

StartCom Certification Authority

Extended Validation Certificates Policy Appendix

Version: 1.0
Status: Final/Approved
Updated: 04/23/09
Copyright: Start Commercial (StartCom) Ltd.
Author: Eddy Nigg

Introduction

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.

According to the "*StartCom Certification Authority Policy & Practice Statements*", 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 Certification Authority Policy & Practice Statements*" about aspects which are not already explicit or inexplicit covered by the "*StartCom Certification Authority Policy & Practice Statements*" 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.

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.

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.

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.

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 so on a case to case basis.

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.

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 EV 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*”. 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 EV Guidelines.

Information Verification Requirements


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.

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: | Thu Apr 23 12:24:58 IDT 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.