# Start Commercial (StartCom) Limited

**StartSSL™ Certificates & Public Key Infrastructure**

**Eilat, Israel**

# Addendum to the StartCom Certification Authority Policy & Practice Statements

Version: 1.0
Status: Final/Approved
Updated: 28/12/08

Author: Eddy Nigg

## Purpose of this Document

The purpose of this Addendum to the Policy & Practice Statements is to amend version 2.0 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 Obligations:]***

## Registration Authority Obligations

StartCom does not maintain registration authorities.

***[Add after Compliance Audit:]***

## COMPLIANCE IMPROVEMENT

Upon detection of deficiencies and possible weaknesses of the CA infrastructure and/or established procedures as a result of internal or external auditing or in case of non-compliance thereof, the StartCom CA shall take corrective measures and actions in order to correct deficiencies and ensure future compliance within a reasonable time-frame. StartCom shall record, approve and report any corrective action steps taken and/or action steps that are anticipated to correct the non-compliant areas. The annual audit shall confirm the improvements and corrective measures taken.

***[Add at Physical Infrastructure:]***

*Data shall be backed up daily in a rolling and increasing mode, including critical system data or any other sensitive information, like personal data and event log files.* Archives and other materials of critical system data important for recovery in case of a disaster are stored in a secure manner at a off-line facility beyond 150 miles of the StartCom CA infrastructure. Recovery of the CA infrastructure and/or relocation plans are maintained and shall be possible within 48 hours in case of a disaster.

***[Add at section Notifications:]***

## Certificate Issuance

Notification of issuance of a certificate to others than the subscriber and subject of the certificate are generally not performed. Issuance and delivery of a certificate is part of the procedures for obtaining a certificate by the subscriber.

***[Add to Subscriber Private Key and Certificate Usage:]***

Renewing a certificate follows the same procedures as with a new certificate. Re-keying or reusing the same private key for any new or renewed certificate shall be avoided by the subscriber.

***[Add to Subscriber Private Key Generation and Delivery:]***

Subscribers may use smart cards, hardware tokens or integrated circuit card for the storing of private keys. The StartCom CA does not deliver certificates on such devices however.

*The StartCom CA checks the submitted keys for known vulnerabilities and eventual weak randomness.* Private keys generated by the StartCom CA or by the subscriber shall have adequate key sizes and signature algorithms deemed secure at the time of creation in order to provide sufficient protection.

***[Add after Revocation:]***

## Suspension

Certificates issued to subscriber may be either valid, expired or revoked. The StartCom CA does not perform certificate suspension and subscribers are advised to request a new certificate in case of expiration or revocation of previously valid certificates.

This document is signed by:

| | | |
|---|---|---|
|  | Signator: | EMAILADDRESS=certmaster@startcom.org, CN=Eddy Nigg, OU=StartCom Trusted Certificate Member, O=StartCom Ltd., L=Eilat, ST=South, C=IL |
| | Date: | Wed Feb 11 17:09:28 IST 2009 |
| | Issuer: | CN=StartCom Class 3 Primary Intermediate Client CA, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL |
| | Serial: | 56 |

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.