Start Commercial (StartCom) Limited

StartSSL™ Certificates & Public Key Infrastructure

Eilat, Israel

Addendum to the StartCom Certification Authority Policy & Practice Statements

Version: 1.9
Status: Approved
Updated: 01/30/12

Author: Eddy Nigg

Purpose of this Document

The purpose of this Addendum to the Policy & Practice Statements is to amend version 2.2 of the StartCom Certification Authority Policy & Practice Statements ("CPS") to include, add or modify current established policies and practice disclosure. All provisions of the CPS not specifically amended or added herein remain in full force and effect. Nothing in the CPS shall be deemed omitted, deleted or amended unless expressly stated in this ACPS or identified accordingly below. Headings from the original CPS are included to identify the location of the Amended information, and are not intended to be duplicative.

[Add at Certificate Classes – Class 1:]

Class 1 certificates are limited to client and server types, whereas the later is restricted in its usage for non-commercial purpose only. Subscribers should upgrade to Class 2 or higher level for any domain and site of commercial nature, when using high-profile brands and names or if involved in obtaining or relying sensitive information such as health records, financial details, personal information etc.

[Add at Obligations – Relying Party Obligations:]

Must not use the information contained in the certificates to harass or spam the party stated in the certificate, harvest or use the details other than necessary in order to build an opinion about it's content for reliance.

[Replace at Obligations – Subscriber Obligations:]

Subscriber Obligations

- Provide and supply correct and truthful information (including personal)

whenever indicated and requested.

- Never sign up for an account in the name of somebody else even if allegedly authorized or requested by somebody else, e.g. the account details apply to the person that physically applies and submits the request.
- Use the submission forms, web interfaces and applications of StartCom only with common web browsers and as instructed at the web sites. Refrain from batch submissions, circumvention of control validations or otherwise use the web sites other than intended.
- Maintain **exclusive** control of accounts, access thereof and related client authentication certificates.
- Never share private keys with any third party and use adequate protection and best security practices to secure private keys in order prevent losses and compromises thereof.
- Notify StartCom immediately in case of a private key compromise and request revocation of the affected certificate(s).
- Review and verify the accuracy of the data in issued certificate(s).
- Refrain from using certificates which contain erroneous, misleading or incomplete data.
- Notify StartCom immediately in case erroneous data is detected in account profiles or certificates.
- Use the certificates in accordance with all applicable laws and never use them for illegal or immoral purposes, which includes but is not limited to:
    - threaten, discriminate or harass others
    - make fraudulent offers of products, items, or services
    - forge message headers, in part or whole, of any electronic transmission
    - distribute viruses, malware or spam mail
    - impersonate, misrepresent or obtain the identity of another party
    - the use of trademarks, high-profile names and domain names of another party
    - publish discriminating material
- Use the certificates for the permitted Key Usage and Extended Key Usage only. Never sign with an end-entity certificate other certificates.
- Obtain and use the keys and certificates only for the intended purpose as defined in this policy, e.g. according to "Types and Classes of digital X.509 Certificates" of this policy.

- Never obtain and use a certificate that belongs to a different entity other than the entity referenced in the certificate and the entity that has been validated, e.g. a validated individual may obtain certificates for domain names he/she owns, but not for other individuals or organization, even if allegedly authorized or requested. Likewise a validated organization shall not obtain a certificate for a domain belonging to another entity or third party.
- Never obtain and use a certificate to operate nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system requiring fail-safe operation whose failure could lead to injury, death or environmental damage.
- Reimburse StartCom and pay related fees to StartCom for its services whenever they apply and without unnecessary delay.
- Defend, indemnify, save and hold StartCom, its directors, officers, agents, employees, contractors, affiliates or subsidiaries (collectively, the 'Indemnified Parties') harmless from any demands, liabilities, losses, costs and claims.
- Accept this policy, its terms, conditions and applicable obligations.

[Add at Security - CA Public Key Delivery to Subscribers:]

The public root CA keys are published at the following repository:

- http://www.startssl.com/certs/ca.cer (DER encoded - SHA1)
- http://www.startssl.com/certs/ca.pem (PEM encoded – SHA1)
- http://www.startssl.com/certs/ca-sha2.cer (DER encoded – SHA2)
- http://www.startssl.com/certs/ca-sha2.pem (PEM encoded – SHA2)
- http://www.startssl.com/certs/ca-g2.cer (DER encoded – SHA2)
- http://www.startssl.com/certs/ca-g2.pem (PEM encoded - SHA2)

[Add at Security - Validations – Class 1 – Domain Names:]

Remove “Likewise multiple domain names within the same certificate are not supported in the Class 1 settings” and add “Multiple domains and sub domains may be supported provided they don't include keywords such as “shop”, “credit”, “finance”, “bank” that might suggest commercial purpose, likewise any high-profile brand and name should be avoided.

[Insert at Security - Validations – Class 2 - Organization:]

The subscriber has to provide in a secure and reliable fashion supporting documentation *which must be either from a Qualified Government*

Information Source, Qualified Government Tax Information Source or Qualified Independent Information Source.

[Add at Security - Validations – Class 2 - Organization:]

StartCom confirms and verifies that the subscriber is duly authorized to represent the organization and obtain the certificates on their behalf by obtaining an authorization statement and by contacting the authorizer. The obtained and confirmed organization documents should state the authorizer and position, but StartCom may rely on other means and sources to obtain the necessary authority if necessary. StartCom may assume proper authorization in case the validated subscriber is either the appointed CEO, Director, President or owner and sole proprietor.

[Add at Certificate Profiles – Naming conventions:]

Class 1

Client Authentication and S/MIME certificates

The fields common name (CN) and organization (O) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 these fields MUST be omitted.

SSL/TLS server certificates

The fields organization (O) and organizational unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 these fields MUST be omitted.

Class 1 + Web-of-Trust Community Validated

Client Authentication and S/MIME certificates

The organization (O) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

SSL/TLS server certificates

The organization unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

Start Commercial (StartCom) Limited

StartSSL™ Certificates & Public Key Infrastructure

Eilat, Israel

Class 2

Client Authentication and S/MIME certificates

The organization (O) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

SSL/TLS server certificates

The organization unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

Object Code Signing certificates

The organization unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

Class 3

Client Authentication and S/MIME certificates

The organization (O) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

SSL/TLS server certificates

The organization unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

Object Code Signing certificates

The organization unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

Extended Validation

SSL/TLS server certificates

The organization unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted.

Other Certificate Attributes

Code Signing Certificates:

Under Extended Key Usage, the Lifetime Signing OID MAY be omitted. For

subscribers with valid and current Extended Validations the Kernel Mode EKU 1.3.6.1.4.1.311.61.1.1 MAY be included in the EKU.

Change Basic Constraint to CA:FALSE

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:	Mon Jan 30 02:53:14 IST 2012
	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.