

StartCom Certification Authority

Intermediate Certification Authority Policy Appendix

Version: 1.4
Status: Final
Updated: 07/18/08
Copyright: Start Commercial (StartCom) Ltd.
Author: Eddy Nigg

Introduction

This document describes the policies and practices of the StartCom CA governing Intermediate Certification Authorities not directly operated by the StartCom CA but under supervision of the StartCom CA.

According to the StartCom Certification Authority Policy & Practice Statements, the StartCom Certification Authority, hereby called and referred to as the StartCom CA, may empower organizations to act as a limited intermediate certification authority. This document outlines the regulations, terms and conditions concerning Intermediate Certification Authorities not directly operated by StartCom, hereby called and referred to as an ICA.

Copyright, Reserved Rights

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.

Intermediate Certification Authority (ICA)

Organizations and Institutions may need to establish their own certification authority within their organization for various reasons.

The StartCom CA may empower such entities with the ability to run their own dedicated certification authority by providing a web based solution for the issuing subscriber certificates according to the regulations outlined in this document.

Organizations wishing to operate an external intermediate CA enter into a contractual relationship with the StartCom CA and must commit to all requirements of the StartCom CA policies, including the lowest validation levels, physical and operational standards and practices. Many times the capabilities of the intermediate CA are limited in scope and size. Subordinated CAs may however implement more restrictive practices and validation procedures based on their own requirements.

Organizations may also request to have their already operational and/or a newly created self-signed CA root cross-signed by the StartCom CA and transfer overall responsibility to the StartCom CA. The StartCom CA will act as caretaker for such CA roots and incubate the root into the Intermediate CA Program. All requirements of the ICA Program shall apply as if the CA root is an intermediate CA certificate issued by and under the StartCom hierarchy.

Benefits

StartCom works to enable native support and for the embedding of the StartCom CA root certificate in major applications and operating systems and therefore offers better compatibility and integration into the organization's existing systems.

The StartCom CA provides to the organization a complete Internet based on-line solution for the signing and managing of subscriber certificates. The organization may be empowered to issue digital certificates to the general public through Internet facing public interfaces which allows for an easy and customized integration into the organization's web site or portal.

Acceptance

Acceptance is at the sole discretion of the StartCom CA and every request is evaluated on a case to case basis. The StartCom CA is not required to provide any reasons for accepting or rejecting an application. The criteria considered by the StartCom CA in making its decisions includes but is not limited to:

- The obvious and reasonable need to run an ICA
- Establishment, trustworthiness and reputation
- Experience in PKI and other related requirements
- Ability to adhere to the obligations, requirements and conditions of the StartCom CA

Privacy

StartCom fully respects the privacy of any applicant for an ICA prior to their acceptance. Therefore the StartCom CA will refrain from providing information about inquiries and requests for operating an ICA to third parties. Related information the StartCom CA may have received will be kept confidential. Any documents obtained physically, will be returned to the owner in the case such a request has been denied. Other information, except trivial ones, such as organization name, addresses and contact details shall be destroyed at the end of the application process in case such a request has been denied. Electronic communication between the applicant and the StartCom CA shall be via signed and encrypted electronic mail messages.

Approved applicants agree to have details like organization name, incorporation, address, locality, purpose, limitations and signer certificate of the intermediate CA published and made available to third parties.

The StartCom CA keeps all documents and other supporting materials it receives from the applicant, confidential, such as letters of incorporation, information about ownership, personal information about owners, personal details about the executive officers. The applicant keeps insider or any other information it receives from the StartCom CA confidential, except if ordered to do so by law. The StartCom CA shall be notified immediately of such circumstance. Providing any information about the StartCom CA or its subscribers and/or about subscribers of the operating ICA to third parties will be viewed as a gross violation of this policy and may have legal consequences and will result in the immediate suspension of the ICA.

Limitations

An ICA may be limited in scope and purpose; any such limitations are decided on a case to case basis.

There are two types of external ICA certificates:

- Class 1 Server certificates
- Class 1 Client Authentication & S/MIME certificates

The ICA operations may be limited to issuing of only client or only server certificates and/or only for certain domain name(s) and/or only within a certain scope of their organization / members / customers and/or any other limitation the StartCom CA deems necessary.

An ICA must use the web based and protected interfaces provided by the StartCom CA for the requesting, issuing and revoking of subscriber certificates. The ICA may integrate the solution provided by the StartCom CA into the organization's web site or portal. Under no circumstances is the organization capable of implementing its own web based distribution of certificates. Under no circumstances is the organization in the possession of the private key of the intermediate CA certificate.

Certificates signed by an ICA may not be sold exclusively, but may be offered as a extended service of the organization's products, subscriptions etc. In that case, the certificate shall not be the primary focus of the product, subscription or service

offered by the organization.

Non compliance with the limitations will result in the immediate suspension of the ICA.

Liability

The organization operating the ICA shall be liable for gross negligence and intent. The ICA operations are automatically covered by the StartCom CAs insurance policy.

Fees

Fees are subject to changes and part of the contractual agreements between the StartCom CA and the organization operating the ICA. Changes to fees take effect 90 days after notification.

Obligations

- Accept certification requests from entitled entities
- Issue certificates based on requests from authenticated entities
- Accept revocation requests according to the CA policy
- Inform the the StartCom CA of revocation requests
- Provide details of issued certificates to the StartCom CA
- Protect private and individual data obtained
- Maintain the highest security standards possible
- Accept the requirements and conditions of the StartCom CA
- Accept the philosophy as outlined in the CA policy
- Defend, indemnify, save and hold StartCom harmless from any demands, liabilities, losses, costs and claims.

Security

Physical

The ICA is exclusively hosted and served from the designated infrastructure at StartCom's premises. Handling of the ICA private keys, archival, retrieval and storing at HSM thereof is strictly and exclusively handled by the StartCom CA. Interaction for the requesting, signing and revoking of certificates is handled exclusive via the web interfaces and solutions StartCom provides to the organization.

The administrative interfaces for the managing of the ICA are protected with client certificates and access shall be limited to the certification master of the organization. The responsible certification master should have basic knowledge about PKI and about the related functions.

Technical

All other aspects are covered by the StartCom CA Policy & Practice Statements, section "Security".

Certification Rules

Validations

The StartCom CA may assist the organization operating the ICA to process server and client certificates in bulk mode after verifying the accuracy of the validations performed by the ICA operator. The ICA certification master verifies without any reasonable doubt that the following details are correct:

- The domain name or IP address belongs to the requesting party
- The email address belongs to the requesting party

All other validations are handled via the designated interfaces provided by the StartCom CA and according to the Class 1 validation requirements of the StartCom CA Policy & Practice Statements, section "Certification Rules".

Termination

The ICA agreement may be terminated under the following circumstances:

- The ICA terminates the agreement with the StartCom CA
- The StartCom CA terminates the agreement with the ICA
- The ICA has failed to comply with the rules of this and of the StartCom CA Policy & Practice Statements
- The ICA violated his/her obligations
- The ICAs private key is suspected to be compromised
- The ICA ends its life cycle (5 years, for self-signed CA roots not applicable)

A new intermediate certificate shall be issued one year (365 days) prior to expiry of the current intermediate certificate. The new certificate shall be valid for another 5 years and be replaced again one year before expiry and so on. Intermediate CA certificates are rolled over every four years.

In case the intermediate CA certificate represents a self-signed root certificate and is cross-signed by the StartCom CA root, the CA certificate may be valid for longer periods and roll-over does not apply. The root certificate shall be decommissioned after expiration.

In case of agreement termination, each party must notify each the other 90 days prior to the date of termination. The ICA continues to provide its services until the

90th day after the notification. The intermediate certificate shall be revoked after the expiry of the last signed certificate or after 365 days. In case the ICA certificate represents a self-signed root certificate, the root and its private key may be transferred to the organization after the cross-signature has been revoked. All responsibilities of the CA shall be transferred to the organization thereafter.

The ICA shall store and archive all material it received from subscribers for the next 7 years. Alternatively the ICA may send all obtained material to the StartCom CA for archival. After that period all material shall be destroyed.

In the case of violation or non compliance, the ICA shall be notified about the decision and after a reasonable time (24 hours), sufficient for a response and acknowledgment, the intermediate certificate shall be revoked. In this case, the StartCom CA continues to act on behalf of the ICA and overtakes all responsibilities, especially certificate revocation. The StartCom CA will not issue new certificates on behalf of the ICA.

Upon request, the organization operating the ICA shall provide all material received from its subscribers to the StartCom CA, or hand it over to a trusted third party which has been agreed upon by both sides. Under no circumstances shall the material be destroyed. The material shall be archived and stored for 7 years and destroyed in appropriate manner thereafter. The ICA must pay the fees for the next 90 days after revocation. The ICA shall also pay any costs related to the storing of the archived material.

Governing Law

Any party involved shall try to resolve all disputes that might arise in a spirit of cooperation without formal procedures. Any legal dispute which cannot be resolved shall take place in Eilat, Israel or at a different location if the parties agree so or are ordered to do so by law. Interpretation and legal disputes arising from the operation of the ICA will be treated according to Israeli laws.


If any term of this policy should be invalid under applicable laws, this term should be replaced by the closest match according to applicable laws and the validity of the other terms should not be affected.

Glossary

Acronyms

ANSI	The American National Standards Institute
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
EV	Extended Validation
FIPS	United States Federal Information Processing Standards
HTTP	Hyper Text Transfer Protocol
ICA	Intermediate Certification Authority
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	On-line Certificate Status Protocol
OID	International Standards Organization's Object Identifier
PCA	Primary Certification Authority
PIN	Personal identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
SGC	Server Gated Cryptography
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	ITU-T standard for 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 Dec 17 23:57:43 IST 2008
	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.