



StartCom Extended Validation Certificates Policy

Version: 1.1
Status: Final/Approved
Updated: 06/13/10
Copyright: Start Commercial (StartCom) Ltd.
Author: Eddy Nigg

1. INTRODUCTION

1.1 Overview

This document describes the policies and practices of the StartCom CA governing the issuance of Extended Validation Certificates by the StartCom CA according to the [Extended Validation Guidelines](#) as published by the [CA/Browser Forum](#).

The entire content of StartCom's websites and documents is copyrighted and all rights are reserved. You may save to disk or print out individual pages or selections of information contained within StartCom's properties for your own use, provided that you do not collect multiple small selections for the purpose of replicating or copying all or substantial portions of the obtained material.

1.2 Document name and identification

According to the "[StartCom Policy & Practice Statements](#)" (*StartCom CA Policy*), the StartCom Certification Authority, hereby called and referred to as the *StartCom CA*, issues digital certificates according to the Extended Validation Guidelines as published by the CA/Browser Forum. This document extends the StartCom CA Policy about aspects which are not already explicit or implicit covered by the StartCom CA Policy in relation to Extended Validation Certificates. The StartCom CAs regular Non-EV CA business and practices may implement requirements of the Extended Validation Guidelines already in full, in which case no special stipulation is needed.

1.3 PKI participants

1.3.1. Certification authority

1.3.1.1. Principal Statement

The StartCom CA issues EV Certificates to Private Organizations,

Government Entities, and Business Entities that satisfy the requirements specified in the Extended Validation Guidelines as published by the CA/Browser Forum.

See also section *The StartCom Certification Authority* of the StartCom CA Policy.

1.3.1.2. Commitment to Comply with Extended Validation Guidelines

The StartCom CA conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates (“Guidelines”) published at the CA/Browser Forum. In the event of any inconsistency between this document and those guidelines, those guidelines take precedence over this document.

1.3.1.3. Implementation of the Extended Validation Guidelines

The StartCom CA implements the Extended Validation Guidelines as published by the CA/Browser Forum and the requirements of the WebTrust Program for CAs and WebTrust EV Program as approved by the CA/Browser Forum. In case multiple or alternative methods or options are possible by the guidelines in order to perform a certain task and/or multiple or alternative methods or options are offered in order to comply to the guidelines, the StartCom CA reserves the right to choose any of the methods or options applicable at any times and may choose to change its procedures at all times and decide to do so on a case to case basis.

1.3.2. Registration authority

Not applicable.

1.3.3. Subscribers

See section *Subscribers* of the StartCom CA Policy.

1.3.4. Relying parties

See section *Relying Parties* of the StartCom CA Policy.

1.3.5. Other participants

Not applicable.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

See section *Subscriber Private Key and Certificate Usage* of the StartCom CA Policy.

1.4.2. Prohibited certificate uses

See section *Subscriber Private Key and Certificate Usage* of the StartCom CA

Policy.

1.5 Policy administration

1.5.1. Organization administering the document

See section *The StartCom Certification Authority* of the [StartCom CA Policy](#).

1.5.2. Contact person

See section *The StartCom Certification Authority* of the [StartCom CA Policy](#).

1.5.3. Person determining CPS suitability for the policy

See section *The StartCom Certification Authority* of the [StartCom CA Policy](#).

1.5.4. CPS approval procedures

See section *CPS Suitability, Amendments and Publication* of the [StartCom CA Policy](#).

1.6 Definitions and acronyms

Definitions and acronyms are according to the [Extended Validation Guidelines](#).

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See *CA Root Public Key Delivery to Subscribers* of the [StartCom CA Policy](#).

2.2 Publication of certification information

See *Distribution of Certificate Revocation List* and *OCSP Responder Service* of the [StartCom CA Policy](#).

2.3 Time or frequency of publication

See *Distribution of Certificate Revocation List* and *OCSP Responder Service* of the [StartCom CA Policy](#).

2.4 Access controls on repositories

See *Relying Party Obligations* of the [StartCom CA Policy](#).

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1. Types of names

See *Certificate Profiles => Naming conventions => Extended Validation* of the [StartCom CA Policy](#).

3.1.2. Need for names to be meaningful

See *Certificate Profiles => Naming conventions => Extended Validation of the StartCom CA Policy*.

3.1.3. Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4. Rules for interpreting various name forms

See *Certificate Profiles => Naming conventions of the StartCom CA Policy*.

3.1.5. Uniqueness of names

See *Certificate Profiles => Naming conventions => Extended Validation of the StartCom CA Policy*.

3.1.6. Recognition, authentication, and role of trademarks

See *Obligations => Subscriber Obligations of the StartCom CA Policy*.

3.2 Initial identity validation

3.2.1. Method to prove possession of private key

See *Subscriber Private Key Generation and Delivery of the StartCom CA Policy*.

3.2.2. Authentication of organization identity

See *Certification Rules => Validations => Extended Validation of the StartCom CA Policy*.

3.2.3. Authentication of individual identity

See *Certification Rules => Validations => Extended Validation of the StartCom CA Policy*.

3.2.4. Non-verified subscriber information

Not applicable.

3.2.5. Validation of authority

See *Certification Rules => Validations => Extended Validation of the StartCom CA Policy*.

3.2.6. Criteria for inter-operation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

See *Subscriber Private Key and Certificate Usage* of the StartCom CA Policy.

3.3.2. Identification and authentication for re-key after revocation

See *Subscriber Private Key and Certificate Usage and Rejected Certificate Applications* of the StartCom CA Policy.

3.4 Identification and authentication for revocation request

See *Revocation => Procedure for Revocation Request* of the StartCom CA Policy.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1. Who can submit a certificate application

According to the EV guidelines and as published at <http://www.startssl.com/?app=30#requirements>

4.1.1.1. Subscriber Agreement Requirements

The subscriber has to enter into a legally valid and enforceable subscriber agreement with the StartCom CA that satisfies the requirements of the CA/Browser Forum Guidelines. The StartCom CA requires that the subscriber makes the commitments and warranties set forth in the “Subscriber Agreement Requirements” section of the CA/Browser Forum Guidelines.

4.1.1.2. Certificate Request Requirements

Applicants for EV certificates must be at least Class 2 validated prior to engagements for extended validation. The applicant shall serve as the “Contract Signer”, “Certificate Approver”, and “Certificate Requester” as defined by the Extended Validation Guidelines. The applicants must make the request by the designated utility at the from the StartCom CA operated web site and sign the “StartCom Extended Validation Subscriber Agreement”.

4.1.2. Enrollment process and responsibilities

The StartCom CA verifies the applicants authorization for signing the “StartCom Extended Validation Subscriber Agreement” and authorization for approving and requesting EV certificates on behalf of the subscriber according to the requirements of the Extended Validation Guidelines.

4.2 Certificate application processing

4.2.1. Performing identification and authentication functions

The StartCom CA verifies the applicants legal existence and identity according to the “Verification Requirements” and “Methods of Verification”

specified in the Extended Validation Guidelines as published by the CA/Browser Forum.

4.2.2. Approval or rejection of certificate applications

See *Notifications => Approval and Rejection of Certificate Applications and Certificate Acceptance* by Subscribers of the StartCom CA Policy.

4.2.3. Time to process certificate applications

See *Notifications => Certificate Issuance* by Subscribers of the StartCom CA Policy.

4.3 Certificate issuance

4.3.1. CA actions during certificate issuance

See *Notifications => Certificate Acceptance by Subscribers* of the StartCom CA Policy.

4.3.2. Notification to subscriber by the CA of issuance of certificate

See *Notifications => Certificate Acceptance by Subscribers* of the StartCom CA Policy.

4.4 Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

See *Notifications => Subscriber Private Key and Certificate Usage* of the StartCom CA Policy.

4.4.2. Publication of the certificate by the CA

See *Notifications => Certificate Acceptance by Subscribers* and *Notifications => Certificate Issuance* of the StartCom CA Policy.

4.4.3. Notification of certificate issuance by the CA to other entities

See *Notifications => Certificate Issuance* of the StartCom CA Policy.

4.5 Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

See *Notifications => Subscriber Private Key and Certificate Usage* of the StartCom CA Policy.

4.5.2. Relying party public key and certificate usage

See *Notifications => Relying Party Public Key and Certificate Usage* of the StartCom CA Policy.

4.6 Certificate renewal

Renewing a certificate follows the same procedures as with a new certificate. See *Notifications => Subscriber Private Key and Certificate Usage* of the StartCom CA Policy.

4.7 Certificate re-key

Re-keying or reusing the same private key for any new or renewed certificate shall be avoided by the subscriber. See *Notifications => Subscriber Private Key and Certificate Usage* of the StartCom CA Policy.

4.8 Certificate modification

Not applicable.

4.9 Certificate revocation and suspension

4.9.1. Circumstances for revocation

See *Revocation => Circumstances for Revocation* of the StartCom CA Policy.

4.9.2. Who can request revocation

See *Revocation => Who Can Request Revocation* of the StartCom CA Policy.

4.9.3. Procedure for revocation request

See *Revocation => Procedure for Revocation Request* of the StartCom CA Policy.

4.9.4. Revocation request grace period

Not applicable.

4.9.5. Time within which CA must process the revocation request

The StartCom CA revokes the EV Certificate and issues a CRL as soon as it has determined that a properly supported revocation request has been made.

4.9.6. Revocation checking requirement for relying parties

See *Obligations => Relying Party Obligations* of the StartCom CA Policy.

4.9.7. CRL issuance frequency

See *Revocations => Distribution of Certificate Revocation List* of the StartCom CA Policy.

4.9.8. Maximum latency for CRLs

Certificate Revocation Lists are published at the on-line repository within a commercially reasonable time after generation. This is generally done automatically and immediately.

4.9.9. On-line revocation/status checking availability

See *Revocations* => *OCSP Responder Service* of the StartCom CA Policy.

4.9.10. On-line revocation checking requirements

See *Obligations* => *Relying Party Obligations* of the StartCom CA Policy.

4.9.11. Other forms of revocation advertisements available

Not applicable.

4.9.12. Special requirements re-key compromise

Not applicable.

4.9.13. Circumstances for suspension

Not applicable.

4.9.14. Who can request suspension

Not applicable.

4.9.15. Limits on suspension period

Not applicable.

4.10 Certificate status services

Not applicable.

4.11 End of subscription

Not applicable.

4.12 Key escrow and recovery

The StartCom CA does not perform escrow or recovery of subscriber private keys.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

See *Security* => *Physical Infrastructure and Records Backup and Disaster Recovery* of the StartCom CA Policy.

5.2 Procedural controls

5.2.1. Trusted roles

See *Security* => *Personnel Management and Practices* of the StartCom CA Policy.

5.2.2. Number of persons required per task

See *Security => CA Key Generation, Protection, Recovery & Publication of the StartCom CA Policy*.

5.2.3. Identification and authentication for each role

See *Security => Personnel Management and Practices of the StartCom CA Policy*.

5.2.4. Roles requiring separation of duties

See *Security => Personnel Management and Practices of the StartCom CA Policy*.

5.3 Personnel controls

See *Security => Personnel Management and Practices of the StartCom CA Policy*.

5.4 Audit logging procedures

5.4.1. Types of events recorded

See *Events, System and Audit Logs of the StartCom CA Policy*.

5.4.2. Frequency of processing log

See *Events, System and Audit Logs of the StartCom CA Policy*.

5.4.3. Retention period for audit log

See *Archival of Records and Retention Period of the StartCom CA Policy*.

5.4.4. Protection of audit log

See *Archival of Records and Retention Period of the StartCom CA Policy*.

5.4.5. Audit log backup procedures

See *Archival of Records and Retention Period of the StartCom CA Policy*.

5.4.6. Audit collection system (internal vs. external)

No stipulation.

5.4.7. Notification to event-causing subject

No stipulation.

5.4.8. Vulnerability assessments

See *Security => Security Program of the StartCom CA Policy*.

5.5 Records archival

5.5.1. Types of records archived

See *Archival of Records and Retention Period and Types of Records* of the StartCom CA Policy.

5.5.2. Retention period for archive

See *Archival of Records and Retention Period* of the StartCom CA Policy.

5.5.3. Protection of archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution or destruction. See also *Privacy and Archival of Records and Retention Period and Form of Records* of the StartCom CA Policy.

5.5.4. Archive backup procedures

See *Archival of Records and Retention Period and Form of Records* of the StartCom CA Policy.

5.5.5. Requirements for time-stamping of records

System times are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every day. All recorded events are time-stamped in the events and audit logs.

5.5.6. Archive collection system (internal or external)

Archive information is collected internally.

5.5.7. Procedures to obtain and verify archive information

See *Archival of Records and Retention Period* of the StartCom CA Policy.

5.6 Key changeover

See *Security => CA Key Changeover* of the StartCom CA Policy.

5.7 Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

See *Security => CA Key Compromise* of the StartCom CA Policy.

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

See *Records Backup and Disaster Recovery* of the StartCom CA Policy.

5.7.3. Entity private key compromise procedures

See *Security => CA Key Compromise* of the StartCom CA Policy.

5.7.4. Business continuity capabilities after a disaster

See *Records Backup and Disaster Recovery* of the StartCom CA Policy.

5.8 CA termination

See *Change Management of the StartCom CA Policy*.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1. Key pair generation

For CA keys see *Security => CA Key Generation, Protection, Recovery & Publication* of the StartCom CA Policy. For subscriber keys see *Security => Subscriber Private Key Generation and Delivery* of the StartCom CA Policy.

6.1.2. Private key delivery to subscriber

See *Security => Subscriber Private Key Generation and Delivery* of the StartCom CA Policy.

6.1.3. Public key delivery to certificate issuer

See *Notifications => Certificate Acceptance by Subscribers* of the StartCom CA Policy.

6.1.4. CA public key delivery to relying parties

See *Security => CA Root Public Key Delivery to Subscribers* of the StartCom CA Policy.

6.1.5. Key sizes

See *Certificate Profiles => Other Certificate Attributes => Key Attributes* of the StartCom CA Policy.

6.1.6. Public key parameters generation and quality checking

See *Certificate Profiles => Naming Conventions* of the StartCom CA Policy.

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

See *Certificate Profiles => Certificate Extensions* of the StartCom CA Policy.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

See *Security => CA Key Generation, Protection, Recovery & Publication* of the StartCom CA Policy.

6.3 Other aspects of key pair management

6.3.1. Public key archival

Copies of all Public Keys for archival in accordance with Section 5.5.

6.3.2. Certificate operational periods and key pair usage periods

See *Certificate Profiles* of the StartCom CA Policy.

6.4 Activation data

No stipulation.

6.5 Computer security controls

See *Security* => *Security Program* of the StartCom CA Policy.

6.5.1. Specific computer security technical requirements

See *Physical Infrastructure* => *Access Control* of the StartCom CA Policy.

6.5.2. Computer security rating

See *Physical Infrastructure* => *Site Location and Construction* of the StartCom CA Policy.

6.6 Life cycle technical controls

6.6.1. System development controls

See *Security* => *Systems Development and Maintenance* of the StartCom CA Policy.

6.6.2. Security management controls

See *Security* => *Systems Development and Maintenance* of the StartCom CA Policy.

6.6.3. Life cycle security controls

No stipulation.

6.7 Network security controls

See *Physical Infrastructure* => *Network Security* of the StartCom CA Policy.

6.8 Time-stamping

See section 5.5.5

7. CERTIFICATE, CRL, AND OCSP PROFILES

See *Certificate Profiles* of the StartCom CA Policy.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

See *Compliance Audit and Compliance Improvement* of the StartCom CA Policy.

8.1 As part of its Security Program, StartCom controls its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

See *Legal and Limitations => Fees* of the StartCom CA Policy.

9.2 Financial responsibility

9.2.1. Insurance coverage

See *Legal and Limitations => Financial Responsibility* of the StartCom CA Policy.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

See *Legal and Limitations => Certificate Insured Warranty* of the StartCom CA Policy.

9.3 Confidentiality of business information

See *Legal and Limitations => Privacy* of the StartCom CA Policy.

9.4 Privacy of personal information

See *Legal and Limitations => Privacy* of the StartCom CA Policy.

9.5 Intellectual property rights

See *Legal and Limitations => Copyright and Ownership of Certificates* of the

StartCom CA Policy.

9.6 Representations and warranties

See *EV Certificate Warranties and Representations* of the Extended Validation Guidelines.

9.7 Disclaimers of warranties

See *Legal and Limitations => Liability* of the StartCom CA Policy.

9.8 Limitations of liability

See *Legal and Limitations => Liability* of the StartCom CA Policy.

9.9 Indemnities

See *Obligations => Subscriber Obligations* of the StartCom CA Policy.

9.10 Term and termination

See *Change Management* of the StartCom CA Policy.

9.11 Individual notices and communications with participants

9.12 Amendments

See *CPS Suitability, Amendments and Publication* of the StartCom CA Policy.

9.13 Dispute resolution provisions

See *Governing Law* of the StartCom CA Policy.

9.14 Governing law

See *Governing Law* of the StartCom CA Policy.

9.15 Compliance with applicable law

See *Governing Law* of the StartCom CA Policy.

9.16 Miscellaneous provisions

9.16.1. Entire agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended

usage of the product or service described herein. Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.16.2. Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of the StartCom CA.

9.16.3. Severability

See *Legal and Limitations* => *Liability of the StartCom CA Policy*.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

See *Governing Law of the StartCom CA Policy*.


9.16.5. Force Majeure

THE STARTCOM CA INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITTS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.16.6. Other provisions

Not applicable.

This document is signed by:

	Signator:	EMAILADDRESS=certmaster@startssl.com, CN=Eddy Nigg, OU=StartCom Trusted Certificate Member, O=StartCom Ltd. (Start Commercial Limited), L=Eilat, ST=HaDarom, C=IL, OID.2.5.4.13=212311-mx47a9sjhm0y1f4Y
	Date:	Wed Jun 16 00:42:45 IDT 2010
	Issuer:	CN=StartCom Class 3 Primary Intermediate Client CA, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL
	Serial:	132

Add the StartCom CA root to your PDF reader in order to verify the signature. Download the file ca.crt from <http://www.startssl.com/certs/> and add this certificate under Document -> Manage Trusted Identities -> Certificates.