StartCom Certification Authority

Policy & Practice Statements

Version: 2.0
Status: Final
Updated: 07/18/08

Author: Eddy Nigg

Introduction

This document describes the Certification Policy (CP) of StartCom Certification Authority and related Certification Practice Statements (CPS):

This document, "*StartCom Certification Authority Policy and Practice Statements*", is the principal statement of policy governing the **StartCom Certification Authority**, hereby called and referred to as the StartCom CA. The Certification Policy (CP) sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing digital certificates.

The related Certification Practice Statements (CPS) states the practices that the StartCom CA employs for the secure managing of the CA public key infrastructure and the issuing, managing, revoking and renewing of digital certificates in accordance with the specific requirements of this Certification Policy.

Many times the policy set forth in this document is also the practice employed by the StartCom CA and therefore presented together in this document. Whenever needed, the certification policy is followed by the related practice statement.

StartCom maintains the StartCom Certification Authority as a service to the Internet community. StartCom is committed to and supports the free flow of information and ideas over the Internet. The StartCom CA is an instance for the issuing of digital certificates in order to secure websites, encrypt and secure critical and sensitive data during exposure at network based electronic data transfers, digitally sign object code or other content, digitally sign and encrypt documents and email messages.

As such, the StartCom CA provides to its subscribers digital certificates for public and private Internet web servers, personal certificates for electronic mail and documents and object code base (executable objects) for the reliance and benefit of third parties.

Depending on the class and type of certificate, digital certificates may be used by subscribers to secure websites, digitally sign code or other content, and digitally sign documents and email messages.

The StartCom Certification Authority

Address:

Start Commercial (StartCom) Ltd.
P.O. Box 1630
88000 Eilat
Israel

Internet:

StartCom Ltd:	http://www.startcom.org/
StartCom CA:	http://www.startssl.com/
IANA assigned OID:	1.3.6.1.4.1.23223

Email:

StartCom CA:	certmaster@startcom.org
Support:	support@startcom.org
Abuse:	abuse@startcom.org
Website:	webmaster@startcom.org

Phone:

General USA: +1.213.341.0390

Chief Executive Officer:

Nigg Revital
Email: revital@startcom.org
Phone: +972.57.631.5630

Chief Operations and Technical Officer:

Nigg Eddy
Email: eddy_nigg@startcom.org
Phone: +972.57.631.5629

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.

Philosophy

StartCom provides and operates various computer software and Internet related products and services, including the maintaining and operating of the StartCom Certification Authority. StartCom has extensive knowledge and experience in Public Key Infrastructures, IT management, software programming and more. StartCom is also actively involved at various the open source code and open standards projects and stands for the free flow of information and innovation.

StartCom believes in the basic right to protect and secure information between two entities without discrimination of race , origin or religion. StartCom further believes that this right should not be bound to the financial capabilities of individuals, institutions, companies, or organizations whenever possible. StartCom aims to provide during the operation of the StartCom CA viable alternatives compared to other commercial certification authorities and providers, without discrimination, limits or reduced values at any given time and whenever possible.

StartCom reserves the right to offer free (without costs) and fee based services and products through the StartCom CA at any given time.

Subscribers

Subscribers are all end users of certificates issued by an issuing certification authority. A subscriber is the entity named as the end user subscriber of a digital certificate. Subscribers may be individuals, organizations or infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an organization. In most cases certificates are issued directly to individuals or entities for their own and direct use. The subscriber is the person to whom the credential is legally bound.

Relying Parties

A relying party is an individual or entity that acts in reliance of a certificate and/or of a digital signature issued under the StartCom CA. A relying party may or may not also be a subscriber of the StartCom CA. Naturally the person who ultimately receives a signed document or communication, or accesses a secured website is referred to as the “Relying Party”, e.g. he/she is relying on the certificate and has to make a decision on whether to trust it.

Types and Classes of digital X.509 Certificates

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates. The StartCom CA acts as root CA for a set of subordinated issuers called Intermediate Certification Authorities (ICA). Each ICA is responsible for a specific class (level) of subscriber certificates, such as the classes 1 through 3 and extended validation (EV) certificates. The ICAs are further separated by their end-user purpose and key usage, such as 1.) web server (SSL), 2.) email (S/MIME), document and authentication, 3.) object code signing.

The StartCom CA operates its own set of intermediate CA certificates and may also issue and sign subordinated CA issuer certificates to third parties, according and as outlined in the section for third party intermediate certification authorities.

The StartCom CA may introduce and issue additional root and/or intermediate CA certificates at any given time by complying and maintaining the basic requirements of the this policy and lowest validation level (Class 1). The StartCom CA may cross-sign new CA root certificates it issues and/or cross-sign intermediate CA certificates which may be also root certificates. If needed and appropriate, additional policies may be published without replacing, reducing, devaluing or changing the lowest validation requirements and basic terms set forth by this policy.

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. Subordinated CAs may however implement more restrictive practices based on their own requirements. Internal to StartCom, external, cross-signed or subordinated CA must adhere at least to the validation requirements of Class 1 as set forth in this policy.

Certificate Types

1. **Client Certificates** are typically used for authentication purpose, signing and encryption of electronic mail and digital documents. They are also referred as S/MIME certificates and may be used for all purposes mentioned above or only for individual usage depending on the key usage limitations found in the certificate.
2. **SSL/TLS Server Certificates** are typically used by server software for the identification of the server operator and the encrypting of sensitive information during its exposure at the networks.
3. **Object Code Signing Certificates** are typically used to sign software objects, macros, device drivers, firmware images, virus updates, configuration files or mobile applications.
4. **Intermediate CA Certificates** are used exclusively for the issuing and signing of end user certificates and certificate revocation lists. Each CA certificate is responsible for the signing of a different Class and end purpose.
5. **CA Root Certificate** is used to exclusively sign and issue the intermediate CA certificates and corresponding certificate revocation

list.

Certificate Classes

1. **Class 1 Certificates** provide modest assurances that the email originated from a sender with the specified email address or that the domain address belongs to the respective server address. These certificates provide no proof of the identity of the subscriber or of the organization. Class 1 certificates are limited to client and server types, whereas the later is restricted in its usage.
2. **Class 2 Certificates** provide medium assurances about the subscribers identity and subscribers of Class 2 certificates have to prove their identity by various means. Organizations are required to designate a responsible person which is at least Class 2 identity validated prior to engagement for organization validation. Organizations have to prove their incorporation by various means.
3. **Class 3 Certificates** provide a high level of assurance about the subscribers identity in comparison with Class 1 and 2 certificates and are issued only to organizations and individuals to which the StartCom CA has a relationship or are known to the StartCom CA by means of face-to-face verification. This includes typically employees, investors, business partners and operators of intermediate CAs.
4. **Extended Validation (EV) Certificates** implements the validation procedures and requirements of the Extended Validation Guidelines as published by the CA/Browser Forum. EV extends Class 2 validation and organizations are required to designate a responsible person which is at least Class 2 identity validated prior to any engagement for extended validation.

CA Structure

Below is a simple graph outlining the hierarchy of the SFSCA, showing the Root CA

followed by a few classes of the ICA's used be the SFSCA and one external authorized

ICA.

StartCom CA Root

|_____

| Intermediate Class 1 Server CA

| |

| End User Class1 Server Certificates

|_____

| Intermediate Class 1 Client CA

| |

| End User Class 1 Client Certificates

|_____

| Intermediate Class 2 Server CA

| |

| End User Class 2 Server Certificates

< cut >

|_____

External Class 1 Server CA

|

End User Class 1 Certificates

Obligations

CA Obligations

- Accept certification requests from entitled entities
- Issue certificates based on requests from authenticated entities

- Issue intermediate authority certificates to entitled entities
- Notify subscribers of certificate issuance
- Accept revocation requests according to this document
- Issue Certificate Revocation Lists (CRL)
- Publish the CRL's issued
- Provide OCSP service
- Inform subscriber of certificate revocation
- Keep audit logs of the certificate issuance process
- Protect private and individual data obtained
- Maintain best security standards possible

Intermediate CA Obligations

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

Subscriber Obligations

- Generate a key pair using a trustworthy method
- Selecting an adequately secure pass phrase
- Protecting the pass phrase from others
- Never share the private key with others
- Protect the private key properly

- Provide correct personal information
- Notify the StartCom CA immediately in case of private key loss or compromise
- Use the certificates for the permitted uses only
- Use the from the StartCom CA issued certificates in accordance with all applicable laws and not to use them for illegal or immoral purposes, which includes but is not limited to:
  - threaten, discriminate or harass other individuals and entities
  - make fraudulent offers of products, items, or services
  - forge message headers, in part or whole, of any electronic transmission
  - distribute viruses
  - obtain the identity of other individuals or entities
  - publish discriminating material
  - use it for any unlawful activities
- Accept the requirements and conditions of the StartCom CA
- Defend, indemnify, save and hold StartCom harmless from any demands, liabilities, losses, costs and claims.

Relying Party Obligations

- Read the procedures published in this document
- Use the certificates for the permitted uses only
- Not assume any authorization attributes based solely on an entity's possession of a StartCom CA issued certificate
- Should verify the certificate against the revocation list (CRL) and/or OCSP responder, check against expiry time, certificate chain, the validity check of the certificates in the chain and the identification of the domain and email.

Legal and Limitations

Liability

StartCom gives no guaranties whatsoever about the security or suitability of the services provided that are identified by a certificate issued by the StartCom CA or the use of thereof, including but not limited to the use of its websites and programs or any other service offered currently or in the future. The certification services are operated according to the highest possible

levels of security and to the highest industry standards, but without any warranty.

Relying parties have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a certificate, and as such are solely responsible for deciding whether or not to rely on such information, and therefore shall bear the legal consequences of their failure to perform the Relying Party Obligations outlined in this policy.

Under no circumstances, including negligence, shall StartCom or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this or other services, even if advised of the possibility of such damage.

Financial Responsibility

StartCom's operations related to the issuing of regular digital certificates (Classes 1 through 3) shall be covered by a Professional Liability Insurance Policy in order to guarantee continued operation of the CA. For every 50,000 issued and valid certificates at any given time, the coverage of the policy shall be one million New Israeli Shekels (NIS) and increased as needed. Valid certificates includes all subscriber certificates issued by any issuing CA certificate, including externally operating CAs, which have not been expired or revoked. The current Insurance Policy covers 1,000,000 NIS (US$ ~300,000) and up to US$ 10,000 per certificate.

Beyond the coverage of the insurance policy above, StartCom denies any responsibility for damages or impairments resulting from its operation and assumes no financial responsibility with respect of the use of any issued certificate or provided service.

Certificates issued in accordance to the Extended Validation Guidelines shall be treated according to those guidelines as published by the CA/Browser Forum in respect to liability and insurance policy requirements. StartCom shall adhere to those requirements only for certificates explicitly marked as EV certificates and which where issued according to the EV guidelines.

Copyright and Ownership of Certificates

Digital certificates which are the result of the operations of the StartCom CA, are at any given time and remain during their whole life-time the property of the StartCom CA. Ownership of digital certificates issued by and through the operations of the StartCom CA can't be claimed by subscribers, relying parties, software vendors or any other party. Issuance of a certificate to the end user gives the subscriber the right to use the issued certificate(s), subjected to the requirements and obligations set forth in this policy, acceptance of the terms and conditions of the StartCom CA as published on

the related web site(s) and to the extent of the key usage and extended key usage fields of the certificate, until expiration or revocation of the certificate, whichever comes first. StartCom exclusively retains the copyright of all certificates produced, created, published and issued by the StartCom CA at all times and all rights are reserved.

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 without formal procedures shall take place in Eilat, Israel or at a different location if the parties agree or are ordered to do so by law. Interpretation of legal disputes arising from the operation of StartCom CA shall be treated according to the Israeli legal system and laws.

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

Disputes arising in relation to certificates issued according to the Extended Validation Guidelines as published by the CA/Browser Forum shall be treated according those guidelines and only to the extend and scope set forth by those guidelines. This may include different interpretation of applicable laws and the locality of jurisdiction. The parties may however agree to solve disputes under different applicable laws and jurisdiction.

Fees

StartCom and the StartCom CA provide a wide range of services and products, some of which carry a fee and some of which are exempted from any payment. Exempted from any fees are currently all Class 1 certificates and revocations of all certificates without relation to the class level or type, but also other related products and services.

StartCom publishes clearly at the relevant web sites and other medium which services and products carry a fee and which are exempt from payments. StartCom notifies subscribers and customers about impending charges. Except as otherwise expressly provided for herein, all payments made to StartCom are non-refundable.

StartCom and the StartCom CA reserves its rights to add, remove, suspend and change any service and product in part or in full and retains its rights to affect changes to any related fees at any given time and without prior notice. Fees charged for services and products provided by StartCom and the StartCom CA are subject to changes and at the sole discretion of StartCom and the StartCom CA.

Privacy

StartCom respects the privacy of individuals and entities and shall not disclose personal details of certificate applicants or other identifying information it retains from and about them to third parties.

Any information about subscribers that is not publicly available through the content of the issued certificate, certificate directory and certificate revocation lists, shall be treated as private and regarded as protected information. Obtained private details and informations shall not be used without the consent of the party to whom that information applies beyond the tasks the StartCom CA has to perform for successful validation and verification purpose. The StartCom CA shall save and secure subscriber information it retains from compromise and disclosure to third parties and shall comply with applicable local privacy laws for the protection of such information. If disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents, the StartCom CA shall be entitled to disclose private information to law officials without penalty.

The StartCom CA may register its databases with local authorities for holders of databases with more than 10,000 individual names as suggested by applicable local legislation.

Archival of Records

StartCom retains the records of the from the StartCom CA issued certificates and the associated documentation for no less than 7 years. The retention term begins on the date of expiration or revocation. Copies of certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that StartCom may see fit.

Such records are archived and maintained in a form that prevents unauthorized modification, substitution or destruction.

Notifications

Subscriber Private Key and Certificate Usage

By accepting a certificate from the StartCom CA, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this CP and the relevant CP statements. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

Subscribers are notified hereby that electronic signatures can be legally binding. The extent to which they are trusted depends on local legislation. That means that legislation will decide on a case by case base whether or not they are legally binding. Because of these legal implications, subscribers must protect their private keys.

Digital encryption is not meant to be recovered without the private key. If the private key is lost, encrypted data may be lost and cannot be recovered. The StartCom CA does not keep any private keys except its own.

Relying Party Public Key and Certificate Usage

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, relying parties shall independently assess:

- That the certificate is being used in accordance with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the end entity certificate and all the CA certificates in the chain that issued the certificate. If any of the certificates in the certificate chain have been revoked, the relying party shall not rely on the end user certificate or other revoked certificates in the certificate chain.

Compliance Audit

The practices specified in this CA policy & practice statements have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework,

and other industry standards related to the operation of CAs. An annual audit is or will be performed by an independent external auditor to assess the StartCom CAs compliance with the AICPA/CICA WebTrust program for Certification Authorities. Topics covered by the annual audit include but are not limited to the following:

- CA business practices disclosure
- Service integrity
- CA environmental controls

Change Management

The StartCom CA policy is subject to changes and it is the responsibility of the subscribers and relaying party's to review the policy from time to time. All changes, if at all, including the CA policy itself are published at the designated web site for the CA operations. Subscribers and relaying parties will not be notified of impending changes of the policy. The policy is legally binding from the moment of its publication.

Subscriber certificates for the Classes 1 through 3 include an policy identifier whose root OID is 1.3.6.1.4.1.23223.1.X.X, where "X.X" represents the policy version the identifier is referring to. Changes to the policy requires increasing of the policy version number by one. Extended Validation certificates include a policy identifier whose OID is 1.3.6.1.4.1.23223.2.

StartCom shall continue its CA operations for one year (365 days) in case of the termination of the StartCom CA, excluding issuance of new subscriber certificates. All remaining certificates still valid after the one year extension period shall be revoked on the last day and included in the corresponding certificate revocation list.

Intermediate Certification Authorities not directly operated by the StartCom CA shall be notified of impending changes, including termination, three months (90 days) before the changes will take effect and before officially published.

The regulations for terminating Intermediate CA's are outlined in the StartCom Intermediate Certification Authority Policy Appendix.

Security

Physical Infrastructure

The StartCom CA operates a tightly controlled and restricted PKI infrastructure at its Headquarters in Eilat, Israel. The infrastructure is comprised of physical boundaries, computer hardware, software and procedures that provide an acceptable resilience against security risks and provide a reasonable level of availability, reliability and correct operation and the enforcing of a security policy.

The hardware is located in a dedicated, resistant server room. Access to the

facility by individuals (personnel and others) is strictly controlled and restricted to authorized and trusted personnel only. Maintenance and other services applied to the cryptographic devices and server systems must be authorized by the CEO or COO of StartCom. Physical access to the server infrastructure and facilities shall be logged and signed by at least one other witness on the four eyes principal. Otherwise physical access to the systems shall be avoided.

Besides the attached hardware security modules, no removable media or devices shall be accessible or in existents at the operating on-line CA server systems. Maintenance operations, changes, modifications or removal of devices or hardware components of the CA server systems are strictly restricted and must be authorized by the CEO or COO of StartCom. Any removed device which may contain data (like hard drives) must be wiped out of any data before disposal.

The hardware and software shall be protected and constantly monitored by authorized service personnel for intrusion and compromise. Various programs and tools shall assist in this task. Hardware equipment and operating systems shall be maintained at the highest possible level of security.

The locality shall be fully air conditioned, provide electricity power backup (UPS) and shall be supported by an external, independent electricity power source for cases of prolonged power outages.

Fire alarm and prevention equipment shall be installed and available at the premise.

The server room shall be monitored by a closed-circuit camera and television monitoring system with recording capabilities and records shall be archived in a rolling and increasing mode.

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.

The StartCom CA shall implement procedures for the disposal of waste (paper, media, or any other waste) in order to prevent the unauthorized use of, or access to, or disclosure of waste containing confidential information.

CA Key Generation, Protection, Recovery & Publication

Key pair generation shall be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

The StartCom CA root is an off-line CA and shall be used only for the signing of Intermediate CA certificates and the relevant Certificate Revocation Lists. For key generation and other signing procedures by the CA root, a strictly off-line system shall be used. The resulting private and public keys and certificate revocation lists shall be stored in removable devices and/or security modules according to the defined procedures.

The private CA root key shall be stored in encrypted form in safety vaults, divided into two external media devices and stored at two different locations and protected by a pass phrase. Only both external devices may recreate the private CA root key, which is needed for signing actions such as issuance of Intermediate CA certificates and Certificate Revocation Lists.

The signing of Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer of StartCom.

The private keys of the Intermediate CA certificates shall be stored in Hardware Security Modules (HSM) , suitable for the signing of Subscriber Certificates and the on-line Certificate Revocation Lists.

The signing of subscriber certificates is strictly and only performed by the Intermediate CA keys which are operating at the on-line equipment.

The Intermediate CA certificates are structured per class and per purpose:

- SSL/TLS Server Certificates
- S/MIME Client Certificates
- Object Code Signing Certificates

and

- Classes 1 through 3
- Extended Validation

Each Intermediate CA issues an OCSP signer certificate for the OCSP responder service.

CA Root Public Key Delivery to Subscribers

The public root CA key is published from the following repository:

- http://www.startssl.com/certs/ca.crt (PEM encoded)
- http://www.startssl.com/certs/ca.cer (DER encoded)

The public root CA key shall be embedded within popular software applications, making special root distribution mechanisms unnecessary.

Intermediate CA public keys are published and distributed via Internet from the following repository:

- http://www.startssl.com/certs/

All public CA keys of the StartCom CA may be downloaded via secured and encrypted protocols (SSL).

Distribution of Intermediate CA public keys to relaying parties is generally unnecessary, provided that the public CA root key is installed in the software used by the relying party.

Digital Certificate Management

The StartCom CA certificate management refers to functions that include but are not limited to the following:

- Verification of the relevant attributes for certificates.
- Authorizing the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- De-commissioning of the corresponding private keys through expiration or revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.
- Storing certificates.
- Retrieving certificates in accordance with their particular intended use.

The StartCom CA conducts the overall certification management within the StartCom CA PKI directly or through approved intermediate CA operators.

Subscriber Private Key Generation and Delivery

The StartCom CA offers the creation of key pairs and certificate signing requests (CSR) for server certificates through the CA system. The private key is delivered encrypted and protected by a pass phrase via SSL secured connection to the subscriber. The private key generation utility employs a Real Hardware Random Number Generator for the seeding of the entropy. The use of the private key generation utility at the StartCom CA web site is at the sole risk of the subscriber. The StartCom CA doesn't keep any private keys and pass phrases/passwords and any such information is deleted and/or overwritten if necessary.

Subscribers may produce and prepare their own private keys and certificate signing requests (CSR) for server certificates and submit them via SSL secured connection to CA system. In this case, private key delivery to the subscriber is unnecessary. The StartCom CA checks the submitted keys for known vulnerabilities and eventual weak randomness.

Client S/MIME and Object Code Signing keys are always generated at the client side via appropriate browser functions. In this case, private key delivery to the subscriber is unnecessary.

Certification Rules

Validations

The StartCom CA performs the following validations and verifications according to the following rules:

Class 1

- **Email Addresses**

  Email accounts are validated by sending an electronic mail message with a verification code to the email account in question. The subscriber has to return and submit the verification code as prove of ownership of the email account within a limited period sufficient enough to receive an electronic mail message.

  The validation may be valid for 30 days for the generation of digital certificates.

- **Domain Names**

  Fully qualified domain names, typically “www.domain.com” or “domain.com” are validated by sending an electronic mail message with a verification code to one of the following administrative electronic mail accounts:

  - webmaster@domain.com
  - hostmaster@domain.com
  - postmaster@domain.com

  The subscriber has to return and submit the verification code as prove of ownership of the domain name within a limited period sufficient enough to receive an electronic mail message.

  Additionally the existence of the domain name is verified by checking the WHOIS records provided by the domain name registrar. If the WHOIS data contain additional email addresses, they may be offered as additional choices to the above mentioned electronic mail accounts.

  The StartCom CA performs additional sanity and fraud prevention checks in order to limit accidental issuing of certificates whose domain names might be misleading and/or might be used to perform an act of fraud, identity theft or infringement of trademarks.

  Wild card domain names like “*.domain.com” are only issued to Class 2 or higher validated subscribers. Likewise multiple domain names within the same certificate are not supported in the Class 1 settings.

  The validation may be valid for 30 days for the generation of certificates.

- **IP Addresses**

  IP Addresses representing a dotted IPv4 address, typically “10.0.0.1” (*) are validated by sending a electronic mail message with a verification code to one of the following administrative mail accounts:

  - webmaster@10.0.0.1
  - hostmaster@10.0.0.1
  - postmaster@10.0.0.1

  The subscriber has to return and submit the verification code as prove of ownership of the domain name within a limited period sufficient enough to receive an electronic mail message.

  The validation may be valid for 30 days for the generation of digital certificates.

  (*) The IP 10.0.0.1 is an illustrative example.

Class 2

- **Personal Identity**

  The verification process of personal identities of subscribers are performed manually. The StartCom CA validates without any reasonable doubt that the following details are correct:

  - First and last name
  - Residence, Address
  - State or Region
  - Country

  The subscriber has to provide in a secure and reliable fashion two scanned or photographed identification papers in high quality and resolution. The documents must be valid in every respect and not be expired.

  If the accuracy of the documents are in doubt as to the correctness of the details provided, the StartCom CA may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority or Latin notary via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of the StartCom CA and shall be returned to the sender via registered postal mail.

  The validation may be valid for 365 days for the generation of digital certificates.

- **Organization**

  The verification process of organizations implies same level identity validation of the subscriber (responsible person) and are performed manually. The StartCom CA validates without any reasonable doubt that

the following details are correct:

- Registered organization name
- Address
- State or Region
- Country

The subscriber has to provide in a secure and reliable fashion supporting documentation. The documents must be valid in every respect and not be expired.

If the accuracy of the documents are in doubt as to the correctness of the details provided, the StartCom CA may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of the StartCom CA and shall be returned to the sender via registered postal mail.

The validation may be valid for 365 days for the generation of digital certificates.

Class 3

- **Personal Identity and Organization**

  Class 3 validation is reserved for specially trusted entities to which the StartCom CA has usually a relationship like business partnership which includes employees, investors, business partners and operators of intermediate CAs. The StartCom CA management knows without any doubt the entity in question. The StartCom CA is in the possession or has reviewed original documents during face-to-face meetings about the entity in question.

  The validation may be valid for 365 days for the generation of digital certificates.

Extended Validation

- **Personal Identity**

  Extended Validation for identities will be performed according to the validation procedures and requirements of the Extended Validation Guidelines once and if such guidelines will be published by the CA/Browser Forum. Applicants for EV must be at least Class 2 Identity validated prior to engagement for Extended validation.

- **Organization**

  Extended Validation for organizations are performed according to the

validation procedures and requirements of the Extended Validation Guidelines as published by the CA/Browser Forum. Applicants for EV must be at least Class 2 Identity validated prior to engagement for Extended validation.

Certificate Profiles

Naming conventions

Class 1

- **Client Authentication and S/MIME certificates**
  - CN = *StartCom Free Certificate Member*
  - O = Subscriber first and last name
  - OU = *Persona not validated*
  - E = Validated email address
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country

  Certificate shall be valid for 365 days.

- **SSL/TLS server certificates**
  - CN = Validated domain name (www.domain.com)
  - O = Base domain name (domain.com)
  - OU = *StartCom Free Certificate Member*
  - E = Validated email address
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country

  Subject Alt Name extension is not critical and contains CN field value and the base domain.

  Certificate shall be valid for 365 days.

Class 2

- **Client Authentication and S/MIME certificates**
  - CN = First and last name
  - O = Validated organization name (otherwise empty)
  - OU = *StartCom Verified Certificate Member*
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country
  - E = Validated email address

  Certificate shall be valid for 365 days.

- **SSL/TLS server certificates**
  - CN = Validated domain name (www.domain.com)
  - O = Validated first and last name or validated organization name
  - OU = *StartCom Verified Certificate Member*
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country
  - E = Validated email address

  Subject Alt Name extension is not critical and may contain multiple validated domain name field values.

  Certificate shall be valid for 365 days.

- **Object Code Signing certificates**
  - CN = First and last name
  - O = Validated organization name (otherwise empty)
  - OU = *StartCom Verified Certificate Member*
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country
  - E = Validated email address

  Certificate shall be valid for 365 days.

Class 3

- **Client Authentication and S/MIME certificates**
  - CN = First and last name
  - O = Validated organization name (otherwise empty)
  - OU = *StartCom Trusted Certificate Member*
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country
  - E = Validated email address

  Certificate may be valid for 2 years.

- **SSL/TLS server certificates**
  - CN = Validated domain name (www.domain.com)
  - O = Validated first and last name or validated organization name (otherwise empty)
  - OU = *StartCom Verified Certificate Member*
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country
  - E = Validated email address

  Subject Alt Name extension is not critical and may contain multiple validated domain name field values.

  Certificate may be valid for 2 years.

- **Object Code Signing certificates**
  - CN = First and last name
  - O = Validated organization name (otherwise empty)
  - OU = *StartCom Verified Certificate Member*
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country
  - E = Validated email address

  Certificate may be valid for 2 years.

Extended Validation

- **SSL/TLS server certificates**
  - CN = Validated domain name (www.domain.com)
  - O = Validated organization name
  - OU = *StartCom Extended Validation*
  - L = Locality
  - ST = State, administrative or geographical region
  - C = Country
  - E = Validated email address
  - OID 2.5.4.5 = Serial or registration number
  - OID 2.5.4.9 = Street address
  - OID 2.5.4.17 = Postal or zip code
  - OID 1.3.6.1.4.1.311.60.2.1.3 = Locality of in corporation
  - OID 1.3.6.1.4.1.311.60.2.1.2 = State or province of incorporation (optional)
  - OID 1.3.6.1.4.1.311.60.2.1.3 = Country of incorporation (optional)

  Subject Alt Name extension is not critical and may contain multiple validated domain name field values.

  Certificate shall be valid for 365 days.

Intermediate Class 1 – 3 Certificates

- E = Validated email address (optional)
- CN = StartCom Class [1-3] [Server | Client | Object] CA
- OU = Organizational Unit
- O = Organization
- C = Country

Certificate shall be valid for 5 years. Subscriber certificates are issued during the first to fourth year, whereas during the last 365 days of the validity of the intermediate CA certificate no subscriber certificates are issued. The intermediate certificate continues to issue the corresponding CRL during the fifth year.

Intermediate Extended Validation Certificates

- CN = StartCom Extended Validation [Server | Client | Object] CA
- OU = Organizational Unit
- O = Organization
- C = Country

Certificate shall be valid for 10 years. Subscriber certificates are issued during the first to ninth year, whereas during the last 365 days of the validity of the intermediate CA certificate no subscriber certificates are issued. The intermediate certificate continues to issue the corresponding CRL during the tenth year.

Other Certificate Attributes

- **Version Number**
  - X.509 v3 for CA and subscriber certificates
  - X.509 v1 for CRL certificates

- **Serial Number**
  - Unique value.

- **Validity**
  - Start: MM/DD/YYYY hh:mm:ss GMT
  - End: MM/DD/YYYY hh:mm:ss GMT

- **Certificate extensions**

  Subscriber S/MIME Client Certificates:

  - Basic Constraint: CA:FALSE, Path Length Constraint 0
  - Key Usage: Digital Signature, Key Encipherment, Data Encipherment
  - Extended Key Usage:
    - Client Authentication (1.3.6.1.5.5.7.3.2)
    - Secure Email (1.3.6.1.5.5.7.3.4)
  - Subject Key Identifier: Hash
  - CRL Distribution Points: URL
  - Authority Info Access: Access Method (1.3.6.1.5.5.7.48.2), OCSP URL

- Authority Key Identifier: Key ID, Certificate Issuer
- Issuer Alternative Name: URI:http://url
- Certificate Policies: Policy Identifier (1.3.6.1.4.1.23223.1.1.X)

Subscriber SSL/TLS Server Certificates:

- Basic Constraint: CA:FALSE, Path Length Constraint 0
- Key Usage: Digital Signature, Key Encipherment,
- Key Agreement
- Extended Key Usage:
    - Client Authentication (1.3.6.1.5.5.7.3.2) [Class 2+3 only]
    - Server Authentication (1.3.6.1.5.5.7.3.1)
    - MS Server Gated Crypto (1.3.6.1.4.1.311.10.3.3)
    - NS Server Gated Crypto (2.16.840.11137.30.4.1)
- Subject Key Identifier: Hash
- CRL Distribution Points: URL
- Authority Info Access: Access Method (1.3.6.1.5.5.7.48.2), OCSP URL
- Authority Key Identifier: Key ID, Certificate Issuer
- Issuer Alternative Name: URI:http://url
- Certificate Policies: Policy Identifier (1.3.6.1.4.1.23223.1.1.X)

Intermediate Certificates:

- Basic Constraint: Critical, CA:TRUE
- Key Usage:
    - Digital Signature
    - Key Encipherment
    - Certificate Signing
    - CRL Signing
- Subject Key Identifier: Hash
- Authority Key Identifier: Key ID, Certificate Issuer
- Issuer Alternative Name: URI:http://url

Online Certificate Status Protocol (OCSP) Responder:

- Online Certificate Status Protocol responders conform to RFC

2560.

CRL Certificates:

- Version: v1
- Signature Algorithm: Sha1 with RSA encryption
- Issuer: Identification of the CA issuing the CRL
- Last Update: Time of CRL issue
- Next Update: Time of next CRL issue (every 12 hours)
- Revoked certificates: Listing of information for revoked certificates

Revocation

Circumstances for Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- The subscriber's private key is lost or suspected to be compromised
- The information in the subscriber's certificate is suspected to be inaccurate
- The information supplied may be misleading (e.g., paypa1.com, micr0soft.com)
- The subject has failed to comply with the rules in this policy
- The system to which the certificate has been issued has been retired
- The subscriber makes a request for revocation (*)
- The subscriber violated his/her obligations

* Subscribers of Class 1 certificates are advised to use different sub domains instead of requesting revocation when encountering a user induced or installation error.

Distribution of Certificate Revocation List

The corresponding Certificate Revocation Lists (CRL) of subscriber certificates are updated every 12 hours or every time a certificate is revoked, whichever comes first. The CRL is published via Internet download. Each intermediate CA issues its own corresponding CRL for the certificates issued. The CRL distribution points are included in the certificates.

The CRL of root and intermediate CA certificates may be valid for one year and shall be updated accordingly.

OCSP Responder Service

An OCSP responder service is provided and the respective URL location of the service are included in the certificates. The OCSP responder provides results about the status of a certificate instantly. The current CRLs are reloaded at least every 60 minutes.

Who Can Request Revocation

A certificate revocation can be requested by the subscriber of the certificate or by any other entity presenting proof of knowledge of circumstances for revocation. Subscribers of Class 1 certificates are advised to use different sub domains or email addresses instead of requesting revocation when encountering a user induced or installation error or failure to adequately store and backup the private key(s).

Procedure for Revocation Request

Subscribers may request revocation of a certificate by using the on-line utility provided at the CA web site.

Certificate revocation may also be requested by sending an electronic mail message to certmaster@startcom.org with clear identification and information details, according to the above mentioned circumstances for revocation.

The StartCom CA makes every reasonable effort to verify the claims, reason and identity of the requester.

The subscriber will be notified of the revocation via electronic mail message. Upon the revocation of a subscriber's certificate, the newly revoked certificate is recorded and an updated CRL shall be issued.

StartCom Intermediate CA Program (SICAP)

Middle to bigger sized organizations may request to run an intermediate certification authority, which allows a limited role as intermediate CA operator. Organization wishing to operate such an intermediate CA must be at least two years incorporated, must show a two year business activity and must be a legally registered entity in their country of incorporation. The organization enters a contractual relationship with the StartCom CA which governs all aspects of the intermediate CA and StartCom retains overall responsibility at all times. The intermediate CA is operated at StartCom's premise and the organization must accept all conditions and terms as outlined in the StartCom Intermediate Certification Authority Policy Appendix.

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

Changes:

This CA policy is a revision of the latest published StartCom CA policy and implements aspects for the issuing of Extended Validation Certificates as published by the CA/Browser Forum.

The Policy ID has been updated to version 2.0.

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 23:57:26 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.