Certificate Policy for web site certificates

StartCom CA

Version 1.1

Date: July 5, 2017

Table of Contents

1 Introduction

This document includes the *Certificate Policy* for certificates issued by *StartCom* for different types of website authentication certificates.

The purpose of this document is to detail the procedures to validate, issue, revoke, etc. this type of certificates as indicated in the *Certification Practice Statement,* taking into account the specific documents of the *CA/Browser Forum (Baseline Requirements and EV guidelines* for issuing certificates for websites).

Thus, StartCom adheres to the following certification policies:

- Class 1 for Domain Validation SSL Certificates
- Class 2 for Individual Validation SSL Certificates
- Class 3 for Organizational Validation SSL Certificates
- Class 4 or EV for Extended Validation SSL Certificates

StartCom is committed to improve the webPKI security and follows those specific projects such as the Certificate Transparency, CAA, etc.

Note: This document is not following explicitly the RFC 3647 and all the missing sections are covered in the CPS

1.1 Description of certificates

StartCom issues these certificates to enable subscribers to offer added security to their web sites.

As for the type of certificate issued by StartCom,

SSL	DESCRIPTION
Class 1	**DV (Domain Validation)**
Class 2	**IV (Individual Validation)**
Class 3	**OV (Organization Validation)**
Class 4	**EV (Extended Validation)**

The purpose of this type of certificate is to establish data communications in web servers with SSL/TLS.

They enable the exchange of encrypted communication between the user computer and the web server, which host the website, facilitating the keys needed to encrypt the information sent over the Internet.

- *SSL CERTIFICATES*,

  Depending on the validation the certificate can be,

  - *DOMAIN VALIDATION SSL (**DV SSL**), class 1*

    This certificate verifies the ownership of the domain, or right to use it, that hosts the website, providing no information of the individual or organization behind to the Internet browser user.

    The issuance is automatic (there´s no manual review) but when found misleading domain names, suspicious names as per high-risk domains, malware or phishing

detection by Google Safe browsing API and/or 360 phishing tool, etc. the issuance is stopped and then set to manual review. Approximately, about 20-30%.

These certificates are valid for 2 years.

- *INDIVIDUAL VALIDATION SSL (**IV SSL**), class 2*

  This certificate verifies the person, which owns the domain or has the right to use it, which hosts the website, providing a reasonable guarantee to the Internet browser user.

  The issuance is “manual” meaning that all the validations are done manually and when ok, the system issues the certificate.

  These certificates are valid for 2 years.

- *ORGANIZATION VALIDATION SSL (**OV SSL**), class 3*

  This certificate validates the domain ownership, or right to use it, and the organization, providing the Internet browser user with a reasonable guarantee that the website being accessed belongs to the organization identified in the certificate

  The issuance is “manual” meaning that all the validations are done manually and when ok, the system issues the certificate.

  These certificates are valid for 2 years.

- *EXTENDED VALIDATION SSL (**EV SSL**), class 4*

  This certificate validates the domain ownership and the organization, providing the Internet browser user with a robust guarantee that the website being accessed belongs to the organization identified in the certificate.

  The issuance is “manual” meaning that all the validations are done manually and when ok, the system issues the certificate.

  These certificates are valid for 2 years.

1.2 Identification

In order to identify certificates, StartCom has assigned them the following object identifiers (OID).

CERTIFICATE	StartCom OID	CA/B Forum OID
Class 1 (DV SSL)	1.3.6.1.4.1.23223.1.2.3	2.23.140.1.2.1
Class 2 (IV SSL)	1.3.6.1.4.1.23223.1.2.2	2.23.140.1.2.3
Class 3 (OV SSL)	1.3.6.1.4.1.23223.1.2.1	2.23.140.1.2.2
Class 4 (EV SSL)	1.3.6.1.4.1.23223.1.1.1	2.23.140.1.1

1.3 Community and scope of use

The following will be considered **users,**

Certificate applicant, the natural or legal person that applies for (or seeks renewal of) a certificate. Once the certificate is issued, the applicant is referred to as the subscriber.

Certificate subscriber, natural or legal person identified in the certificate.

Scope of use: The certificates will be used in the scope of the competences of the natural or legal persons (or devices) which hold the certificates.

1.4 General provisions

Identification obligations

StartCom checks and verify the identity and any other personal information concerning certificate applicants and subscribers.

StartCom may set a legal instrument, contract or agreement, between the parties for performing the identification obligations in accordance with the indications of the *CA/Browser Forum* documents.

Certificate subscriber obligations

The subscriber's obligations are specified in the Certification Practice Statement´s section 4.1.2 “Subscriber agreement requirements”.

2 Operational steps

2.1 List of required documentation

According to the different type of SSL/TLS certificate types, it´s required the following:

CERTIFICATE	DOCUMENTATION
DV	➢ Application request form duly completed ➢ The applicant shall accept the applicable Terms of Use agreement
IV	All DV plus: ➢ One ID document with photo. ➢ A picture of the applicant holding the ID ➢ Verification method (paypal, phone bill/third party phone directory, a wire transfer, verification letter) ➢ Whois screenshot ➢ Domain authorization letter ➢ McAfee trusted source screenshot
OV	All IV plus: ➢ Proof of the organization's validity/activity, – Original certification provided by the customer, or copy of it – Or a simple note from the correspondent registry ➢ Registry information from a third party, public and reliable, DB ➢ StartCom organization validation subscriber agreement
EV	All OV plus: ➢ EV application subscriber agreement ➢ Legal opinion letter or delegated authorization letter plus evidence of bank account and address ➢ Blacklist checking

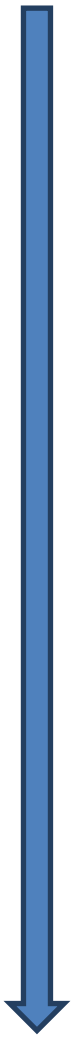
2.2 Validation procedure

Once the applicant submits all the information requested, StartCom CA will start validating all the documentation provided.

There´s an internal document for the manual validations performed by the StartCom CA personnel.

These are the manual steps for validating documentation

DV **IV** **OV** **EV**	➢ Domain validation: Verification that the applicant is entitled to use the domain or subdomain, or is the owner. Using Whois for: • General domains (.com, .net, .org, .info, .biz, etc.) from ICANN or IANA • Specific domains according to local providers The registrant should coincide with the subscriber. If not, the applicant must provide proof of the subscriber's right to use the domains. Screenshots are added to the documentation except for DV
IV **OV** **EV**	➢ Verification of all natural and legal person information • Data Protection Agencies. • Telephone operator pages. • Etc. ➢ In the case of IV and OV SSL certificates wildcards will be allowed in subdomains or host names, provided the applicant entity can prove its legitimate control of the complete domain name. Otherwise, the request will be rejected. For example, *.co.uk or *.local cannot be issued, but *.example.com can be issued to the company Example, Inc. ➢ Verification that the domain does not appear on high risk lists in, • The internal databases of StartCom; or • The McAfee Trusted Source Web Database (http://www.trustedsource.org/); or • The official journals or website for different countries such in the US, EU, China, etc.
EV	➢ Checklist and double validation for documentation verified by, • China office manager • UK office manager



Additionally, there are some other technical validations performed automatically by the system.

These are as follows:

- Domain validation applicable to all SSL certs based on method 2 of the section 3.2.2.4 according to the BRs v 1.4.1. This means automatic checking of the whois.

- Domain validation applicable to class 2, 3 and 4 based on method 5 of the section 3.2.2.4 according to the latest BRs version, as of 1.4.2. This step is performed additionally to method 2 explained above.

- Implementation of the 360 anti-phishing tool plus the Google SAFE browsing API to detect any malware or phishing site at the time of issuance. StartCom, with the help of these tools, maintains a blacklist, whitelist and phishing site list, refusing the issuance for suspicious

domains. Firstly, the 360 tool screens the requests and then compare with the Google API, only if both are ok the certificate is issued.

- This process is also combined with the following tasks to ensure there´s no misleading information in the domain and subdomains:
  - Sensitive words: such as amazon for the company name and user name and domain name, all match + similar + all inclusive, once matched would directly flag in our backend CMS to do the appropriate treatment according to the flag.
  - IDN domain name detection: IDN domain name would directly flag in our backend CMS;
  - Blacklist: managing a list of blacklisted domains;
  - Fraud keywords: such as g00gle; flagging again into our backend CMS and act accordingly

- Implementation of a Primekey Validation/Conformance check tool, which is a tool for running tests on issued certificates or OCSP responses to see that they match the configured criteria.
- Logging all SSL issued certificates in Certificate Transparency log providers.
- Future implementation of the automatic CAA checking at the issuance time according to RFC 6844 expect by August 2017.

2.3 Issue and delivery of the certificate

Once all the validation steps have been done, StartCom processes the CSR provided by the user and generate the certificate accordingly to the class that was requested. This is done automatically according to the workflow.

When the certificate is generated, it is uploaded to the customer area in the CMS and inform the customer and the customer can download the certificate from its account on StartCom's website.

2.4 Fees

StartCom CA charges for the validation of the applicants/subscribers, certificates are free.

The applicable fees are posted on the Startcom CA website at www.startcomca.com

2.5 Verification of certificate

Only if operational defects are due to technical reasons, or to errors made by StartCom in the data contained in the certificate, StartCom will revoke the certificate and issue a new one if needed.

2.6 Revocation of Certificates

Revocation request

The revocation of a certificate can be requested by:

- The subscriber.
- The applicant.
- StartCom is authorized to request the revocation of end-entity subscriber certificates for technical reasons, as indicated in the CPS and in this document.
- Any other entity presenting evidence as indicated in the CPS

Procedure

The procedure is explained in the CPS.
The certificate can be revoked at any time.
There are several channels to revoke a certificate

Causes for revocation

Causes are described in the Certification Practice Statement available at www.startcomca.com

In addition, in the case of certificates regulated in this specific documentation,

1. StartCom informs the subscriber, third parties and Internet browsers with clear instructions on how to report complaints or suspicions of private key compromise, certificate misuse or other kinds of fraud, compromise, misuse or improper behaviour related to certificates.
2. StartCom will investigate problem reports within the 24 hours of their receipt and will decide whether or not to revoke them, considering at least the following criteria:
   - The nature of the case at hand;
   - The number of problem reports received for a certificate or web page.
   - The identity of those making the complaint.
   - Current legislation.

2.7 Renewal of the Certificate

To renew a certificate the applicant must follow the certificate issuance process established, taking into account that the validations are valid for 12 months.

In the internal document for validations is explained how a certificate can be renewed

2.8 Audits and incidents

Criteria referring to audits and analysis of incidents,

- ☐ Ways in which to present complaints or suggestions,

  A complaint and suggestion form is available at www.startcomca.com/index/contactus

- ☐ Internal registry of incidents.

  The StartCom management manages security incidents.

- ☐ The annual auditing plan is performed in accordance with Webtrust criteria.
- ☐ StartCom CA may report phishing incidents to the Anti-Phishing Working Group website (www.apwg.org) according to what´s indicated in http://www.apwg.org/report-phishing/

3 Change management

The StartCom BoD is in charge and will approve all the changes and modifications made to this document as stated in the CPS.

Similarly to the CPS, StartCom will create an updated document with all the changes made from previous versions.

This documentation is available at www.startcomca.com

4Certificate profiles

4.1 DV SSL certificate

Field/extension	Optional/Critical	Content
Version		Version 3
serialNumber		Unique random number with 64 bits
Signature algorithm		Sha256WithRSAencryption
Issuer		Note: Same as subject field of the issuing CA
Validity		2 years
Subject		
CN OU C	 Optional Optional	DNS domain or IP address Organizational Unit, i.e. Department Country
subjectPublicKeyInfo		RSA 2048 bits minimum
extensions		
Subject Alternative Name		SubjectAltCN =
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		True
Authority Key Identifier		True Note: include only the KeyIdentifier field
Basic Constraints		Subject Type=End Entity,

		Path Length Constraint=None
Certificate Policies Policy Identifier Policy Identifier cpsURI		 1.3.6.1.4.1.23223.1.2.3 2.23.140.1.2.1 http://www.startcomca.com/policy
Authority Information Access OCS AIA		 http://ocsp.startcomca.com http://aia.startcomca.com/certs/sca.server1.crt
CRL Distribution Points		http://crl.startcomca.com/sca-server1.crl
Key Usage	Critical	Digital Signature, Key Encipherment

4.2 IV SSL certificate

Field/extension	Optional/Critical	Content
Version		Version 3
serialNumber		Unique random number with 64 bits
Signature algorithm		Sha256WithRSAencryption
Issuer		Note: Same as subject field of the issuing CA
Validity		2 years
Subject		
CN OU O or GivenName&surname STREET L	 Optional Optional	DNS domain Organizational Unit, i.e. Department Organization or name&surname Address Locality, i.e. City

ST C PostalCode	Optional	State, i.e. Province Country Postal Code
subjectPublicKeyInfo		RSA 2048 bits minimum
extensions		
Subject Alternative Name		SubjectAltCN =
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		True
Authority Key Identifier		True Note: include only the KeyIdentifier field
Basic Constraints		Subject Type=End Entity, Path Length Constraint=None
Certificate Policies Policy Identifier Policy Identifier cpsURI		 1.3.6.1.4.1.23223.1.2.2 2.23.140.1.2.3 http://www.startcomca.com/policy
Authority Information Access OCS AIA		 http://ocsp.startcomca.com http://aia.startcomca.com/certs/sca.server2.crt
CRL Distribution Points		http://crl.startcomca.com/sca-server2.crl
Key Usage	Critical	Digital Signature, Key Encipherment

4.3 OV SSL certificate

Field/extension	Optional/Critical	Content
Version		Version 3
serialNumber		Unique random number with 64 bits
Signature algorithm		Sha256WithRSAencryption
Issuer		Note: Same as subject field of the issuing CA
Validity		2 years
Subject		
CN OU O STREET L ST C PostalCode SERIALNUMBER	 Optional Optional Optional Optional	DNS domain or IP address Organizational Unit, i.e. Department Organization Address Locality, i.e. City State, i.e. Province Country Postal Code Example: Company ID
subjectPublicKeyInfo		RSA 2048 bits minimum
extensions		
Subject Alternative Name		SubjectAltCN =
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		True

Authority Key Identifier		True Note: include only the KeyIdentifier field
Basic Constraints		Subject Type=End Entity, Path Length Constraint=None
Certificate Policies Policy Identifier Policy Identifier cpsURI		 1.3.6.1.4.1.23223.1.2.1 2.23.140.1.2.2 http://www.startcomca.com/policy
Authority Information Access OCS AIA		 http://ocsp.startcomca.com http://aia.startcomca.com/certs/sca.server3.crt
CRL Distribution Points		http://crl.startcomca.com/sca-server3.crl
Key Usage	Critical	Digital Signature, Key Encipherment

4.4 EV SSL certificate

Field/extension	Optional/Critical	Content
Version		Version 3
serialNumber		Unique random number with 64 bits
Signature algorithm		Sha256WithRSAencryption
Issuer		Note: Same as subject field of the issuing CA, i.e.: CN = StartCom EV SSL ICA OU = StartCom Certification Authority O = StartCom CA C = ES
Validity		2 years
Subject		
CN OU O STREET L ST C PostalCode SERIALNUMBER Business Category	 Optional Optional Optional	DNS domain Organizational Unit, i.e. Department Organization Address Locality, i.e. City State, i.e. Province Country Postal Code Example: Company ID [OID: 2.5.4.15] Possible values: - Private Organization - Government Entity - Business Entity

		- Non-comercial entity
JurisdictionOfIncorporationLocalityName JurisdictionOfIncorporationStateorProvinceName JurisdictionOfIncorporationCountryName	Optional Optional	[OID: 1.3.6.1.4.1.311.60.2.1.1] [OID: 1.3.6.1.4.1.311.60.2.1.2] [OID: 1.3.6.1.4.1.311.60.2.1.3]
subjectPublicKeyInfo		RSA 2048 bits minimum
extensions		
Subject Alternative Name		SubjectAltCN =
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		True
Authority Key Identifier		True Note: include only the KeyIdentifier field
Basic Constraints		Subject Type=End Entity, Path Length Constraint=None
Certificate Policies Policy Identifier Policy Identifier cpsURI		1.3.6.1.4.1.23223.1.1.1 2.23.140.1.1 http://www.startcomca.com/policy
Authority Information Access OCS AIA		http://ocsp.startcomca.com http://aia.startcomca.com/certs/sca.server4.crt
CRL Distribution Points		http://crl.startcomca.com/sca-server4.crl
Key Usage	Critical	Digital Signature, Key Encipherment