StartCom®

Certification Policy & Practice Statement

StartCom CA

Version 3.1

Date: May 5, 2017

Contents

1 Introduction

1.1 Overview

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

The StartCom Certification Authority provides to its subscriber 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.

1.1.1 Philosophy

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 Certification Authority 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.

StartCom believes in the basic right to protect and secure information between two entities without discrimination of race, gender, origin or religion and to provide to the relying parties information and reasonable assurances about the identity of the certificate holders and service addresses.

1.1.2 Copyright, reserved rights

1.2 Document name and identification

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 Certification Authority or 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 Certification Authority 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 Certification Authority and therefore presented together in this document. Whenever needed, the certification policy is followed by the related practice statement.

The current and successive versions of this document intends to meet or exceed the requirements of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”) and the Guidelines for Extended Validation Certificates (“EV Guidelines”) and EV Code Signing Certificate Guidelines, as published by the Certification Authority / Browser Forum ("CAB Forum Guidelines") at http://www.cabforum.org. If any inconsistency exists between this CP/CPS and the Baseline Requirements or EV Guidelines, the Baseline Requirements and EV Guidelines take precedence. It also takes into account the minimum requirements for the issuance and management of publicly-trusted code signing certificates (“Baseline Requirements for code signing certificates”).

In case multiple or alternative methods or options are possible by the baseline requirements or guidelines in order to perform a certain task and/or multiple or alternative methods or options are offered in order to comply to those requirements and guidelines, StartCom 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 to do so on a case to case basis.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this document is divided into nine parts that cover the security controls and practices and procedures for certificate or time-stamping services within the StartCom PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation."

StartCom may publish additional certificate policies or certification practice statements as necessary to describe other product and service offerings. These supplemental policies and statements are available to applicable users or relying parties through the online repositories.

Version: 3.1
Updated: 5/5/2017

Previous versions

CPS version	Applicable dates
2.4	18/12/2015 to 22/3/2016
2.5	23/3/2016 to 15/5/2016
2.5.1	16/5/2016 to 30/8/2016
2.5.2	1/9/2016 to 9/4/2017
3.0	10/4/2017 to 5/5/2017

StartCom´s IANA assigned OID is: 1.3.6.1.4.1.23223

In section 1.3.3 is indicated how this OID is used within subscriber certificates.

1.3 PKI participants

The parties involved in the management and operations of the Certification Authority are:

- Certification Authorities.
- Registration Authorities.
- Subscribers.
- Relying parties

1.3.1 Certification Authorities

StartCom defines a hierarchy in which includes root CAs and Intermediate or Issuing CAs. The Certification Authorities shall:

- Perform its operations according to the CPS
- Issue and publish certificates in a timely manner as stated in the CPS
- Revoke a certificate following the procedures stated in this document
- Publish and update CRLs accordingly
- Notify subscribers if or when needed

This is the list of the root CAs and subordinate CAs of StartCom

Root CAs:

- (1) StartCom Certification Authority G3
  Serial number: 3f ad 7f d6 a9 bf b8 3a
  Hash algorithm: sha256
  Public Key: RSA (4096 bits)
  Validity dates: from 22/3/2017 to 22/3/2042
  Fingerprint: 68 9a 12 29 d6 98 d1 72 e9 9e 1b f0 0b 9c 19 85 41

19 c9 fc

- (2) StartCom Certification Authority ECC
  Serial number: 16 9b 25 01 86 74 b1 45
  Hash algorithm: sha384
  Public Key: ECC (384 bits)
  Validity dates: from 22/3/2017 to 22/3/2042
  Fingerprint: b5 10 85 d9 5b 95 da 91 20 12 d2 c3 b0 01 9a 2d c4 6d 26 e3

- (3) StartCom Certification Authority CS
  Serial number: 33 6e bf 7e e4 c9 73 28
  Hash algorithm: sha256
  Public Key: RSA (4096 bits)
  Validity dates: from 22/3/2017 to 22/3/2042
  Fingerprint: 8e 20 7f 5d c0 a6 9a a3 37 65 8d 23 67 43 3e c2 7d 85 06 d0

Subordinates CAs:

- (1) EV SSL Intermediate CA
  Serial number: 42 7d d2 61 7c e7 cf 7d
  Hash algorithm: sha256
  Public Key: RSA (4096 bits)
  Validity dates: from 7/4/2017 to 22/3/2042
  Fingerprint: 18 c2 ce 89 28 b8 74 49 6c 47 f7 76 e2 76 ea a6 cd 9d 80 ac

- (2) BR SSL Intermediate CA
  Serial number: 14 c9 79 2b 2b 1d a9 26
  Hash algorithm: sha256
  Public Key: RSA (4096 bits)
  Validity dates: from 7/4/2017 to 22/3/2042
  Fingerprint: 37 7b 35 1c cb 87 a4 f5 f1 d3 99 78 56 13 15 cd 46 0d 67 1a

- (3) CC Intermediate CA
  Serial number: 38 14 77 99 d6 2c c5 cd
  Hash algorithm: sha384
  Public Key: ECC (384 bits)
  Validity dates: from 7/4/2017 to 22/3/2042
  Fingerprint: 73 6b 8a b6 a7 0a 65 23 b4 76 d9 db bd d4 47 dd cc 73 b6 30

- (4) CS Intermediate CA
  Serial number: 1a 72 88 b2 7b c8 9d 29
  Hash algorithm: sha256
  Public Key: RSA (4096 bits)
  Validity dates: from 4/5/2017 to 4/5/2037

Fingerprint: 5c b6 19 e3 08 4e 8f 1f 30 48 df c4 0a 5f 79 f4 a4 85 fa 95

- (5) CS2 Intermediate CA
  Serial number: 7a 98 92 87 57 75 b3 2b
  Hash algorithm: sha256
  Public Key: RSA (4096 bits)
  Validity dates: from 7/4/2017 to 22/3/2042
  Fingerprint: 4a 99 de ad ff 97 17 2a e2 a8 0e ef f9 5d 9b de 05 fb 5d 52

- (6) CC2 Intermediate CA
  Serial number: 30 b5 82 5c 07 bb c4 9c
  Hash algorithm: sha384
  Public Key: ECC (384 bits)
  Validity dates: from 28/4/2017 to 28/4/2037
  Fingerprint: 46 d2 5e 74 ed d7 ae 14 f5 99 48 b4 18 47 a2 b9 60 2d 58 91

1.3.2 Registration Authorities

This Certification Practice Statement applies to the Registration Authorities managed by StartCom CA in procedures when issuing and managing certificates.

Registration Authorities identify applicants, subscribers and holders of certificate keys, verify the documentation accrediting the circumstances appearing in the certificates, and validate and approve requests to issue, revoke and renew certificates.

The StartCom Certification Authority or the user entities with which StartCom Certification Authority signs the corresponding legal instrument are the registration authorities.

1.3.3 Subscribers

Subscribers are all end users of certificates issued by an issuing certification authority. A subscriber is the authorized person of the entity named as the end user of a digital certificate. Subscribers may be individuals (natural persons), organizations (legal persons) 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 subject referenced in the certificate is the entity identified to whom the credential is legally bound.

Subscriber certificates for the Class 1 through Class 4 include a policy identifier whose root OID is 1.3.6.1.4.1.23223.X.X.X, where "X.X.X" represents the policy version the identifier is referring to, meaning the first number the root number, the second the intermediate CA number and the last one a correlative number starting by 1.

1.3.4 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 Certification Authority. A relying party may or may not also be a subscriber of the StartCom Certification Authority. 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.

1.4 Certificate usage

1.4.1 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 Certification Authority acts as and provides root CAs 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, called class 4. The ICAs are further separated by their end-user purpose and key usage, such as web server (SSL), email (S/MIME), document and authentication, object code signing.

The StartCom Certification Authority 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 below in this section.

1.4.2 Obligations

1) 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, expiration and revocation
• Accept revocation requests according to this document
• Issue Certificate Revocation Lists (CRL)
• Publish the CRL's issued
• Provide OCSP service
• Keep audit logs of the certificate issuance process
• Protect private and individual data obtained
• Maintain best security standards possible

2) Intermediate CA Obligations

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

3) Subscriber Obligations

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.
• Provide and supply correct and truthful information including personal whenever indicated and requested.
• 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.

Prohibited certificate usages

• 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 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 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.

4) Relying Party Obligations

• Read the procedures published in this document.
• Use the certificates for the permitted uses only.
• Understand the limitations of the liability and warranties as published in this document.
• Not assume any authorization attributes based solely on an entity's possession of a StartCom Certification Authority issued certificate.

- Must 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.
- 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 its content for reliance.

1.5 Policy administration

Information located in this section includes the contact information of the organization responsible for drafting, registering, maintaining, updating and approving this CPS.

The policy is legally binding from the moment of its publication and is updated at least once a year.

The StartCom Certification Authority policy is subject to changes, and it is the responsibility of the subscribers and relaying parties 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. The policy is legally binding from the moment of its publication.

1.5.1 Organization administering the document

StartCom CA maintains this Certificate Practice Statement.

1.5.2 Contact information

The StartCom CA may be contacted at:

StartCom CA
Plaza Circular 4, 5ºizda
48001 Bilbao
Spain

Tfno: +34 944 007 736
Email: startcom@startssl.com

Additional information can be found at the StartCom CA website: https://www.startcomca.com

For specific contact details, different StartCom teams may be contacted through these emails:

Validation: certmaster@startssl.com
Help: help@startssl.com
Support: support@startssl.com
Abuse: abuse@startssl.com
Website: webmaster@startssl.com

1.5.3 Person in charge adapting CPS suitability

The StartCom CA Board of Directors is the body responsible for determining the suitability of this Certificate Practice Statement and any proposed changes prior to the publication of an amended version.

1.5.4 CPS approval procedure

The StartCom CA Board of Directors is the body approving this Certificate Practice Statement and any subsequent changes or amendments.

Changes to the policy requires increasing of the policy version number by one. Additional policy identifiers for the recognition by software vendors may be included as necessary.

Controls are in place to reasonably ensure that the policy and practice statements are not amended and published without the prior authorization by the management of StartCom.

1.6 Definitions and acronyms

1.6.1 Definitions

Applicant is the natural or legal person that applies or request a certificate. Once the certificate is issued, the applicant is named or referred to as the subscriber

Audit report is a document that states the qualified auditor´s opinion on whether an entity´s processes and controls comply with the provisions of the standards applied.

Certificate is an electronic document that uses a digital signature to bind a public key and a natural or legal person

Certification Authority is an organization that is responsible for the creation, issuance, revocation, and management of certificates. The term applies equally to both Roots CAs and subordinate/intermediate/issuing CAs.

Certificate Management System is a tool to process, approve issuance of, or store certificates or any other additional information.

Issuing CA is the CA that issues certificates

Private Key means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key means the key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Qualified auditor means natural person or Legal Entity that meets the requirements as indicated in the CAB Forum documents

Relying party is a natural or legal person that relies upon the information contained in the certificate

Root CA is the top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate is the self-signed certificate issued by the Root CA to identify itself and to facilitate verification of certificates issued to its subordinate CAs.

Subordinate CA is a Certification Authority whose certificate is signed by the Root CA, or another subordinate CA. It may be also called intermediate CA or issuing CA if this subordinate CA is issuing end user certificates.

Subscriber means a natural or legal person that has been issued a certificate

Subscriber Agreement is a document that has to be read and accepted by a certificate requester or applicant before applying for a certificate.

WebTrust means the current version of the AICPA/CICA WebTrust Program for Certification Authorities.

1.6.2 Acronyms

CA Certification Authority
CAA Certification Authority Authorization
CAB CA/Browser
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List
CSR Certificate Signing Request
EV Extended Validation

EKU Extended Key Usage
FIPS United States Federal Information Processing Standards
FQDN Fully Qualified Domain Name
HSM Hardware Security Module
IANA Internet Assigned Numbers Authority
HTTP Hyper Text Transfer Protocol
HTTPS Hyper Text Transfer Protocol Secured
ICA Intermediate Certification Authority
ITU International Telecommunication Union
ITU-T ITU Telecommunication Standardization Sector
OCSP On-line Certificate Status Protocol
OID Object Identifier
SHA Secure Hashing Algorithm
PKI Public Key Infrastructure
PKIX Public Key Infrastructure (based on X.509 Digital Certificates)
S/MIME Secure multipurpose Internet mail extensions
SSL Secure Socket Layer
TLS Transport Layer Security
TSA Time-Stamp Authority
URL Uniform Resource Locator
X.509 ITU-T standard for Certificates

2. Publication and repository responsibilities

StartCom makes a reasonable effort to provide access to its certificate repositories, certificate revocation lists, certificate policy and practice statements and other documents to the public on an ongoing basis. StartCom implements logical and physical controls to prevent unauthorized write access to those repositories and files.

StartCom publishes a repository of policies, agreements and notices as well as any other information it considers necessary for providing its services at:

- http://www.startcomca.com/policy/

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

- http://www.startcomca.com/root/

The public root CA keys 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:

- https://www.startcomca.com/root/

All public CA keys of the StartCom Certification Authority may be downloaded via secured and encrypted protocols (SSL) from this URL. 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.

For CRL issuance frequency please refer to section 7.4 of this CPS.

3. Identification and authentication

3.1 Naming

3.1.1 Types of digital X.509 certificates

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) Time Stamping Certificates are used to ensure that the signing took place at a specific point in time, thus extending the validity of the code past its certificate expiration date.

5) Online Certificate Status Protocol (OCSP) Certificates are issued to the OCSP responders operated by the StartCom Certification Authority for the signing of OCSP responses upon requests by client software.

6) Intermediate CA Certificates are used exclusively for the issuing and signing of end user certificates and certificate revocation lists.

7) CA Root Certificate is used to exclusively sign and issue the intermediate CA certificates and corresponding certificate revocation list.

3.1.2 Classes of digital x.509 certificates

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 certificates.

2) Class 2 Certificates provide medium assurances about the subscribers' personal identity and subscribers of Class 2 certificates have to prove their identity by various means.

3) Class 3 Certificates provide a high level of assurance about the subscribers' organizational identity in comparison with Class 1 and 2 certificates and are issued to organizations that successfully completed a class 3 Validation.

4) Class 4 Extended Validation (EV) Certificates implements the validation procedures and requirements of the Extended Validation Guidelines as published by the CA/Browser Forum.

3.1.3 Need for names to be meaningful

When applicable, Issuer CAs shall use Distinguished Names (DN) to identify both the subject and issuer of the certificate.

3.1.4 Rules for interpreting various name forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of names

Distinguished Names shall be unique within the same CA issuer public key infrastructure (e.g. final issuer CA).

3.1.6 Recognition, authentication and role of trademarks

Subscribers SHALL NOT request certificates with any content that infringes the intellectual property rights of another entity. Issuer

CAs may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial identity validation

3.2.1 Subscriber private key generation and delivery

Subscribers SHALL NOT reuse private keys for successive certificates after expiration thereof and it's highly recommended to create a new key for every certificate. Private keys of certificates which where revoked MUST NOT be reused.

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

SSL/TLS Server Certificates

The StartCom Certification Authority doesn’t offer the creation of key pairs and certificate signing requests (CSR) for server certificates through the CA system.

Subscribers may produce and prepare their own private keys and certificate signing requests (CSR) for server certificates and submit the CSR via SSL secured connection to the CA system and the CSR shall serve as prove of possession of the private key.

Client S/MIME and Code signing certificates

Client S/MIME and Object Code Signing keys are usually generated at the client side via appropriate browser functions. In this case, private key delivery to the subscriber is unnecessary and the submitted CSR shall serve as prove of possession of the private key.

Subscribers shall use smart cards, hardware tokens or integrated circuit card for the storing of private keys in case of code signing certificates.

However the StartCom Certification Authority may deliver certificates on such devices offering the creation of key pairs and certificates.

3.2.2 Validations

1) Class 1

3.2.2.1.1 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 to receive an electronic mail message.

The validation MAY be valid for up to 90 days from the validation finished day.

3.2.2.1.2 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

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

Furthermore, StartCom also requests a domain authorization letter to cross check with the WHOIS information.

The validation MAY be valid for up to 90 days from the validation finished day.

The StartCom Certification Authority performs additional sanity and fraud prevention checks in order to limit accidental issuing of certificates using internal high-risks list whose domain names

might be misleading and/or might be used to perform an act of fraud, identity theft or infringement of trademarks. For example, domain names resembling well-known brands and names like PAYPA1.COM and MICR0S0FT.COM, or when well-known brands are part of the requested hostnames like FACEBOOK.DOMAIN.COM or WWW.GOOGLEME.COM. StartCom however may consider issuance of a certificate containing a possible high-profile brand or name depending on the circumstances and reasonable judgment.

Only wild card domain names like "*.domain.com" are issued to Class 2 and class 3 SSL certificate. Multiple domains and sub domains may be supported in the Class 1 level provided they don't include any high-profile brand and keyword.

Note: StartCom performs and follows validation method 2 and 5 according to the CAB Forum Baseline Requirements

3.2.2.1.3 IP Addresses

IP Addresses representing a dotted IPv4 address usually, typically "10.0.0.1" (*) are validated by sending an 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.

If subscriber can't receive email from the above 3 email account, he/she can choose to do the website control validation that the subscriber must upload a website control validation code file to the website(IP address) root directory to finish the website control validation.

The validation MAY be valid for up to 90 days for the generation of digital certificates.

(*) The IP 10.0.0.1 is an illustrative example.

2) Class 2

3.2.2.2.1 Personal Identity

Domain Control and Email Control Validations are implied as a requirement as per Class 1.

The StartCom Certification Authority validates without any reasonable doubt that the following details are correct:

- First and last name
- city (if verified)
- State or Region (if verified)
- Country

The subscriber has to provide in a secure and reliable fashion 2 (two) scanned or photographed identification documents in reasonable quality and resolution that were issued by either a local, state or federal authority. The documents must be valid in every respect and not be expired; modifications and/or obscuring details of the original documents or provided images is prohibited. StartCom MUST reject such evidence if the documents are not compliant to this requirement.

If the accuracy of the documents are in doubt as to the correctness of the details provided, the StartCom Certification Authority 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 premises of the StartCom Certification Authority.

StartCom verifies the correctness of the identity through an internal confirmation procedure of the submitted personal details with third party sources and cross-verification of the claimed identity. In the absence of third party sources or listing thereof, a registered postal mail may be sent to the claimed address and identity. If neither verification procedure succeeds, the validation request MUST NOT be approved.

The validation MAY be valid for up to 365 days from the validation finished day.

3) Class 3

3.2.2.3.1 Organization Identity

Domain Control and Email Control Validations are implied as a requirement as per Class 1.

The StartCom Certification Authority validates without any reasonable doubt that the following

details are correct:

- Legal Entity (Trading Name Optional *)
- city
- State or Region
- Country

(*) When using a trading or assumed name (DBA), the legal entity is stated in brackets after the assumed name. This may be a registered/incorporated entity or a sole proprietor's name.

The subscriber has to provide in a secure and reliable fashion supporting documentation, which must be from either a Qualified Government Information Source, Qualified Government Tax Information Source or Qualified Independent Information Source. The documents must be valid in every respect and not be expired.

If the accuracy of the documents is in doubt as to the correctness of the details provided, the StartCom Certification Authority 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 Certification Authority.

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 confirm the necessary authority if necessary. StartCom may assume proper authorization in case the validated subscriber is either the appointed CEO, Director, President, owner or sole proprietor.

StartCom verifies the correctness of the organization details through an internal confirmation procedure of the submitted documents with third party sources and cross-verification of the claimed organization. In the absence of third party sources or listing thereof, a registered postal mail is sent to the claimed address and organization name. If no verification procedure succeeds, the validation request MUST NOT be approved.

Subscribers that have been validated for Extended Validation are equally considered Class 3 validated.

The validation MAY be valid for up to 365 days from the validation finished day.

4) Class 4 Extended Validation

3.2.2.4.1 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.

StartCom 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.

The validation MAY be valid for up to 365 days from the validation finished day.

3.2.3 Criteria for interoperation

The StartCom Certification Authority 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. The StartCom Certification Authority may cross-sign new CA root certificates it issues, or be cross-signed, 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 Certification Authority and must commit to all requirements of the StartCom Certification Authority 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, external, cross-signed or subordinated CA must adhere to the validation requirements of this policy.

3.3 Identification and authentication for re-key requests

Not applicable

3.4 Identification and authentication for revocation requests

StartCom authenticates revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised or based on other evidence provided (such as host names used within a certificate). Authenticated subscribers may request revocation through the provided user accounts and control panels at StartCom's web sites.

4. Certificate Life-Cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Any individual or organization may apply for enrollment of Class 1 certificates, based on the requirements thereof.

Any individual may apply for Class 2 Identity Validation, however the StartCom Certification Authority reserves the rights to reject an application if an individual is listed on a government denied list, list of prohibited persons under the applicable laws.

Any Organization may apply for Class 3 Identity Validation, however the StartCom Certification Authority reserves the rights to reject an application if an entity is listed on a government denied list, list of prohibited persons in the organization, or other list that prohibits doing business with such organization or person under the applicable laws.

Applicants for Extended Validation MUST NOT be listed on any government denial list or prohibited list.

4.1.2 Subscriber agreement requirements

By accepting a certificate from StartCom, 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. The certificate applicants can acknowledge the acceptance of CP and CPS electronically on StartCom website.

Applicants of certificates have to enter into a legally valid and enforceable subscriber agreement with the StartCom Certification

Authority for every new or renewal request.

4.1.3 Certificate request requirements

The applicant shall serve as the “Contract Signer”, “Certificate Approver”, and “Certificate Requester” as defined by the CA/Browser Forum Guidelines. The applicants must make the request by the designated utility at the StartCom Certification Authority operated web site and sign the correspondent Subscriber Agreement.

4.1.4 Enrollment process and responsibilities

The StartCom Certification Authority is responsible for ensuring that the identity of each Certificate Applicant is verified in accordance with this CP/CPS prior to the issuance of a certificate. Applicants are responsible for submitting sufficient information and documentation in order to perform the required verification of identity prior to issuing a Certificate. The StartCom Certification Authority shall authenticate and protect all communication made during the certificate application process.

The StartCom Certification Authority validations are valid for 1 year and hence performs and validates all the subscriber information at least once a year.

The StartCom Certification Authority 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 Extended Validation Guidelines.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

As per section “3.2.2 Validations” for doing technical validations and section “4.1.4 Enrollment process and responsibilities” for the validity of the validated information

4.2.2 Approval and rejection of certificate applications

Following successful completion of all required validations of a certificate application the StartCom Certification Authority approves an application for a digital certificate.

If the validation of a certificate application fails, the StartCom

Certification Authority rejects the certificate application. StartCom reserves its right to reject applications to issue a certificate to applicants if, on its own assessment and may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal. Applicants whose applications have been rejected may subsequently re-apply.

When a certificate request is to be used for server authentication, the StartCom Certification Authority will check the CAA records as specified by the RFC 6844 according to the dates set by the CA/Browser Forum.

4.2.3 Rejected certificate applications

The private key associated with a public key, which has been submitted as part of a rejected certificate application, may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate. The private key may also not be resubmitted as part of any other certificate application.

4.3 Certificate issuance

The StartCom Certification Authority makes reasonable efforts to confirm certificate application information and issue certificates within a reasonable time frame. This greatly dependents on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, the StartCom Certification Authority aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application or according to the EV SSL Certificate Guidelines, SSL Baseline Requirements and Code Signing Baseline Requirement.

StartCom is committed with the security of the internet in order to fight against phishing and malware content, the StartCom Certification Authority is implementing a phishing and malware status check for the issuance of server certificates based on the use of 2 complementary tools, the 360 keyword list tool and the Google Safe browsing API, also with the combination of a potential high-risk domain list. The 360 keyword tool searches and screens for combinations of sensitive/fraud keywords, IDN domain name detection, blacklist and cross-check with Google tool and refuse to issue certificates that are flagged as phishing or malware sites.

StartCom logs all SSL Certificates in two or more Certificate Transparency databases. See RFC 6962 for technical information. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the certificate is stored in a database.

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.

4.4 Certificate acceptance

An issued certificate is either delivered through an on-line collection method, retrieved from the provided on-line interfaces or delivered in a hardware device. A subscriber is deemed to have accepted a certificate when delivered and installed into client or server software or when retrieved from the on-line interfaces.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

By accepting a certificate from the StartCom Certification Authority, 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 Certification Authority does not keep any private keys except its own. 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.

4.5.2 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 MUST NOT rely on the end user certificate or other revoked certificates in the certificate chain.

4.5.3 Prohibited certificate usage

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued. Code signing certificates do not indicate that the signed code is safe to install or is free from malware, bugs, or vulnerabilities.

Certificates issued under this policy may not be used for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or where prohibited by law.

4.6 Certificate renewal

Certificate “renewal” is performed by the subscriber by obtaining a new certificate for the intended purpose according to the policy. StartCom doesn't renew certificates it previously issued.

4.7 Certificate re-key

StartCom doesn't “rekey” existing certificates and subscribers should always obtain or create a new key for the certificates.

4.8 Certificate modification

StartCom doesn't “modify” existing certificates and subscribers should obtain a new certificate with the desired properties and according to this policy.

4.9 Certificate revocation and suspension

4.9.1 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:

1) The subscriber's key is suspected to be compromised;
2) The technical content or format of the certificate presents an unacceptable risk;
3) The information in the subscriber's certificate is suspected to be inaccurate;
4) The information supplied may be misleading (e.g., PAYPA1.COM, MICR0S0FT.COM);
5) The subject has failed to comply with the rules and obligations of this policy;
6) The subscriber makes a request for revocation

4.9.2 Who can request revocation

Certificate revocation can be requested by the subscriber of the certificate or by any other entity presenting evidence or knowledge of possible circumstances for revocation. A handling fee may be charged for revocations.

4.9.3 Procedure for revocation request

Subscribers may request revocation of a certificate by using the on-line utility provided at the web site (control panel).
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 Certification Authority makes every reasonable effort to verify the claims, reason and identity of the requester will begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1) The nature of the alleged problem
2) The number of reports received
3) The entity making the complaint
4) Relevant legislation

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. Notification of revocation of a certificate to others than the subscriber and subject of the certificate, beyond the published CRL, are generally not performed.

4.9.4 Suspension

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

4.10 Certificate status service

4.10.1 Distribution of Certificate Revocation List

The corresponding Certificate Revocation Lists (CRL) of subscriber certificates are updated at least 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.

The last CRL of issuer certificates which reach end-of-life (expired) shall remain published available for a period of 365 days. Such last CRL shall be archived with other related records of the expired issuer certificate.

4.10.2 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. Error responses by the OCSP responder may be unsigned and include regular HTTP status errors.

4.10.3 Service availability

Certificate status services shall be available 24x7 without interruption.

4.11 End of subscription

A Subscriber's subscription service ends if its certificate(s) expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

The StartCom Certification Authority makes reasonable efforts to notify subscribers via e-mail of the imminent expiration of a digital certificate. Notice shall ordinarily be provided within a two week period prior to the expiration of the certificate.

4.12 Key escrow and recovery

Not applicable

5. Facility, management and operational controls

5.1 Physical security controls

5.1.1 Site location and construction

The StartCom Certification Authority operates a tightly controlled and restricted infrastructure and 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 and software is protected and constantly monitored by authorized service personnel for intrusion and compromise. Various programs and tools are installed to assist in this task. Hardware equipment and operating systems are maintained at the highest possible level of security.

5.1.2 Physical access

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 StartCom management. Physical access to the server infrastructure and facilities shall be logged and signed. Otherwise physical access to the systems shall be avoided.

The StartCom Certification Authority implements various access codes, smart cards, electronic tokens and physical locks in multiple combinations thereof for facility access, work stations, CA administration programs, server administration programs and monitoring devices to restrict and control access according to the defined roles and permissions.

5.1.3 Maintenance

Besides the attached hardware security modules, no removable media or devices shall be accessible or in existence 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 StartCom management. Any removed device which may contain data (like hard drives) must be wiped out of any data before disposal or stored in safety vaults.

5.1.4 Power and air condition

The locality is fully air conditioned to prevent overheating and to maintain a suitable humidity level. Primary and secondary power supplies ensure continuous, uninterrupted access to electric power. Electricity power backup (UPS) is supported by an external, independent electricity power source for cases of prolonged power outages.

5.1.5 Water exposures

All server equipment and devices are elevated above the ground. No water lines exist above equipment.

5.1.6 Fire prevention and protection

Fire alarm and intrusion prevention equipment are installed, maintained and available at the premise.

5.1.7 Media storage

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

5.1.8 Waste disposal

The StartCom Certification Authority implemented 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.

5.1.9 Off-site backup

Daily backup of its CA related data that are rotated and stored according to either on-site or off-site according to an established backup rotation schedule.

The frequency, retention, and extent of the backup is specified in the backup procedure, for example, data is 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.

Access to backup servers/media is restricted to authorized personnel only. Backup media is regularly tested through restoration to ensure it can be relied on in the event of a disaster.

Other data is backed up in a rolling fashion and secure manner at a off-site facility beyond 150 miles of the StartCom Certification Authority infrastructure.

5.2 Procedural controls

5.2.1 Trusted roles

A "trusted role" is defined as a person assigned with responsibilities than can lead to security problems if not performed satisfactorily, whether accidentally or maliciously.

StartCom CA has defined all roles within the organisation. The roles and responsibilities are defined for each one of them.

All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of StartCom CA operations.

Persons acting in trusted roles are only allowed to access a CMS after they are authenticated using a method approved as being suitable.

Administrators

The administrator installs and configures the CA software, including key generation, and key backup (as part of key generation) and subsequent recovery.

Validation Officers

The Validation Officer role is responsible for issuing and revoking certificates, the verification of identity, and compliance with the required issuance steps and recording the details of approval.

Validation Officers must identify and authenticate themselves to the CMS system before access is granted. Identification is via a username, with authentication requiring a password and digital Certificate.

Operator

Operators install and configure system hardware, including servers, routers, firewalls, and networks. Also keeps CA, web, CMS and RA systems updated and monitored.

Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits.

5.2.2 Number of person required per task

To reinforce system security, more than one person is assigned to each role. Several individuals may also be assigned to the same role.

For accessing the PKI system StartCom CA requires at least 2 administrators for taking actions related to key pairs.

5.2.3 Identification and authentication for each role

All personnel are required to authenticate themselves to CA and RA (CMS) systems before they may perform the duties of their role involving those systems.

5.2.4 Roles requiring separation of duties

No other trusted role can assume any other role except operators.

5.3 Personnel controls

The StartCom Certification Authority follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

5.3.1 Background, qualifications, experience and clearence requirements

StartCom CA employs personnel with the experience and qualifications needed to perform their job responsibilities.

Every role needs sufficient training in StartCom´s policies and procedures. For EV (Class 4) certificates this training period is more exhaustive before issuance privileges are granted.

5.3.2 Background check procedures

StartCom CA carries out pertinent research before hiring anyone.

These checks may include, but are not limited to, verification of the individual's identity using a government issued photo ID, employment history, education, social security number, criminal background, etc. Due to legal limitations in some countries, a criminal background check may not be included.

5.3.3 Training requirements

StartCom CA provides its personnel with the training needed to perform their job responsibilities competently and satisfactorily. Training is carried out at least once per year, which includes at least the following points:

- A copy of the Certification Practice Statement
- Security procedures for each specific role
- Management and operation procedures for each specific role
- Incident management procedures

5.3.4 Retraining frequency and requirements

Any significant change in industry standards or in the StartCom PKI operations will call for a training plan. In any case, annual training shall always include content review.

5.3.5 Job rotation frequency and sequence

No stipulation

5.3.6 Sanctions for unauthorized actions

There is an internal regime for disciplinary faults which includes sanctions against personnel. But in case that these unauthorized actions of any person reveal a failure or deficiency of training, sufficient training or retraining will be employed to rectify the shortcoming.

5.3.7 Independent contractor requirements

All personnel subcontracted by StartCom CA to carry out roles related to operating StartCom services is subject to the same requirements as StartCom personnel.

Once the independent contractor completes the work for which it was hired, or the employment is terminated, physical access rights assigned to that contractor are removed as soon as possible and within 24 hours from the time of termination.

5.3.8 Documentation supplied to personnel

All personnel with trusted roles may receive:

- A copy of the Certification Practice Statement

- Documentation which defines the procedures associated with each role including industry standards such as CAB Forum documents

- Operational and technical documentation.

5.4 Audit logging procedures

5.4.1 Events, systems and audit logs

Events and audit logs are produced on ongoing basis and reviewed constantly. System reports are produced on a regular basis and reviewed by the StartCom management. Records are produced on hardware and software introduction and/or modifications and/or maintenance.

5.4.2 Forms of records

The StartCom Certification Authority retains records in electronic or in paper-based format for a period detailed in section Records Retention Period below. The StartCom Certification Authority may require subscribers to submit appropriate documentation in support of a certificate application. This may include personal identity documents, corporate and organizational records including tax, registry and good standing, phone numbers, financial records and records obtained from third parties.

5.4.3 Types of records

All accesses to the on-line and off-line systems and actions are logged as events including but not limited to remote IP addresses, identity, role, user agent, type of event, type of action, description, date and time. Security related events are additionally recorded with an issues tracking tool. Critical events are logged in a special report.

5.4.4 Vulnerability and risk assessments

A vulnerability is a weakness in the organization or in an information system that might be exploited by a threat, with the possibility of causing harm to assets. In order to mitigate the risk or possibility of causing harm to assets, StartCom performs regular vulnerability and risk assessments.

StartCom's Security Program includes regular risk assessments that:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any data or processes.

- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal data and certificate issuance processes.

- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the StartCom Certification Authority has in place to control such risks.

- Based on the Risk Assessment, StartCom implements and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the data and processes, as well as the complexity and scope of the activities of the StartCom Certification Authority.

- The Security Plan includes administrative, organizational, technical and physical safeguards appropriate to the size, complexity, nature, and scope of the StartCom’s business.

- The Security Plan also takes into account the available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 Records archival

5.5.1 Type of records archived

StartCom may archive the following information:
- Audit logs as specified in the previous section
- Certificate application information
- Documentation supporting a Certificate application
- Certificate lifecycle information

5.5.2 Retention period

The StartCom Certification Authority retains the records of the issued certificates and the associated documentation for no less than seven (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.

5.5.3 Protection of archive

Archives and other materials of critical system data are stored in a secure manner at a off-site facility of the StartCom Certification Authority infrastructure.

Access to this archive is restricted to authorized personnel only.

5.5.4 Archive backup procedures

There is a security policy and contingency plan that define the criteria and strategies for action should an incident occur. The design of the strategy for action in the case of incidents is based on the corresponding assets inventory and risk analysis.

5.5.5 Requirements for time-stamping of records

The information systems used by StartCom ensure that a record is kept at the exact time each logged event occurs. That exact time comes from a reliable time source for the date and time.

5.5.6 Archive system

The archive collection system is both internal and external, located at StartCom´s facilities and at the facilities of the entities taking part in rendering of services

5.5.7 Procedures to obtain and verify archive information

Access to this information is limited to authorised personnel only and is therefore protected in accordance with sections 5 and 6 of this Certification Practice Statement.

5.6 Key changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, the StartCom Certification Authority ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs. A new CA signing key pair is commissioned and all subsequently issued certificates and CRL's are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in this policy.

5.7 Compromise and disaster recovery

5.7.1 Incident management procedure

All incidents are reported for investigation. The reporter of an incident has to document the incident details to help with incident assessment, investigation, solution, and future operational changes.

The steps to manage the incident are as follows:

- Report incident
- Managing the incident
- Solution provided
- Improvements

Once the incident is reported, an initial assessment is needed. Next, a containment strategy is chosen and implemented. After an incident has been contained, eradication is necessary to eliminate components of the incident.

StartCom has an incident response program and a contingency plan that describe all the actions carried out, including personnel, to solve an incident, whether intentional or accidental.

The main objectives are:

- To maximise the effectiveness of recovery operations
- Identify the activities, resources and procedures needed
- Assign responsibilities to designated personnel.
- Ensure coordination.

5.7.2 Software or data corrupted action plan

When an incident compromises the StartCom computing resources, software, or data, then will investigate the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise, StartCom reserves the right to revoke affected certificates, to revoke entity keys, to provide new public keys to users, and to recertify subjects if necessary.

5.7.3 CA private key compromise

In the event that a StartCom Certification Authority private key is suspected to have been compromised, StartCom management will immediately convene an emergency response to assess the situation to determine the degree and scope of the incident and take appropriate actions. Those include collection of information related to the incident, investigation, informing law enforcement and other interested parties, further prevention and short term corrections, compiling and issuing of a critical events report. In case it was determined that a CA private key was compromised, the affected key shall be revoked (where possible) and a replacement issued after appropriate solutions are implemented to prevent recurrence.

The CA root private key must be stored in encrypted form in different safety vaults, divided into two external media devices and protected by a token and a PIN number. Only both external devices may recreate the CA root private key, which is needed for signing actions such as issuance of Intermediate CA certificates and Certificate Revocation Lists. Strict dual control is implemented for the handling of the CA root keys and controls are in place to prevent compromise of the CA root keys.

5.7.4 Business continuity after a disaster

Recovery of the CA infrastructure and/or relocation plans are maintained and shall be possible within 48 hours in case of a disaster.

The operation of the CA will be suspended until the disaster recovery procedure has been finalised and secure operations are re-established at the primary site location or an alternative facility.

This is detailed in the business contingency and continuity plan.

5.8 CA or RA termination

StartCom has a termination plan which specifies the procedure to carry out.

StartCom shall continue its CA operations for one year (365 days) in case of the termination of the StartCom Certification Authority, 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 Certification Authority shall be notified of impending changes, including termination, three months (90 days) before the changes will take effect and before officially published.

StartCom will notify its customers prior to the termination of its operations and all third parties with which there´s any relationship, contractual or not.

For the RA termination and after the RA ceases to perform its operations, it shall transfer to StartCom any records it is required to retain; any other information will be cancelled and destroyed.

6. Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

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.

StartCom's CA key pairs are generated on a FIPS-140 approved Hardware Security Module (HSM).

The StartCom Certification Authority 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 must be used. The computer system utilizes a real hardware random number generator for entropy seeding. The resulting private and public keys and certificate revocation lists must be then stored in removable devices and/or security modules according to the defined procedures.

6.1.2 Private key delivered to subscriber

StartCom may generate subscriber keys for code signing certificates so when subscriber keys are generated on StartCom's servers, they are delivered to the subscriber over a shipping system with the hardware device in which have been generated.

6.1.3 CA public keys deliver

As indicated in section 2 of this document.

6.1.4 Key usages

StartCom certificates are based on X.509v3 standard and are for general purpose and may be used without restriction on geographical area or industry. StartCom certificates include key usage extension fields to specify the purposes for which the certificate may be used and to technically limit the functionality of the certificate.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic modules standards

StartCom stores the private keys of the root CA and Intermediate CA certificates in Hardware Security Modules (HSM) FIPS 140-2 Level 3 certified devices or higher, suitable for the signing of Subscriber Certificates and the on-line Certificate Revocation Lists. For recovery and archival purpose, the private keys of the Intermediate CA certificates shall be also stored off-line according to the same procedure as the CA root key.

The signing of CA Root and Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer of StartCom and attendance of at least one witness.

The signing of subscriber certificates is strictly and only performed by the Intermediate CA keys which are operating at the on-line equipment. CA private keys shall be archived after expiration of the public key according to the same procedure as the CA root key.

6.2.2 Private key (n out of m) multi-person control

The use of CA private keys requires the approval of at least two persons.

6.2.3 Private key escrow

No stipulation

6.2.4 Private key backup

Backup copies of CA Private Keys and activation data are stored on-site in separate safety vaults accessible only by trusted personnel. Another backup copy of the CA root key(s) is stored off-site.

There is a procedure for the recovery of cryptographic module keys of the CA (root or subordinate) which can be applied in the case of contingency.

6.2.5 Private key archival

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration.

6.2.6 Transfer of the private key into or from a cryptographic module

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

6.2.7 Private key storage on cryptographic modules

In the CA root key ceremony document is described the processes for generating the private key and the use of the cryptographic module.

Private Keys are generated and stored inside the StartCom's HSMs, which have been certified to at least FIPS 140-2 Level 3.

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment.

6.2.8 Method of activating private key

The Root CA and subordinate CA keys are activated by a process that requires the simultaneous use of n out of m cryptographic tokens.

Private keys are activated in accordance with the specifications of the cryptographic module and remain active until deactivated.

6.2.9 Method of deactivating private key

CA keys are deactivated when the session has no activity for a time.

6.2.10 Method of destroying private key

Destroying a private key means the destruction of all active keys, both backed-up and stored. Destroying a private key may comprise of removing it from the HSM or removing it from the active backup set and can also conduct to the destroy of the HSM itself.

6.2.11 Cryptographic module rating

See section 6.2.1 of this document.

6.3 Other aspects of key pair management

6.3.1 Public key archival

As per section 5.5 of this document.

6.3.2 Certificate operational periods and key pair usage periods

Certificate validity for CA root certificates up to 25 years.
Certificate validity for intermediate CA certificates is usually up to

the CA root validity period except for 2 specific intermediate CAs for code signing certificates and s/mime certificates.

Certificate validity period for Class 1, Class 2 and Class 4 levels end user certificates is 2 years.
Certificate validity period for Class 3 level end user certificates is 3 years, except for SSL/TLS certificates which is 2 years.

Certificate validity for OCSP Responder is 2 days.

6.4 Activation data

All parties must use sufficient and reasonable measures to protect its private keys and other material including passwords where necessary. Private keys generated by the StartCom provided tools are AES encrypted and a password containing letters and numbers with at least ten chars must be provided by the user. Certificate Authority keys are handled according to the section 6.1 and other provisions within this policy.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

StartCom has a list of control that ensures the integrity and security of its computer systems for their different components, such as

- Maintaining Root CA Systems in a high security zone and in an offline state or air-gapped from other networks; and issuing CA systems in secure zones;

- Configuring, maintaining and reviewing all issuing systems, Certificate Management Systems (CMS), security systems, etc.;

- Undergoing penetration tests on a periodic basis and after significant infrastructure or application upgrades;

- Access control for granting administration access to the Certificate Managament Systems (CMS) only to persons acting in trusted roles

6.5.2 Computer security rating

No stipulation.

6.6 Lifecycle technical controls

6.6.1 System development controls

Development of the CA related infrastructures, hardware, libraries, programs, protective programs are performed by personnel with the appropriate knowledge and training. Changes to configuration files and settings, sources, binaries and hardware components must be reviewed and approved by the management. Modifications to the processes and certificates are tested for eventual flaws. Maintenance and other activities on hardware are logged accordingly, monitored and recorded.

6.6.2 Security management checks

StartCom monitors all operational systems and applications to ensure they retain their integrity and remain configured securely according to StartCom's Security Policy.

6.6.3 Life-cycle security controls

No stipulation

6.7 Network security controls

StartCom has implemented reasonable safeguards and controls to prevent unauthorized access to the various systems and devices that comprise the CA infrastructure and to various degrees depending on the sensitivity of the function. The StartCom Root certificates are strictly kept offline and protected by various means.

The CA root key(s) are kept off-line and brought online only when necessary to sign intermediate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

6.8 Timestamping

StartCom provides a RFC 3161 compliant time-stamping utility that is synchronized using the Network Time Protocol (NTP) and updated at least once every 24 hours. The time-stamping service is available at the internet address **http://tsa.startssl.com/rfc3161**

7. Certificate, CRL and OCSP profiles

7.1 Certificate profile

The StartCom Certification Authority uses the standard X.509, version 3 to construct digital certificates for use within the StartCom PKI. X.509 allows a CA to add certain certificate extensions to the basic certificate structure. The StartCom Certification Authority uses a number of certificate extensions for the purposes intended by X.509 version 3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1.1 Class 1

1) Client (Authentication and S/MIME) certificates

CN = Validated email address
E = Validated email address

Certificate is valid for 2 years.

2) SSL/TLS server certificates

CN = Validated domain name

Subject Alt Name extension is not critical and MUST contain the CN field value in addition of other supported hostnames.

Certificate is valid for 2 years.

7.1.2 Class 2

1) Client (Authentication and S/MIME) certificates

CN = Common Name
E = Validated email address
CN = First and last name
SN = Validated Surname
G = validated Given Name
L = Locality
ST = State, administrative or geographical region
C = Country

Certificate is valid for 2 years.

2) SSL/TLS server certificates

CN = Validated domain name

SN = Validated Surname
G = validated Given name
L = Locality
ST = State, administrative or geographical region
C = Country

Subject Alt Name extension is not critical and MUST contain the CN field value in addition of other supported hostnames.

Certificate is valid for 2 years.

3) Object Code Signing certificates

CN = First and last name, Common Name
O = Organization
L = Locality
ST = State, administrative or geographical region
C = Country

Certificate is valid for 2 years.

7.1.3 Class 3

1) Client (Authentication and S/MIME) certificates

E = Validated email address
CN = First and last name, Common Name
O = Validated organization name
L = Locality
ST = State, administrative or geographical region
C = Country

Certificate is valid for 3 years.

If the subscriber identity is validated by the organization, not by StartCom, then the certificate will add an additional description.

E = Validated email address
CN = First and last name
Description = This employee certificate Common Name is validated by this Organization
O = Validated organization name
L = Locality
ST = State, administrative or geographical region
C = Country

2) SSL/TLS server certificates

```
   CN = Validated domain name (www.domain.com)
   O  = Validated organization name
   L  = Locality
  ST  = State, administrative or geographical region
   C  = Country

  Subject Alt Name extension is not critical and MUST
  contain the CN field value in addition of other
  supported hostnames.

  Certificate is valid for 2 years

3) Object Code Signing certificates

   CN = Validated organization name
   O  = Validated organization name
   L  = Locality
  ST  = State, administrative or geographical region
   C  = Country

Certificate is valid for 3 years.
```

7.1.4 Class 4 extended validation

```
1) SSL/TLS server certificates

   CN = Validated domain name (www.domain.com)
   O  = Validated organization name
   L  = Locality
  ST  = State, administrative or geographical region
   C  = Country
   OID 2.5.4.5   = Serial or registration number
   OID 2.5.4.15  = Business Category (This field MUST
   contain one of the following strings: "Private
   Organization", "Government Entity", "Business Entity",
   or "Non-Commercial Entity" depending upon whether the
   Subject qualifies under the terms of the EV
   Guidelines.)
   OID 2.5.4.9   = Street address (optional)
   OID 2.5.4.17  = Postal or zip code (optional)
   OID 1.3.6.1.4.1.311.60.2.1.1 = Locality of
   incorporation (optional)
   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

   Subject Alt Name extension is not critical and MUST
   contain the CN field value in addition of other
   supported hostnames.

   Certificate is valid for 2 years.
```

7.1.5 Intermediate CA class 1-4 validation certificates

CN = StartCom [EV|BR|CC(2)|CS(2)] ICA
OU = Organizational Unit
O = Organization
C = Country

For StartPKI service, the Intermediate CA certificate will add an OU field to declare this intermediate CA is hosted in StartCom PKI facility, controlled by StartCom, just used for this organization:

CN = StartPKI Customer name [Server | Client] CA
OU = Controlled by StartCom exclusively for this Organization
O = Organization
C = Country

This certificate may be valid up to 15 years.

7.2 Other certificate attributes

Version Number

X.509 v3 for CA and subscriber certificates (populate version field with integer “2”)
X.509 v2 for CRL certificates (populate version field with integer “1”)

Serial Number

Unique value
Key Attributes

Key length

2048 bits or higher for subscriber certificates
RSA 4096 bits for CA certificates G3 and CS
ECC 384 bits for CA certificate ECC

Hash Algorithm

SHA256 minimum

Validity

Start: MM/DD/YYYY hh:mm:ss GMT
End: MM/DD/YYYY hh:mm:ss GMT

7.3 Certificate extensions

7.3.1 Subscriber S/MIME client certificates

```
Basic Constraint: CA:FALSE
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
Subject Alternative Name Extension: email: Email Address
Authority Info Access: Access Method (1.3.6.1.5.5.7.48.2),OCSP URL
Authority Key Identifier: Key ID
Certificate Policies: Policy Identifier (1.3.6.1.4.1.23223.2.X.X)
```

7.3.2 Subscriber SSL/TLS server certificates

```
Basic Constraint: CA:FALSE
Key Usage: Digital Signature, Key Encipherment
Extended Key Usage: Client Authentication (1.3.6.1.5.5.7.3.2)
      Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Key Identifier: Hash
CRL Distribution Points: URL
Subject Alternative Name Extension:
      dnsName: Domain names
Authority Info Access: Access Method (1.3.6.1.5.5.7.48.2),OCSP URL
Authority Key Identifier: Key ID, Certificate Issuer
Certificate Policies:
 Policy Identifier 1.3.6.1.4.1.23223.1.1.X or 1.3.6.1.4.1.23223.1.2.X
 CAB Forum Baseline Requirements Policy Identifier 2.23.140.1.2.X
 EV SSL Certificate Policy OIDs: 1.3.6.1.4.1.23223.1.1.1 and
                 2.23.140.1.1 as per CAB Forum
```

7.3.3 Code signing certificates

```
Basic Constraint: CA:FALSE
Key Usage (Critical): Digital Signature
Extended Key Usage (Critical):
      Code Signing (1.3.6.1.5.5.7.3.3)
      Kernel Mode (1.3.6.1.4.1.311.61.1.1) [Class 3 only]
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
Certificate Policies:
      Policy Identifier 1.3.6.1.4.1.23223.3.X.X or
1.3.6.1.4.1.23223.1.3.1
      Baseline Requirements Policy Identifier 2.23.140.1.4.1
```

7.3.4 Intermediate certificates

```
Basic Constraint (Critical): CA:TRUE
Key Usage: Certificate Signing, CRL Signing
Subject Key Identifier: Hash
Authority Key Identifier: Key ID, Certificate Issuer
Certificate Policies:
      Any Policy (2.5.29.32.0)

      Except: CS with “code signing” (2.23.140.1.4.1)
```

7.3.5 Time Stamping Authority (TSA) certificate

```
Basic Constraint: CA:FALSE
Key Usage (Critical):
Digital Signature
Non Repudiation
Extended Key Usage (Critical):
Time Stamping
```

7.4 CRL profile

```
Version: v2
Signature Algorithm: SHA2 with RSA encryption
Issuer:           Identification of the CA issuing the CRL
Last Update:      Time of CRL issue
Next Update:      Time of next CRL issue (48 hours)

Revoked certificates: Listing of information for revoked certificates

CRLs are updated at least every 12 hours or upon adding of a new
entry, e.g. every time a certificate is revoked. However the next
update entry in the CRL is set to 48 hours.
```

7.5 OCSP profile

```
Online Certificate Status Protocol responders conforms to RFC 6960.
Basic Constraint: critical, CA:FALSE
Key Usage: Digital Signature , Key Encipherment , Key Agreement
Extended Key Usage: OCSP Signing , No Check
```

8. Compliance audit and other assessment

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 Certification Authority 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

8.1 Audit frequency

The audit mandates that the period during which a CA issues Certificates be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

8.2 Auditors qualification

The audit is performed by a qualified auditor with the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in a WebTrust for Certification Authorities v2.0;
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ETSI EN 319 403
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Auditor´s relationship to audited entity

The auditor is independent of StartCom, and does not have a financial interest, business relationship, or course of dealing that would create a conflict of interest or create a significant bias (for or against).

8.4 Topics covered by the audit

The topics covered by the compliance annual audit include but are not limited to the following:

- PKI processes, key and certificate lifecycle management
- Business practices disclosures, CPS
- Information systems, CA environment control
- Data centre infrastructure and security
- Documentation

8.5 Actions taken as a result of deficiencies

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 Certification Authority 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.

8.6 Communication of results

StartCom will make the audit report available to the public, but is not required to make publicly available any general audit finding that does not affect the overall audit opinion.

9. Other business and legal matters

9.1 Fees

StartCom and the StartCom Certification Authority 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 access to certificate status information by relying parties.

StartCom publishes clearly on its 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 Certification Authority reserves the 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 Certification Authority are subject to changes and at the sole discretion of StartCom and the StartCom Certification Authority.

9.2 Financial responsibility

StartCom's operations related to the issuing of digital certificates are covered by a Professional Liability/Errors & Omissions insurance with policy limits of at least US$ 5 million in coverage and include coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining digital certificates, and (ii) claims for damages arising out of un intentional infringement of any intellectual property right of any third party (excluding patent, including copyright and/or trademark infringment), and invasion of privacy and advertising injury.

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 were issued according to the EV guidelines.

Certificates issued in accordance to this policy, excluding EV Certificates, are treated according Certificate Insured Warranty below.

9.3 Confidentiality of business information

All information about an individual and/or organization and/or other entity that is not publicly available or published in the contents of a certificate or CRL is treated as private information. StartCom protects such private information using appropriate safeguards and reasonable controls.

9.4 Privacy of personal information

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 information shall not be used without the consent of the party to whom that information applies beyond the tasks the StartCom Certification Authority has to perform for successful validation and verification purpose.

The StartCom Certification Authority 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 Certification Authority shall be entitled to disclose private information to law officials without penalty.

9.5 Intelectual property rights

9.5.1 Copyright and ownership of certificates

Digital certificates which are the result of the operations of the StartCom Certification Authority, are at any given time and remain during their whole life-time the property of the StartCom Certification Authority. Ownership of digital certificates issued by and through the operations of the StartCom Certification Authority 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 Certification Authority 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 Certification Authority at all times and all rights are reserved.

9.6 Representations and warranties

9.6.1 Displaying liability limitations and warranty disclaimers

StartCom certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply. Subscribers must agree to StartCom's Terms & Conditions before signing-up for a certificate.

9.7 Disclaimers of warranties

In case of erroneous issuance of a digital certificate that resulted in a loss to a relying party, relying parties may be eligible under the certificate warranty to receive up to US$ 10,000 per incident (in respect to the USA and Canada this is up to US$ 25,000 per incident). Except to the extent of willful misconduct, the liability of StartCom is limited to the negligent issuance of certificates. The cumulative maximum liability of StartCom to all applicants, subscribers and relying parties for each certificate cumulative is set to US$ 10,000 (for USA and Canada US$ 25,000).

Beyond the coverage of the certificate insured warranty 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.

9.8 Limitations of 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 Certification Authority 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.

9.9 Indemnities

Subscribers of all kind shall 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 including reasonable attorney's fees, related to any misrepresentation or omission of material fact by subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional;
Subscriber's breach of the Subscriber Obligations, this CPS, or applicable law;
Compromise or unauthorized use of a certificate or private key caused by the subscriber's negligence or intentional acts and/or misuse of the certificate or private Key by the subscriber.

9.10 Term and termination

This CP/CPS and any amendments to it are effective from the moment of publication at the online repository and remain in effect until replaced with a newer version.

9.11 Individual notices and communications with participants

Communications are generally done either by email, via the web site interfaces or via registered postal mail or courier services. Postal mail must be acknowledged via registered mail.

9.12 Amedments

Amendments and/or addendum may be published at the online repository whenever necessary or an updated version of this CP/CPS published. Controls are in place to authorize amendments and reasonable protections to prevent unauthorized publication.

9.13 Dispute resolution procedures

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 Bilbao, Spain 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 Certification Authority shall be treated according to the applicable legal system and laws.

9.14 Governing law

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 of Spain and the validity of the other terms should not be affected.

Disputes arising in relation to certificates issued according to the 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.

9.15 Compliance with applicable law

StartCom shall first and foremost comply to the various guidelines and requirements set forth by the various software vendors that act as relying parties, guidelines as set forth by the CA/Browser Forum and according to this CP/CPS. StartCom shall meet compliance with the applicable laws while protecting the interests of its subscribers and relying parties to any reasonable extend.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of the StartCom Certification Authority.

9.16.3 Force majeure

THE STARTCOM CERTIFICATION AUTHORITY INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE

LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.17 Other provisions

No stipulation