# StartCom Subscriber Agreement for Code Signing Certificate

## Instructions:

The following documents are required to be completed and submitted to StartCom before requesting for the code signing certificate from StartCom:

1. A StartCom Subscriber Agreement for Code Signing Certificate signed by the applicant.

Print and complete the documents. Send them by -

- Uploading them to your StartSSL account
- Digitally signed email with attachment to certmaster@startssl.com

TO BE PRINTED ON ORGANIZATION'S LETTERHEAD
---------- BEGIN SUBSCRIBER AGREEMENT LETTER CONTENT ----------

**To: StartCom Certification Authority**

## StartCom Subscriber Agreement for Code Signing Certificate

I _____<Full Name> am the Applicant intends to request for Individual Validation Certificates including code singing certificate - which is the digital equivalent of a personal stamp or seal - with the StartCom Certification Authority on behalf of myself('Applicant').

I have read and confirm the Applicant's acceptance and acceptance by myself of all obligations placed upon me and the Applicant by this Agreement and the StartCom Certification Authority Policy & Practice Statements(hereinafter referred to as Policy), including all Individual Validation terms and conditions on behalf of Myself. The Applicant acknowledges and accepts that the CA may modify the Agreement or Policy when necessary to comply with any changes in the *Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* or the *Baseline Requirements* or other regulations formulated by CA/Browser Forum.

The Applicant shall provide accurate and complete information at all times in connection with the issuance of a Certificate, including in the Certificate Request and as otherwise requested by the CA. Further the Applicant is aware that the loss or misuse of this identity in form of a digital certificate can result in great harm to the Applicant.

The Applicant represent that it is capable of generating and operating any device storing private keys in a secure manner described as in the Appendix hereto. The Applicant must maintain sole control of, keep confidential, and properly protect, at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token).

The Applicant shall not use a private key which has been used or to be used in other certificate request for certificate request from StartCom.

The Applicant shall review and verify the Certificate contents for accuracy before using the Certificate and use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Agreement or the Policy. And adequate network and other security controls shall be in place to protect against misuse of the Private Key and that StartCom will revoke the Certificate immediately without requiring prior notification if there is unauthorized access to the Private Keys or there is misuse of the certificate, including but not limited to signing of malware.

The Applicant shall promptly cease using a Certificate and its associated Private Key and promptly request that the CA revoke the Certificate if the Subscriber believes that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code.

The Applicant acknowledges and accepts that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the Agreement or the CPS. And the CA is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.)

The applicant will promptly cease using the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of the Certificate.

The Applicant agrees to indemnify StartCom and its directors, officers, agents, employees, contractors, partners, affiliates, or subsidiaries (collectively, the 'Indemnified Parties') and hold the Indemnified Parties harmless from and against any losses, costs, damages, and fees (including reasonable attorney's fees).

Regards,

Full Name: _____

Place: _____

Signature: _____

Date: _____

## Appendix

Please confirm by which option below that the applicant is capable of using to generate and protect the Code Signing Certificate private keys by marking in the brackets before the option. Thanks.

[ ] 1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber's private key protection through a TPM key attestation.

[ ] 2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.

[ ] 3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

Please be informed that if the Applicant is not be able to provide any option for protection above, then StartCom cannot provide a code signing certificate.

---------- END SUBSCRIBER AGREEMENT LETTER CONTENT ----------