SSL Certificate Practice Statement

SSLCOM Group Ltd.

December, 2018

Table of Contents

1. Introduction 6
1.1. Overview 6
1.2. Document Name and Identification 6
1.3. PKI Participants 6
.1.3.1 Certification Authority 6
1.3.2. Registration Authority 6
1.3.3. Subscribers 7
1.3.4. Relying Parties 7
1.4. Certificate Usage 7
1.4.1. Certificate Usage 7
1.4.2. Prohibited Usage 7
1.5. Policy Administration 7
1.5.1. Organization administrating the document 7
1.5.2. Contact person 8
1.6. Definitions and Acronyms 8
2. Publication and Repository Responsibilities 9
2.1. Legal Document Repositories 9
2.2. Publication of Certification information 9
2.2.1. CRL publishing 9
2.3. Time and Frequency of Publication 10
2.4. Access Controls 10
3. Identification and Authentication (I&A) 10
3.1. Naming 10
3.1.1. Types of Names 10
3.1.2. Meaning of Names 11
3.1.3. Anonymity or pseudonymity of subscribers 11
3.1.4. Rules of Interpretation 11
3.1.5. Uniqueness of names 11
3.1.6. Recognition, authentication, and role of trademarks 11
3.2. Initial Identity Validation 11
3.2.1. Private Key Possession 11
3.2.2. Authentication of Organization and Domain Identity 11
3.2.3. Personal Identification 12
3.2.4. Non Verified Subscriber Information 12
3.2.5. Validation of Authority 12
3.2.6. Criteria for interoperation 12
3.3. Identification and Authentication for Re-key Requests 12
3.4. Identification and Authentication for Revocation Requests 13
4. Certificate Life-Cycle Operational Requirements 13
4.1. Certificate Application 13
4.1.1. Who can submit a Certificate Application 13
4.1.2. Enrollment process and responsibilities 13
4.2. Certificate Application Processing 13
4.2.1. Performing identification and authentication functions 13
4.2.2. These verification procedures shall include 13

4.2.3. Time to process Certification applications 13
4.3. Certificate Issuance 14
4.3.1. CA actions during Certificate acceptance 14
4.3.2. Notification to Subscriber of Certificate issuance 14
4.4. Certificate Acceptance 14
4.4.1. Conduct constituting certificate acceptance 14
4.4.2. Publication of the certificate by the CA 14
4.5. Key Pair and Certificate Usage 14
4.5.1. Subscriber Key Usage Responsibilities 14
4.5.2. Relying Party Key Usage Responsibilities 14
4.6. Certificate Renewal 15
4.7. Certificate Re-key 15
4.8. Certificate Modification 15
4.9. Certificate Revocation and Suspension 15
4.9.1. Circumstances for Revocation 15
4.9.2. Who Can Request Revocation 16
4.9.4. Revocation Request grace Period 16
4.9.5. Time for Processing Revocation Request 17
4.9.6. Revocation checking requirement for relying parties 17
4.9.7. CRL Issuance Frequency 17
4.9.8. Maximum latency for CRLs 17
4.9.9. On-line Revocation Availability 17
4.9.10. On-line Revocation Checking Requirements 17
4.9.11. Other forms of revocation advertisements available 17
4.9.12. Special requirements re key compromise 18
4.9.13. Certificate Suspension 18
4.9.14. Who can request suspension 18
4.9.15. Procedure for suspension request 18
4.9.16. Limits on suspension period 18
4.10. On-line Revocation Checking Requirements 18
4.10.1. Operational characteristics 18
4.10.2. Service availability 18
4.11. End of Subscription 18
4.12. Key Escrow and Recovery 18
5. Facility, Management, and Operational Controls 18
5.1. Physical Security Controls 18
5.1.1. Location and Construction 18
5.1.2. Physical Access 18
5.1.3. Power and Air Conditioning 19
5.1.4. Water Exposures 19
5.1.5. Fire Prevention and Protection 19
5.1.6. Media Storage 19
5.1.7. Waste Disposal 19
5.1.8. Off-Site Backup 19
5.2. Procedural Controls 19
5.2.1. Trusted Roles 19
5.2.2. Number of persons required per task 19
5.2.3. Identification and authentication for each role 20

5.2.4. Separation of Duties 20
5.3. Personnel Controls 20
5.3.1. Qualifications 20
5.3.2. Training Requirements 20
5.4. Audit Logging Procedures 20
.5.4.1 Types of Events Recorded 20
5.4.2. Content of Logs 20
5.4.3. Retention Period for Audit Logs 21
5.4.4. Log Backup 21
5.5. Records Archival 21
5.5.1. Types of Records archived 21
5.5.2. Retention Period for Archive 21
5.5.3. Protection of Archive 21
5.5.4. Archive Backup Procedures 21
5.5.5. Requirements for Time-stamping of Records 21
5.6. Key Changeover 21
5.7. Compromise and Disaster Recovery 22
5.8. CA or RA Termination 22
6. Technical Security Controls 23
6.1. Key Pair Generation and Installation 23
6.1.1. Key Pair Generation 23
6.1.2. Private Key Delivery to Subscriber 23
6.1.3. Public Key Delivery to Certificate Issuer 23
6.1.4. CA Public Key Delivery to Relying Party 23
6.1.5. Key sizes 24
6.1.6. Public Key Parameters Generation and Quality Checking 24
6.1.7. Key usage purposes 24
6.2. Private Key Protection and Cryptographic Module Engineering Controls 24
6.2.1. Cryptographic module standards and controls 24
6.2.2. Private Key Multi-Person control 24
6.2.3. Private Key Escrow 24
6.2.4. Private Key Backup 24
6.2.5. Private Key Archival 24
6.2.6. Method of Activating Private Key 24
6.3. Other Aspects of Key Pair Management 25
6.3.1. Public Key Archival 25
6.3.2. Key Usage Periods 25
6.4. Activation Data 25
6.5. Computer Security Controls 25
6.5.1. Specific computer security technical requirements 25
6.5.2. Computer security rating 25
6.6. Life Cycle Security Controls 25
6.6.1. System Development Controls 25
6.6.2. Security Management Controls 25
.6.7 Network Security Controls 26
6.8. Timestamping 26
7. Certificate, CRL, and OCSP Profiles 26
7.1. Certificate Profile 26

7.1.1. ROOT CA Certificate Profile 26
7.1.2. ONLINE CA Certificate Profile 27
7.1.3. Web Server Subscriber DV Certificate Profile 29
7.2. CRL Profile 31
7.3. OCSP Profile 32
8. Compliance Audit and Other Assessment 32
8.1. Frequency or circumstances of assessment 32
8.2. Identity/qualifications of assessor 32
8.3. Topics covered by assessment 32
8.4. Communication of results 33
9. Other Business and Legal Matters 33
9.1. Fees 33
9.1.1. Certificate Issuance or Renewal Fees 33
9.1.2. Certificate Access Fees 33
9.1.3. Revocation or Status Information Revocation Fee 33
9.2. Financial Responsibility 33
9.3. Confidentiality of Business Information 33
9.4. Privacy of Personal Information 34
9.5. Intellectual Property Rights 34
9.6. Representations and Warranties 34
9.6.1. CA Representations and Warranties 34
9.6.2. RA Representations and Warranties 35
9.6.3. Subscriber Representations and Warranties 35
9.7. Disclaimers of Warranties 35
9.8. Limitations of Liability 36
9.9. Indemnities 36
9.10. Term and Termination 36
9.11. Individual notices and communications with participants 37
9.12. Amendments 37
9.13. Dispute resolution provisions 37
9.14. Governing Law 37
9.15. Compliance with applicable law 37
9.16. Miscellaneous provisions 37
9.17. Other Provisions 37

1. Introduction

1.1. Overview

This document describes the establishment of a Certification Authority for the Public Key Infrastructure used by SSLCOM for issuance of SSL/TLS Server Certificates, and aims at assuring secure and reliable practices for identification and usage of such certificates.

This Certification Practice Statement defines the processes, procedures and requirements that govern SSLCOM public key infrastructure, for the issuance of SSL/TLS certificates using two forms of validation:

- Domain Validated (DV) certificates
- Organization validated (OV) Certificates

1.2. Document Name and Identification

This document shall be titled SSLCOM Certification Practice Statement (CPS) for provision of SSL Certificates, based on the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile as published by the Internet Engineering Task Force (IETF)

This document is based on the requirements of RFC 3647 as published by IETF, and adheres to the CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.3, published at http://www.cabforum.org. (hereinafter referred to as: CabForum). The Baseline Requirements describe certain minimum requirements that a Certification Authority (CA) must meet in order to issue SSL Certificates. In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this CPS.

This document shall govern the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, SSLCOM Certificates and providing associated trust services for all Participants, and is conformant to the requirements of the CA Browser Forum, in accordance with the audit standard WebTrust, version 2.3.

1.3. PKI Participants

1.3.1. Certification Authority

Certification Authority (CA) is a term that refers to all entities authorized to issue, manage, revoke, and renew certificates.
Under the SSLCOM PKI system, only CA's authorized by SSLCOM Root CA may issue SSLCOM certificates.

1.3.2. Registration Authority

Registration Authorities (RAs) are entities that approve and authorize applications to issue, renew, or revoke Certificates. RAs are generally responsible for identifying and

authenticating Applicants for Certificates, verifying their authorization to request Certificates, approving entities, and/or devices to be named in Certificates, and authorizing and/or requesting a CA to issue, renew, or revoke a Certificate to an individual, entity or device. The SSLCOM Registration Authority will only process Certificate Signing Requests for the SSLCOM CA. In the future it may be able to issue request for external CA's.

1.3.3. Subscribers

Subscribers are parties that have been issued SSLCOM Certificates, hold the Private Key corresponding to the Public Key specified in the Certificate, and are authorized to use such Certificate, upon having agreed to the Subscriber Agreement and the Terms herein. .

1.3.4. Relying Parties

Relying Parties are the recipients of the SSLCOM Certificate, who use it or rely on it for verification or for encryption purposes.

1.4. Certificate Usage

1.4.1. Certificate Usage

Digital Certificates are electronic documents used for identification purposes, by binding a specific Public Key to a certain identity. Under this CPS, Certificates may be used only for purpose of authentication of Internet Servers.
The SSLCOM CA shall issue SSL/TSL Certificates, for Server authentication.
The initial stages of operation, to which this CPS applies, shall include only SSL certificates using two forms of validation:

- **Domain Validated (DV) certificates** – these shall be used for basic security and encryption purposes, and will not provide identification or authentication, beyond identification of the acknowledged Domain.
- **Organization validated (OV) Certificates** - these shall be used as a higher means of security for encryption purposes as well as for organization identification.

Future use may include Extended Validation Certificates (EV), in which case this CPS must be adjusted accordingly.

1.4.2. Prohibited Usage

- Certificate under this CPS shall adhere to any restriction specified within this document or under any applicable law.
- DV Certificates shall not be used as a source of personal identity authentication
- This CA will not issue Certificates for the purpose of individual digital identification or signature.

1.5. Policy Administration

1.5.1. Organization administrating the document

This CPS is issued and managed by SSLCOM Group Ltd.

Version No.	**Day of publish**
SSLCOM Group CPS v1.0	December 23, 2018

1.5.2. Contact person

Contact person for purposes of the SSLCOM CA is as follows:
almostfreessl.com/support/contactus

1.6. Definitions and Acronyms

Term	Definition
Applicant	The entity that applies for a Certificate, or the renewal thereof. This includes the entity applying for a certificate on behalf of a device to be named in the Certificate.
CA	Certification Authority – An organization that is responsible for the creation, issuance, revocation, and management of Certificates.
Certificate	An electronic document that uses a digital signature to bind a public key and an identity
CPS	Certification Practice Statement- One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
CRL	Certificate Revocation List – A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates
HSM	Hardware Security Module – A device used for secure and encrypted storage of critical system data such as the CA Private Key.
PKI	Public Key Infrastructure – A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
OCSP	Online Certificate Status Protocol – An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.
RA	Registration Authority – A Role under the CA that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both
Relying Party	Any natural person or Legal Entity that relies on a Valid Certificate.

Term	Definition
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
ROOT CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Subscriber	An Entity that has been issued a Certificate.
Online CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates
X.509	The International Telecommunications Union standard for Certificates and their corresponding authentication framework
CRL	Certification Revocation List - A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

2. Publication and Repository Responsibilities

2.1. Legal Document Repositories

SSLCOM CA shall make all relevant, public, legal documents pertaining to its CA and PKI services, available to the public at https://www.sslcomgroup/cps, and shall be reviewed annually for any updates and changes. A revised version shall be published within a week of final approval, in accordance with section 9.12 of this CPS.

2.2. Publication of Certification information

2.2.1. CRL publishing

The SSLCOM CA shall make its revocation information publicly available on a regular basis, in accordance with the terms and conditions under the SSLCOM CPS.

The SSLCOM CA shall make available publish of its CRLs in two different Repositories, updated on a regular basis. These CRLs will be made available at:

a. http://crl01.sslcomgroup.com/SSLCom_TLS_DV_CA_G1.crl
b. http://crl02.sslcomgroup.com/SSLCom_TLS_DV_CA_G1.crl

2.3. Time and Frequency of Publication

2.3.1. CRLs will be updated immediately upon revocation of a Certificate, and no later than 24 hours from revocation. In addition, CRLs will be periodically updated and published, no less than once every 4 days.

2.3.2. In addition to its CRL services, the SSLCOM CA shall maintain an online OCSP Repository, constantly updated, available at:

http://ocsp.sslcomgroup.co/ocsp.cgi

2.4. Access Controls

All documents published to the SSLCOM Repositories are governed by the SSLCOM CPS and shall be fully available for public reference.

Logical access control and version control measures are used to prevent unauthorized modification of the Repository.

3. Identification and Authentication (I&A)

3.1. Naming

3.1.1. Types of Names

The Subject names in the SSL Certificate comply with the ITU X.500 Distinguished Name (DN) form. The following naming convention shall be used:

Root CA	
CA Name	**SSLCom Root G1**
Organizational Unit	Certification Services
Organization	SSLCom Group ltd.
Locality	<City>
State or Province	<City>
Country	IL
Cryptographic Service Provider	PKCS#11
Hash Algorithm	SHA2
Key Length	4096 bits
Validity Period	25 Years

Online CA	
CA Name	**SSLCom TLS DV CA G1**
Organizational Unit	Domain Validation SSL
Organization	SSLCom Group ltd.
Locality	<City>

State or Province	<City>
Country	IL
Cryptographic Service Provider	PKCS#11
Hash Algorithm	SHA2
Key Length	2048 bits
Validity Period	12 Years

3.1.2. Meaning of Names

Domain names included in the CN shall identify the object or entity to which they are assigned, in a meaningful way.
The names in the Certificates will properly identify the Subject and Issuer.

3.1.3. Anonymity or pseudonymity of subscribers

Pseudonyms will not be accepted for issuance of SSL Certificates.

3.1.4. Rules of Interpretation

Names shall be interpreted according to their assigned meaning, and in compliance with ITU Standard x500.

3.1.5. Uniqueness of names

Uniqueness of a Subject Name is not enforced, but each Certificate shall include a unique serial number identifier.

3.1.6. Recognition, authentication, and role of trademarks

A subscriber shall not request the inclusion of a Name in which he has no legitimate rights.

3.2. Initial Identity Validation

This CPS allows for two methods of subscriber identification, as follows:

i. Domain Validated (DV)
ii. Organization Validated (OV)

3.2.1. Private Key Possession

A Digital Certificate includes a Public Key, which is uniquely connected to a single Private Key.
The Applicant must prove possession of the companion private key for the public key being registered. This process is accomplished by submitting a Certificate Signing Request (CSR), compliant with PKCS #10 format requirements. This process assures that the Encryption key pair will be generated by the Applicant, and therefore the private key will at no point in time be in the possession of the SSLCOM CA.

3.2.2. Authentication of Organization and Domain Identity

For DV Certificates, either of the following methods may be used to validate Domain control.
Upon receiving the CSR, the Registration Authority will conduct a Domain Control Validation process, to verify the Applicant's ownership or rightful control of the requested Domain.
The RA will make sure to maintain a record of the Domain Validation process used.

3.2.2.1. Email to Domain Contact

In confirmation of the Applicant's control over the Domain, based on the domain Admin registered email, the RA shall send the Applicant a response email containing a Random Value code, which will then be confirmed by the Applicant, using the email address identified as a Domain Contact.
The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.
This process conforms to the requirements in section 3.2.2.4.2 of the CAB Forum Document.

3.2.2.2. Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.
This process conforms to the requirements in section 3.2.2.4.4 of the CAB Forum Document.

3.2.3. Personal Identification

In applying for an SSL Certificate to be issued by the Online CA, in the event the applicant is a natural person, the Applicant's identity and address shall be verified using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant’s legal creation, existence, or recognition; OR
2. A third party database that is periodically updated and considered a Reliable Data Source; OR
3. A site visit by the CA or a third party who is acting as an agent for the CA; OR
4. An Attestation Letter.

Further requirements regarding Application process are specified in Section 4.2 herein.

3.2.4. Non Verified Subscriber Information

The SSLCOM CA shall not be responsible for any non-verified individual or organizational information submitted for the purpose of inclusion in the certificate.

3.2.5. Validation of Authority

The CA uses a Reliable Method of Communication to verify the authenticity of the Applicant Representative’s certificate request. The method described in section 3.2.4 above shall be considered a reliable method herein.

3.2.6. Criteria for interoperation

SSLCOM maintains the right to interoperate with another CA and any such cross certification shall require listing the external CA within its repository.

3.3. Identification and Authentication for Re-key Requests

Re-key can be required either upon routine re-key, during its Validity Period, or after Certificate Revocation.
In both cases, a full identification and authentication procedure will take place, and a new key pair will be generated: A CSR shall be submitted. original, valid key. The

signature and information in the CSR shall be verified against the registered Domain information. Upon validation, a new Certificate key will be issued.

3.4. Identification and Authentication for Revocation Requests

3.4.1 A Subscriber can at any time request Revocation of his Certificate by either of two methods:

(a) Customer support center
(b) Online Revocation Request

3.4.2 In both cases, the RA will take action to verify the Identification of the Subscriber, and the Certificate will be revoked only upon such validation.
In submitting a request through the SSLCOM Portal, the Subscriber will use the Username and Password given to him upon initial registration,

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can submit a Certificate Application

Applications for a Certificate may be submitted by an Applicant representative.
SSLCOM maintains an internal database of all previously revoked Certificates and previously rejected certificate requests. That database is used to identify subsequent suspicious certificate requests.

4.1.2. Enrollment process and responsibilities

An Applicant will submit a Certificate Application based on the PKCS#10 format.
The Application shall include the following:

- The public key from a key pair generated by the applicant
- A Fully Qualified Domain Name to be included in the Certificate
- Identification Information and Documentation regarding the Subscriber, as required by SSLCOM during the application process
- A Signed Subscriber Agreement
- Any other required information

4.2. Certificate Application Processing

4.2.1. Performing identification and authentication functions

Upon receipt of the Application Request, SSLCOM will follow the rules herein and conduct a reasonable Domain Verification Procedure, to ensure the completeness, accuracy and authenticity of the information provided by the Applicant.

4.2.2. These verification procedures shall include:

- Reading the Domain details from the Request
- Comparing the Domain information with the Registered Domain information
- Validity of the Domain Registration

4.2.3. Time to process Certification applications

Certificate applications will be processed within a reasonable timeframe.

4.3. Certificate Issuance

4.3.1. CA actions during Certificate acceptance

- The SSLCOM RA will verify that the application is intact, that all the required information is included, and that payment is concluded for the Application.
- The RA will make reasonable efforts to process Requests without un-necessary delay, provided that the subscriber provides complete, accurate and reliable information, as required herein.

4.3.2. Notification to Subscriber of Certificate issuance

- Following verification of all required details in Application Request, the RA shall send a confirmation email to the Applicant, including a Random Value generated coded, as specified is Section 3.2.4 above.
- Upon receipt of confirmation of the code by the Applicant, the RA shall proceed to issue the Certificate, and send an email notification to the Subscriber to such effect.

4.4. Certificate Acceptance

4.4.1. Conduct constituting certificate acceptance

A Subscriber is deemed to have accepted a Certificate by using it, or when 15 days have passed from the date of issuance;

4.4.1.1. By accepting a Certificate, the Subscriber agrees to the following:

- It is bound by the continuing obligations and duties under the Subscriber Agreement and this CPS;
- It provided, to the best of its knowledge, complete and accurate information in application for the Certificate;
- Its Private Key, associated with the Public Key on the Certificate, has not been compromised, to the best of its knowledge.
- It will immediately inform SSLCOM of any event that may invalidate or otherwise diminish the integrity of the Certificate;

4.4.2. Publication of the certificate by the CA

The CA will provide the Subscriber with a link to the Certificate.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Key Usage Responsibilities -

- The subscriber may use a SSLCOM Server Certificate and Key only for appropriate applications as set forth in this CPS and the Subscriber Agreement, and as is in consistency with applicable certificate content.
- The Subscriber will take all reasonable measures to safeguard keep confidential his Private Key that corresponds to the Public Key in the Certificate.

4.5.2. Relying Party Key Usage Responsibilities –

- A Relying Party may rely on a subscriber's Certificate only for the purposes set forth in this CPS and in accordance with applicable certificate usage.

- A Relying Party will be responsible to check any limitations or expiration date as listed in the Certificate or associated therein.

4.6. Certificate Renewal

SSLCOM does not offer specific procedures for Renewal, which is different than the original request. In the event of Renewal of a Certificate which is still valid and has not been revoked or expired, the following shall take place:

- The Subscriber shall access the SSLCOM Online Portal using his Username and Password, as defined during initial registration
- The Subscriber will select the Certificate Renewal Option and submit a new Certificate Signing Request.
- Request for Domain shall be verified, using same verification process as specified for Registration in section 4.2.2 above.
- All additional processes shall be identical to Initial Issuance procedures.

4.7. Certificate Re-key

Certificate Re-key is not supported.

4.8. Certificate Modification

In the event of changes to any information in the certificate, a new Certificate will be issued. SSLCOM will not issue modified Certificates.

4.9. Certificate Revocation and Suspension

Certificate revocation is an irreversible process that renders the Certificate invalid, and indicates that it is no longer to be relied upon.

SSLCOM will revoke a Certificate upon receiving a valid Revocation Request from its RA. Such Certificate will no longer be valid, and its serial number will be published in a Certification Revocation List and an OCSP update is produced, as described herein.

Certificate Suspension is not supported.

4.9.1. Circumstances for Revocation

4.9.1.1. Subscriber Certificate Revocation

The CA shall revoke a Certificate within 24 hours from receipt of the Revocation Request, after confirming the Subscriber identity, in one of the following circumstances:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA or RA obtain reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or that the Certificate was misused.
4. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use, or

that it no longer has rightful use of the Qualified Domain registered in the Certificate;

5. The CA is made aware of a material change in the information contained in the Certificate;
6. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
7. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
8. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
9. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Any other reasonable grounds by which the CA or RA need to revoke a Certificate, in compliance with this here CPS

4.9.1.2. Subordinate CA Certificate Revocation

The Root CA shall revoke the Online CA Certificate within seven (7) days if one or more of the following occurs:

1. The Online CA notifies the Root CA that the original certificate request was not authorized and does not retroactively grant authorization;
2. The Root CA obtains reasonable evidence that the Online CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or the Certificate was misused;
3. The Root CA is made aware that the Certificate is not in compliance with any substantive requirements of this document;
4. The Root CA or Online CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
5. Revocation is required by the Root or Online CA's Certification Practice Statement;

4.9.2. Who Can Request Revocation

A subscriber or CA may request Revocation of a Certificate. Third Parties, including Relying Parties, may provide information on which a request may be based, but they are not entitled to submit a Request.

4.9.3. Procedure for Revocation

4.9.3.1. A subscriber that wishes to update or revoke his Certificate, will access the Web Portal using the Username and Password he was given upon registration to the service.

4.9.3.2. Subscriber will select relevant Certificate and request its revocation.

4.9.3.3. The CA shall review the Revocation Request, and send verification request to the subscriber registered email. If the Subscriber information is confirmed, it shall revoke the validity of the Certificate within 24 hours from the Revocation Request submission.

4.9.4. Revocation Request grace Period

No Grace Period is defined with this CPS.

4.9.5. Time for Processing Revocation Request

4.9.5.1. The RA will make all reasonable efforts to conduct verification procedures immediately upon receipt of the Request, and no longer than 24 hours from such request.

4.9.5.2. The CA will publish the Revoked Certificate serial number in the CRLS within 24 hours from completion of verification of the Revocation Request received from the Subscriber, and will update the OCSP responses correspondingly.

4.9.6. Revocation checking requirement for relying parties

4.9.6.1. Revocation Verification options

A Relying Party shall be responsible for checking whether the Certificate it wishes to rely on has been revoked.

It can do so by one of two alternative and interchangeable methods:

a) CRL - A Relying Party can check the Certificate Revocation Lists (CRL) maintained in one of two appropriate Repositories; or

b) OCSP - A Relying Party can perform an immediate, on-line revocation status check using OCSP to determine whether the Certificate it wishes to rely on has been revoked.

4.9.6.2. Relying Party Responsibility

In no event shall the SSLCOM CA be liable for any damages whatsoever due to (i) the failure of a Relying Party to check for revocation or expiration of a Certificate, or (ii) any reliance by a Relying Party on a Certificate that has been revoked or that has expired.

4.9.7. CRL Issuance Frequency

Root CA CRL will be published at least once every 180 days, and upon each change to the CRL. It shall be valid for 200 days from issuance.

Online CA CRL will be published at least every 4 (four) days, or upon each change to the CRL according to the earlier of the two.

The CRL will be valid for 8 days from issuance.

4.9.8. Maximum latency for CRLs

The maximum latency for CRLs refers to the maximum time between generation of CRLs and posting of the CRLs to the repository, considering potential technical or other issues. Generally, the CA will publish CRLs within 1 hour of generation.

4.9.9. On-line Revocation Availability

The SSLCOM CA supports immediate, online validity verification to a certificate, through its OCSP Responder service. Responses conform to RFC6960, and are either:

1. Signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

4.9.10. On-line Revocation Checking Requirements

Relying parties should perform online revocation/status checks prior to relying on the Certificate.

4.9.11. Other forms of revocation advertisements available

No stipulation

4.9.12. Special requirements re key compromise

Not Applicable.

4.9.13. Certificate Suspension

Certificate Suspension Requests are not applicable under SSLCOM Certificates.

4.9.14. Who can request suspension

Not Applicable.

4.9.15. Procedure for suspension request

Not Applicable.

4.9.16. Limits on suspension period

Not Applicable.

4.10. On-line Revocation Checking Requirements

4.10.1. Operational characteristics

The CA offers CRL and OCSP revocation status checking functions.

4.10.2. Service availability

Online Revocation Status s available 24/7, unless affected by maintenance or unexpected error.

4.11. End of Subscription

A subscriber's subscription ends when its Certificate expires or when the Certificate is revoked. A subscription also ends when the applicable subscriber agreement expires and is not renewed.

4.12. Key Escrow and Recovery

Escrow services are not available.

5. Facility, Management, and Operational Controls

5.1. Physical Security Controls

5.1.1. Location and Construction

SSLCOM CA systems are hosted in a highly secure facility in Israel, protected by multi tiers of physical security controls. SSLCOM CA maintains physical security controls which meet or exceed industry standards. All procedures and controls are specified in the Security Plan procedure. The following security measures shall be enforced in regards to the facility housing the CA operational environment.

5.1.2. Physical Access

SSLCOM CA systems are housed in a secure facility (see 5.1.1). Physical access to the CA facility is automatically logged and video recorded on a 24x7 basis. Physical access to the CA facility is monitored 24x7 by onsite security personnel.

5.1.3. Power and Air Conditioning

SSLCOM CA's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- Heating/Ventilation/Air-Conditioning (HVAC) systems to control temperature and relative humidity.

5.1.4. Water Exposures

SSLCOM has taken reasonable precautions to minimize the impact of water exposure to the IT systems.

5.1.5. Fire Prevention and Protection

SSLCOM has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. The facility's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6. Media Storage

Based on SSLCOM Security policy, Media containing production software, production data, and system audit information is stored secured with appropriate physical and logical access controls designed to limit access to authorized personnel.

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Cryptographic devices are physically destroyed or securely erased in accordance the manufacturers' guidance prior to disposal.

5.1.8. Off-Site Backup

SSLCOM performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded additional storage facility and SSLCOM disaster recovery facility.

5.2. Procedural Controls

5.2.1. Trusted Roles

All personnel who have access to or control over cryptographic operations of the CA, that affect the issuance, use, or management of Certificates are considered as serving in a trusted role.

The Following Trusted Roles are maintained by the CA personnel:

- **Security Officers** - Overall responsibility for administering the implementation of the CA's security practices;
- **Implementation Officers** - System configuration and implementation;
- **System Operators** - Day-to-day operation of CA systems and system backup and recovery;
- **System Auditors** - Viewing and maintenance of CA system archives and audit logs;
- **Registration Officers** - Approval of the generation, revocation and suspension of certificates.

5.2.2. Number of persons required per task

At least two Trusted Role employees will be involved in any cryptographic-related activity.

5.2.3. Identification and authentication for each role

All personnel are required to identify and authenticate themselves, using two factor authentication mechanisms, prior to performing any trusted role.

5.2.4. Separation of Duties

No single person can conduct activities involving key generation, signing or back-up activities.

The CA follows detailed and documented procedures in assigning each employee with a Trusted Role, and verifying separation of powers and authority as regards all activities involving Encryption Keys.

5.3. Personnel Controls

5.3.1. Qualifications

The CA verifies that each Trusted Personnel maintains the necessary skill level required to perform all required tasks satisfactorily.

5.3.2. Training Requirements

The CA shall ensure ongoing, relevant training, and will maintain records of such training to ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

5.4. Audit Logging Procedures

The CA documents all actions in the management of the lifecycle of a Certificate, according to the Audit and Control procedure, which include at least the following:

5.4.1. Types of Events Recorded

1. CA key lifecycle management events, including:
    - Key generation, backup, storage, recovery, archival, and destruction;
    - Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    - Certificate requests, renewal, and revocation;
    - All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    - Date, time, email, and end results of verification data;
    - Acceptance and rejection of certificate requests;
    - Issuance of Certificates;
    - Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    - Successful and unsuccessful PKI system access attempts;
    - PKI and security system actions performed;
    - Security profile changes;
    - System crashes, hardware failures, and other anomalies;
    - Firewall and router activities; and
    - Entries to and exits from the CA Cage.

5.4.2. Content of Logs

All logs will include the following elements:

- Date and time of entry
- Serial or sequence number of entry

- Source of entry
- Identity of entity making log entry

5.4.3. Retention Period for Audit Logs

The CA retains any audit logs generated for at least seven years.

5.4.4. Log Backup

All logs are backed up on a daily basis and held at a secure off-site location.

5.4.5. Log Review

Logs are reviewed periodically according to the practices established at the CA proceedures

5.5. Records Archival

5.5.1. Types of Records archived

The following data may be archived by SSLCOM:

- CA and Subscriber Certificate lifecycle management information
- Audit data
- Certificate application information and supporting documentation

5.5.2. Retention Period for Archive

The CA retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3. Protection of Archive

Archive information will be protected in a separate location, with security measures and procedures that will reasonable prevent any unauthorized access, modification or destruction of any information therein.

5.5.4. Archive Backup Procedures

SSLCOM employs backup procedures that ensure a complete set of required copies of the archives, as defined herein, will be available in the event of loss or damage.

5.5.5. Requirements for Time-stamping of Records

Certificate issuance and revocation information will be Timestamped by the CA.
All Audit logs will include system server Time Logging information.

5.6. Key Changeover

Due to technological developments and increased risk of encryption vulnerability over time, SSLCOM will periodically replace the Root CA Certificates and all Online CA Certificates that are signed by the Root CA Certificate.
The old CA Certificates will be managed and subject to CRL publication by the CA, until final expiration.
In order to avoid disruption to Subscriber activity, the Root CA will create a new key pair at every half-life of the CA Certificate, as follows:

CA Server	Validity	Renewal

Root CA	25 years	12 years
Machine CA	12 years	5 years

The old CA Certificates will be managed until they reach their expiration date

5.7. Compromise and Disaster Recovery

The CA at all times maintains updated Business Continuity and Disaster Recovery Plans. These plans set out the procedures necessary to ensure business continuity, recovery or in the event of a disaster, and notification of all relevant parties and stakeholders.
All of the above components allow the CA business and operation continuity, without actually affecting the ongoing CA operations and service.

The SSLCOM CA is designed so as to allow full redundancy and enable operation in cases of a Disaster event. The CA shall at all times maintain a detailed Business Continuity Plan to such effect.
Said Plan includes reference to all of the following components:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes.
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

This disaster recovery plan aims to allow the CA to minimize interruptions to its CA

5.8. CA or RA Termination

In the event that for any reason, SSLCOM will have to terminate operation of its RA or CA, it will make all reasonable efforts to minimalize the impact of such termination. This includes:

- Providing practicable and reasonable prior notice to all Subscribers;

- Assisting with the orderly transfer of service, and operational records, to a successor CA, if any;
- Preserving all records for seven years, as required by this CPS, after which all records will be deleted.
- Revoking all Certificates issued by the CA no later than at the time of termination.

If commercially reasonable, prior notice of the termination will be given at least 2 months before the termination date.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

In any case of a CA key Pair Generation, SSLCOM abides by the following:

a) Generates the keys in a physically secured environment;
b) Generates the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
c) Generates the CA keys within cryptographic modules meeting applicable technical and business requirements. Both Root CA and Online CA Key Pairs are generated pursuant to formal key generation procedures using Trustworthy Systems meeting the requirements of at least FIPS 140-2 Level 3 cryptography module;
d) Logs its CA key generation activities; and
e) Maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certification Practice Statement.

6.1.1.2. RA key Pair Generation

6.1.1.3. Subscriber Key Pair Generation

Subscriber Key Pair is generated by software, normally supplied with the device operating system or relevant application environment, based on RSA encryption. SSLCOM is not involved in the generation of subscriber keys, and does not have access to the private key generated by its subscriber.
Therefore, it is not required to deliver private keys or notify of their generation.

6.1.2. Private Key Delivery to Subscriber

Private Keys are generated by Subscribers. No delivery required.

6.1.3. Public Key Delivery to Certificate Issuer

Subscriber Subscribers provide their public key to SSLCOM for certification through PKCS#10 Certificate Signing Request.

6.1.4. CA Public Key Delivery to Relying Party

Not Applicable

6.1.5. Key sizes

SSLCOM CA key pairs have a minimum key size of 2048 bit RSA. SSLCOM end-user Subscribers key pairs are 2048 bit or higher RSA keys.

Certificate purpose	Minimum RSA key size (bits)	Minimum Digest Algorithm
Root CA	4096	SHA-256
Online CAs	2048	SHA-256
Subscribers	2048	SHA-256

6.1.6. Public Key Parameters Generation and Quality Checking

SSLCOM generates the public key parameters. SSLCOM's CA keys are generated within a FIPS 140-2 certified HSM.

6.1.7. Key usage purposes

CA Private Keys will be used for Certificate signing for Root CA, Online CA, infrastructure certificates, and OCSP Responders.
Certificate Usage is limited by the extensions specified in the X509 Key Usage Extension Fields.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

All CA private keys used to sign certificates, CRLs, or any related information use hardware security modules meeting FIPS 140-2 Level 3 or higher.

6.2.2. Private Key Multi-Person control

The CA private Key shall be split for all purposes between at least two trusted personnel members.

6.2.3. Private Key Escrow

Private Key Escrow is not supported by the CA.

6.2.4. Private Key Backup

1. **CA Private Key** – CA Private Keys will have a backup copy, based on routine procedure to ensure recovery and disaster recovery purposes. Key copies will be stored encrypted within hardware cryptographic module dedicated partitions.
2. **Subscriber Private Key** – the subscriber is solely responsible for protection and backup of its private key. SSLCOM CA does not offer backup services for subscriber private keys.

6.2.5. Private Key Archival

Upon termination, the Private Keys will be archived securely using industry standard hardware cryptographic modules.

6.2.6. Method of Activating Private Key

A private key can be activated by a Subscriber, CA, or other authorized personnel.
Private keys are activated in accordance with the specifications of the cryptographic module.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

To the extent that Public Keys are archived, this will be in compliance with the specifications of Section 5.5 herein.

6.3.2. Key Usage Periods

For SSLCOM CAs and Subscribers, key and certificate usage periods meet the following requirements:

Certificate purpose	Maximum key usage period	Maximum Validity period
Root CA	12 years	25 years
Online CAs	5 years	12 years
Subscribers	24 months	26 months

6.4. Activation Data

Activation data refers to data values other than whole private keys that are required to operate CA private keys or cryptographic modules. This includes PINs, passphrases, and portions of private keys used in a key splitting regime.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

SSLCOM CA system information is protected from unauthorized access through a combination of operating system controls, physical controls and network controls.
The CA Hardware includes various security controls for the cryptographic modules, and the supporting servers and workstations on which the CAs operation is physically secured.

The operating systems of the servers and workstations on which CAs operates, enforce users identification and authentication. Multi-factor authentication method is enforced for all accounts directly involved with certificate issuance

6.5.2. Computer security rating

No stipulation.

6.6. Life Cycle Security Controls

6.6.1. System Development Controls

SSLCOM CA uses software that has been formally tested for suitability and fitness for purpose. Hardware is procured only from industry-standard vendors. Software Developments done by SSLCOM approvals are verified at all stages of development according with SSLCOM development and change management policy.

6.6.2. Security Management Controls

SSLCOM CA operates a framework of internal controls that comprises technical, organizational, and procedural measures.

6.7. Network Security Controls

SSLCOM implements a multi-level security program, designed to protect its CAs environments and networks. In this security program, general protections for the network include:

- Maintaining Root CA System in a high security isolated zone.
- Configuring network boundary controls (firewalls, switches, routers, and gateways) with rules that support only approved services, protocols, ports, and communications;
- For Certificate Systems, implementing detection and prevention controls to guard against viruses and malicious software; and
- Maintaining authentication keys and passwords strict policy for any privileged account or service account on a Certificate System.

6.8. Timestamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

SSLCOM Certification Authorities issue certificates in accordance with the X.509 version 3, containing the standard fields specified in the tables below:

7.1.1. ROOT CA Certificate Profile:

Field	Criticality	OID	Type	Value	Length	Description	Remarks
Root CA certificate							
version			INTEGER	V3		Ver. 3	
serialNumber			INTEGER		Max 20 bytes	Unique number of the certification for the CA	
Signature algorithm		1.2.840.113549.1.1.11	OID	Sha256RSA		Sha256WithRSAEncryption.	
Encryption algorithm		1.2.840.113549.1.1.1	OID	null		RSAEncryption	
issuer						RDNSequence consists of attribute type (OID) and value (String)	The attribute type has to be directoryString with UTF8Encoding
countryName		2.5.4.6	printableString	**IL**	2 bytes		
organizationName		2.5.4.10	printableString	**SSLCOM Group ltd.**	Max 64 Bytes		
organizationUnitName		2.5.4.11	printableString	**Certification Services**	Max 64 Bytes		
commonName		2.5.4.3	printableString	**SSLCom Root G1**	Max 64 Bytes		

validity			SEQUENCE	2 strings of utctime	26 bytes	The value is a sequence of two utctime strings which represent the not before and not after time.	
notBefore			UTCTime	YYMMDDhhmmssZ	13 bytes		
notAfter			UTCTime	YYMMDDhhmmssZ + 25Y	13 bytes		
Subject			Name (RDNSequence)			Details in English	
CN		2.5.4.3	teletexString	**SSLCom Root G1**	Max 64 Bytes		
OrganizationUnit		2.5.4.11	teletexString	**Certification Services**	Max 64 Bytes		
Organization		2.5.4.10	teletexString	**SSLCOM Group ltd.**	Max 64 Bytes		
Country		2.5.4.6	teletexString	**IL**	2 bytes		
Subject Public Key Info							The length can be increased in the future
Subject Public Key			BIT STRING		4096 bit		Root CA Public key
Extensions:							
keyUsage	C	2.5.29.15.5 2.5.29.15.6		keyCertSign cRLSign			This field is critical It has 2 values encoded as bit string

7.1.2. ONLINE CA Certificate Profile:

Field	Criticality	OID	Type	Value	Length	Description	Remarks
Online CA DV certificate							
version			INTEGER	V3		Ver. 3	
serialNumber			INTEGER		Max 20 bytes	Unique number of the certification for the CA	
Signature algorithm		1.2.840.113549.1.1.11	OID	Sha256RSA		Sha256WithRSA Encryption.	
Encryption algorithm		1.2.840.113549.1.1.1	OID	null		RSAEncryption	
issuer						RDNSequence consists of attribute type (OID) and value (String)	The attribute type has to be directoryString with UTF8Encoding

countryName		2.5.4.6	printableString	**IL**	2 bytes		
organizationName		2.5.4.10	printableString	**SSLCOM Group ltd.**	Max 64 Bytes		
organizationUnitName		2.5.4.11	printableString	**Certification Services**	Max 64 Bytes		
commonName		2.5.4.3	printableString	**SSLCom Root G1**	Max 64 Bytes		
validity			SEQUENCE	2 strings of utctime	26 bytes	The value is a sequence of two utctime strings which represent the not before and not after time.	
notBefore			UTCTime	YYMMDDhhmmssZ	13 bytes		
notAfter			UTCTime	YYMMDDhhmmssZ + 10Y	13 bytes		
Subject			Name (RDNSequence)			Details in English	
CN		2.5.4.3	teletexString	**SSLCom TLS DV CA G1**	Max 64 Bytes	Combination of surname and given-name	
OrganizationUnit		2.5.4.11	teletexString	**Domain Validation SSL**	Max 64 Bytes		
Organization		2.5.4.10	teletexString	**SSLCOM Group ltd.**	Max 64 Bytes		
Country		2.5.4.6	teletexString	**IL**	2 bytes		
Subject Public Key Info							The length can be increased in the future
Subject Public Key			BIT STRING		2048bit		Online CA Public key
Extensions:							
keyUsage	C	2.5.29.15.0 2.5.29.15.5 2.5.29.15.6		digitalSignature keyCertSign cRLSign			This field is critical It has 2 values encoded as bit string
extendedKeyUsage		2.5.29.37	List of OID	serverAuth (1.3.6.1.5.5.7.3.1) clientAuth			

				(1.3.6.1.5.5.7.3.2)			
certificatePolicies		2.5.29.32					certificatePolicies
Certificate Policy		2.23.140.1.2.1	Policy identifier	Domain-validation			
CPS Pointer Qualifier		1.3.6.1.5.5.7.2.1	Policy Qualifier Data	https://www.sslcomgroup.com/cps			This field include both OID and URI string which points to the CPS
authorityKeyIdentifier		2.5.29.35	Octet string	Depends on the key of the ca issued the certificate			
subjectKeyIdentifier		2.5.29.14	Octet string				
CRL Distribution Points		2.5.29.31	Octet String	http://crl01.sslcomgroup.com/SSLCom_Root_G1.crl http://crl02.sslcomgroup.com/SSLCom_Root_G1.crl			Two http locations
Authority Information Access		1.3.6.1.5.5.7.48.2	Sequence of two fields.	url= http://crt.sslcomgroup.com/repository/**SSLCom_RootCA_G1**.crt			pointer in url format to a file on a web server which holds the certificate of the issuer OID
		1.3.6.1.5.5.7.48.1		url=http://ocsp.sslcomgroup.com/ocsp.cgi			pointer in url format to web application that serves as an OCSP application

7.1.3. Web Server Subscriber DV Certificate Profile:

Field	Criticality	OID	Type	Value	Length	Description	Remarks
WebServer DV certificate							
version			INTEGER	V3		Ver. 3	
serialNumber			INTEGER		Max 20 bytes	Unique number of the certification for the CA	
Signature algorithm		1.2.840.113549.1.1.11	OID	Sha256RSA		Sha256WithRSA Encryption.	
Encryption algorithm		1.2.840.113549.1.1.1	OID	null		RSAEncryption	
issuer						RDNSequence consists of attribute type	The attribute type has to be directoryString

						(OID) and value (String)	with UTF8Encoding
countryName		2.5.4.6	printableString	**IL**	2 bytes		
organizationName		2.5.4.10	printableString	**SSLCOM Group ltd.**	Max 64 Bytes		
organizationUnitName		2.5.4.11	printableString	**Domain Validation SSL**	Max 64 Bytes		
commonName		2.5.4.3	printableString	**SSLCom TLS DV CA G1**	Max 64 Bytes		
validity			SEQUENCE	2 strings of utctime	26 bytes	The value is a sequence of two utctime strings which represent the not before and not after time.	
notBefore			UTCTime	YYMMDDhhmmssZ	13 bytes		
notAfter			UTCTime	YYMMDDhhmmssZ	13 bytes		Up to 24 months
Subject			Name (RDNSequence)			Details in English	
CN		2.5.4.3	teletexString	***<hostname.domain name>***	Max 64 Bytes	Combination of surname and given-name	
OrganizationUnit		2.5.4.11	teletexString	**Domain Control Validation**	Max 64 Bytes	EmpNo. or ID No. or Passport No.	
Subject Public Key Info							The length can be increased in the future
Subject Public Key			BIT STRING		2048bit		Webserver Public key
Extensions:							
keyUsage	C	2.5.29.15		digitalSignature (0) keyEncipherment (2)			This field is critical It has 2 values encoded as bit string
extendedKeyUsage		2.5.29.37	List of OID	Client Authentication (1.3.6.1.5.5.7.3.2) Smartcard Logon			

				(1.3.6.1.4.1.311.20.2.2)			
certificatePolicies		2.5.29.32					certificatePolicies
Certificate Policy		2.23.140.1.2.1	Policy identifier	Domain-validation			
CPS Pointer Qualifier		1.3.6.1.5.5.7.2.1	Policy Qualifier Data	https://www.sslcomgroup.com/cps			This field include both OID and URI string which points to the CPS
authorityKeyIdentifier		2.5.29.35	Octet string	Depends on the key of the ca issued the certificate			
subjectKeyIdentifier		2.5.29.14	Octet string				
CRL Distribution Points		2.5.29.31	Octet String	http://crl01.sslcomgroup.com/SSLCom_TLS_DV_CA_G1.crl http://crl02.sslcomgroup.com/SSLCom_TLS_DV_CA_G1.crl			Two http locations
Authority Information Access		1.3.6.1.5.5.7.48.2	Sequence of two fields.	url= http://crt.sslcomgroup.com/repository/**SSLCom_TLS DVCA_G1**.crt			pointer in url format to a file on a web server which holds the certificate of the issuer OID
		1.3.6.1.5.5.7.48.1		url=http://ocsp.sslcomgroup.com/ocsp.cgi			pointer in url format to web application that serves as an OCSP application
Subject Alternate Name (OID 2.5.29.17)							
dNSName	C		IA5-STRING (2)	<***hostname.domain name***>			
dNSName			IA5-STRING (2)	<***domainname***>			

7.2. CRL Profile

SSLCOM issues CRLs for its Certification Authorities, conforming to RFC 5280 standard.

Field	Description

Version	V2
Signature Algorithm	SHA-256
Issuer	Issuer Name of the entity who has signed and issued the CRL, in accordance with the Issuer certificate Distinguished Name.
This Update / Effective Date	Date and time of CRL issuance.
Next Update	Date and time by which the next CRL will be issued. The Next Update date for **SSLCOM** CRLs is set as follows: 12 months from the Effective Date for **SSLCOM** Root CAs and 4 days from the Effective Date for other **SSLCOM** Online CAs. CRL issuance frequency is in accordance with the requirements of CPS paragraph 4.9.7.
Revoked Certificates	List of revoked certificates including the following information: • Serial Number, identifying the revoked certificate • Revocation Date, including the date and time of the revocation
CRL Reason code	One of the following reason codes: unspecified (0) keyCompromise (1) cACompromise (2) affiliationChanged (3) superseded (4) cessationOfOperation (5) certificateHold (6) removeFromCRL (8) privilegeWithdrawn (9) aACompromise (10)

7.3. OCSP Profile

OCSP profile provided under this Certification Authority conform to standard IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

8. Compliance Audit and Other Assessment

8.1. Frequency or circumstances of assessment

Compliance Audits are conducted at least annually.

8.2. Identity/qualifications of assessor

Compliance audits are performed by an independent, accounting firm that is familiar with and licensed by WebTrust standard Criteria, and not otherwise affiliated with the subject of the audit.

8.3. Topics covered by assessment

Annual Compliance Audits of the CAs cover a validation of controls relevant for the proper operation of the CAs. In particular they cover an assessment of the auditee's

compliance with the WebTrust Principles and Criteria for Certification Authorities formulated by the CA/Browser Forum's Baseline Requirements.

8.4. Communication of results

The Audit Report will be made publicly available no later than three months after the end of the audit period.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

SSLCOM may charge reasonable fees for issuance, management or renewal of Certificates, in accordance with the Subscriber Agreement.

9.1.2. Certificate Access Fees

SSLCOM may charge a reasonable fee for access to its Certificate databases.

9.1.3. Revocation or Status Information Revocation Fee

SSLCOM does not charge any fee for regular revocation Services.

9.2. Financial Responsibility

SSLCOM maintains applicable professional liability insurance coverage.

9.3. Confidentiality of Business Information

9.3.1. Scope of confidential information

The following Applicant and Subscriber related information is considered confidential information.

1. Certificate applications;
2. Records submitted by the Applicant in support of Certificate applications;
3. Private keys;
4. Log files and other audit records;
5. Transaction records

9.3.2. Information not within the scope of confidential information

Certificates and Revocation Lists are not considered confidential information.

9.3.3. Responsibility to protect confidential information

The CA will make all reasonable effort to protect the confidentiality of information, subject to any law or regulation.

9.4. Privacy of Personal Information

9.4.1. Privacy plan

SSLCOM maintains and follows its Privacy Plan, which applies to all parties issuing, using or relying on SSLCOM Certificates.

9.4.2. Information treated as private

Personal information relating to Subscribers, as specified in Section 9.3.1, and excluding any information published in a Certificate, will be treated as Private information.

9.4.3. Information not deemed private

Information published in a Certificate will not be deemed private.

9.4.4. Responsibility to protect private information

SSLCOM and all relevant parties will take all reasonable measures to secure and protect the privacy of information.

9.4.5. Notice and consent to use private information

SSLCOM CA adheres to all applicable Privacy laws and regulations, and will only use private information after obtaining consent or as required by applicable laws or regulations.

9.4.6. Disclosure pursuant to judicial or administrative process

SSLCOM will disclose private information in the event that is required to do so under any law or regulation or any legal, administrative or judicial proceeding.

9.4.7. Other information disclosure circumstances

SSLCOM will not disclose private information other than as specified above.

9.5. Intellectual Property Rights

SSLCOM owns the intellectual property rights in all the CA services, information and databases, including the Certificates and all information and trademarks used in providing Certificate services and this CPS.

Private and Public Keys remain the property of the Subscribers who rightfully hold them.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

By issuing a Certificate, SSLCOM warrants that during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right or was delegated the right, to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension; (ii) followed the procedure when issuing the Certificate;;
2. That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all relevant information contained in the Certificate (with the exception of

the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate;
3. That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood of including misleading information in the Certificate;
4. That the CA maintains a 24x7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
5. That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

The Root CA SHALL be responsible for the performance and warranties of the Online CA.

9.6.2. RA Representations and Warranties

No stipulation.

9.6.3. Subscriber Representations and Warranties

Upon submitting a Certificate Application, a Subscriber agrees to be bound by this CPS, and warrants the following:

1. That he agrees to the Terms in the Subscriber Agreement and will sign it as a prerequisite for receiving certification services for the CA.
2. That he will provide the CA only with accurate and complete information in relation to the Certificate application, issuance and revocation, and that he has authorization and rights in all names, domains and entities for whom he is requesting a Certificate or any other CA services.
3. That he will take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
4. That he install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. That he will request revocation of the Certificate, and cease using it and its associated Private Key, immediately upon any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and will promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
6. That he will cease using a Certificate and private key associated with it, once it has been revoked due to key compromise.
7. That it is aware that the CA is entitled to revoke the certificate immediately in the event that the Subscriber violates any of the terms of the Subscriber Agreement or uses the Certificate for illegal activities, in addition to any other legitimate reason for revocation.

9.7. Disclaimers of Warranties

Unless specified otherwise, all certificates and any related software and services are provided "as is" and "as available." To the maximum extent permitted by law, the CA disclaims all other warranties, both express and implied, including, without limitation, any implied warranty of merchantability, any warranty of fitness for a particular purpose and any warranty of accuracy of information provided with respect to certificates issued by the CA, the CRL, and any participant's or third

party's participation in the PKI, including use of key pairs, certificates, the CRL/OCSP or any other goods or services provided by the participant.
The CA does not warrant that any service or product will be provided as expected or will be error-free.

9.8. Limitations of Liability

1. The CA may include a limitation of its liability in its agreement with its subscribers, and such terms of limitation will be binding upon all relevant parties. Certificates may indicate liability limitations based on transaction value, Usage purposes or any other limitations, as are specified in the Subscriber Agreement.
2. To the extent permitted by applicable law, SSLCOM shall not be liable for any direct, indirect, special, incidental, consequential, exemplary or punitive damages, including but not limited to damages for lost data, lost profits, lost revenue or costs of procurement of substitute goods or services, however caused and under any theory of liability, including but not limited to contract or tort.

9.9. Indemnities

9.9.1. Indemnification by Subscribers

By accepting a Certificate, the Subscriber agrees to indemnify SSLCOM from any liability for any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that it may incur, that are caused, by act or omission, in relation to 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,, or any person receiving or relying on the Certificate.
- Failure to protect the Subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

9.9.2. Indemnification by Relying Parties

By relying on an SSLCOM Certificate, relying Parties agree, to the extent allowed by applicable law, to indemnify SSLCOM for any harm or damage, caused by act or omission, in relation to reliance in a Certificate, that arises from:

- violation of any applicable law;
- breach of representations and obligations as stated in this CPS;
- reliance on a Certificate that is not reasonable under the circumstances; or
- failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10. Term and Termination

The Term of this CPS comes in force upon its publication, and shall remain in effect until replaces by a newer version.

Upon termination of this CPS, Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates.

9.11. Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, Participants shall use commercially reasonable methods for purpose of communicate with each other;

9.12. Amendments

SSLCOM has the right to make reasonable changes to this CPS, and any significant amendments to this CPS shall be published and made available to all relevant Parties.

9.13. Dispute resolution provisions

Prior to launching a Dispute Revolution proceeding the Party doing so must notify SSLCOM.

9.14. Governing Law

This CPS shall be governed by the Laws of the State of Israel, and jurisdiction over any disagreement under this CPS shall be granted to Israeli Courts of Law.

9.15. Compliance with applicable law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders, including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16. Miscellaneous provisions

No stipulation.

9.17. Other Provisions

No stipulation.