

5.45 Notice

SSLGenie 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 SSLGenie, 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 registered mail, postage prepaid, return receipt requested, addressed as follows:

SSLGenie Certificate Services
M.G InfoCom Pvt. Ltd.
C-22/28, Sector-57
Noida, UP
India-201301.

Attention: Legal Practices

Email: legal@sslgenie.com

This CPS, related agreements and Certificate policies referenced within this document are available online at www.sslgenie.com/repository.

5.46 Fees

SSLGenie charges Subscriber fees for some of the certificate services it offers, including issuance, renewal and reissues (in accordance with the SSLGenie Reissue Policy stated in 5.47 of this CPS). Such fees are detailed on the official SSLGenie website (www.sslgenie.com).

SSLGenie does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a SSLGenie issued certificate using Certificate Revocation Lists.

SSLGenie retains its right to affect changes to such fees. SSLGenie partners, including SSLGenies, Web Host SSLGenies, EPKI Manager Account Holders and Powered SSL Partners, will be suitably advised of price amendments as detailed in the relevant partner agreements.

5.47 SSLGenie Reissue Policy

SSLGenie offers a free reissue policy during the certificate lifetime. During the certificate validation period, the Subscriber may request a reissue of their certificate and incur no further fees for the reissue. If details other than just the public key require amendment, SSLGenie reserves the right to revalidate the application in accordance with the validation processes detailed within this CPS. If the reissue request does not pass the validation process, SSLGenie reserves the right to refuse the reissue application. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant.

5.48 SSLGenie Refund Policy

SSLGenie 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.

SSLGenie is not obliged to refund a certificate after the 30-day refund policy period has expired.

6 General Issuance Procedure

6.1 General - SSLGenie

SSLGenie offers different certificate types to make use of SSL, Code Signing and S/MIME technology for secure online transactions, secure electronic file and secure email respectively. Prior to the issuance of a certificate, SSLGenie will validate an application in accordance with this CPS which may involve the request by SSLGenie to the applicant for relevant official documentation supporting the application.

SSLGenie certificates are issued to organisations or individuals.

The validity period of SSLGenie certificates varies dependent on the certificate type, but typically, a certificate will be valid for either 1 year, 2 years or 3 years. SSLGenie reserves the right to, at its discretion, issues certificates that may fall outside of these set periods.

6.2 Certificates issued to Individuals and Organisations

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by SSLGenie. Additional documentation in support of the application may be required so that SSLGenie verifies the identity of the applicant. The applicant submits to SSLGenie such additional documentation. Upon verification of identity, SSLGenie issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify SSLGenie 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.

SSLGenie may at its discretion, accept applications via email.

6.3 Content

Typical content of information published on a SSLGenie certificate may include but is not limited to the following elements of information:

6.3.1 Secure Server Certificates – Premium SSLGenie and Premium SGC SSLGenie

- Applicant's fully qualified domain name.
- Applicant's organisational name.
- Code of applicant's country.
- Organisational unit name, street address, city, state.
- Issuing certification authority (SSLGenie).
- Applicant's public key.
- SSLGenie digital signature.
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.3.2 Secure Server Certificates – Flash SSLGenie

- Applicant's fully qualified domain name.
- Issuing certification authority (SSLGenie).
- Applicant's public key.
- SSLGenie digital signature.
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.3.3 Code Signing Certificates

- Applicant's organisational name.
- Code of applicant's country.
- Organisational unit name, street address, city, state.
- Issuing certification authority (SSLGenie).
- Applicant's public key.
- SSLGenie digital signature.
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.3.4 Secure Email Certificates

- Applicant's e-mail address.
- Applicant's name.
- Code of applicant's country.

- Organisation name, organisational unit name, street address, city, state.
- Applicant's public key.
- Issuing certification authority (SSLGenie).
- SSLGenie digital signature.
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.4 Time to Confirm Submitted Data

SSLGenie 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, SSLGenie aims to confirm submitted application data and to complete the validation process and issue / reject a certificate application within 2 working days.

From time to time, events outside of the control of SSLGenie may delay the issuance process, however SSLGenie 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.

6.5 Issuing Procedure

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

- a) The applicant fills out the online request on SSLGenie's web site and the applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organisational 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 SSLGenie.
- d) The applicant pays the certificate fees.
- e) SSLGenie verifies the submitted information using third party databases and Government records
- f) Upon successful validation of the application information, SSLGenie may issue the certificate to the applicant or should the application be rejected, SSLGenie 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 SSLGenie websites.
- h) Revocation is conducted as per the procedures outlined in this CPS.

Document Control

This document is version 1.0 of the SSLGenie CPS, created on 23 August 2007 and signed off by the SSLGenie Certificate Policy Authority

SSLGenie Certificate Services
M.G InfoCom Pvt. Ltd.
C-22/28, Sector-57
Noida, UP
India-201301.

URL: <http://www.sslgenie.com>
E-mail: legal@sslgenie.com

Copyright Notice

Copyright SSLGenie, 2007. 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 SSLGenie.

Requests for any other permission to reproduce this SSLGenie document (as well as requests for copies from SSLGenie) must be sent email to: legal@sslgenie.com or by mail to

SSLGenie Certificate Services
M.G InfoCom Pvt. Ltd.
C-22/28, Sector-57
Noida, UP
India-201301.