SK ID Solutions AS – Certification Practice Statement for SK ID Solutions ROOT G1

Version 1.0

Version and Changes		
Date	**Version**	**Changes**
17.02.2022	1.0	First public version

1. INTRODUCTION

SK ID Solutions AS (SK) was founded on March 26th, 2001. The owners of the limited liability company are AS Swedbank, AS SEB Pank and Telia Eesti AS. The principal activities of SK are offering trust services and related technical solutions. These services guarantee secure and verified electronic communication with public institutions as well as businesses in everyday life.

Inspired by the ETSI EN 319 400 series, SK has divided its documentation into three parts:

- SK PS [1] describes general practices common to all trust services;
- Certification Practice Statements and Time-Stamping Practice Statements describe parts that are specific to each Subordinate CA or Time-Stamping Unit;
- Technical Profiles are in separate documents.

Pursuant to the IETF RFC 3647 [2] this CPS is divided into nine parts. To preserve the outline specified by RFC 3647 [2], section headings that do not apply have the statement **"Not applicable"**. References to SK PS [1] and Certificate Profile documents [3] are included where applicable.

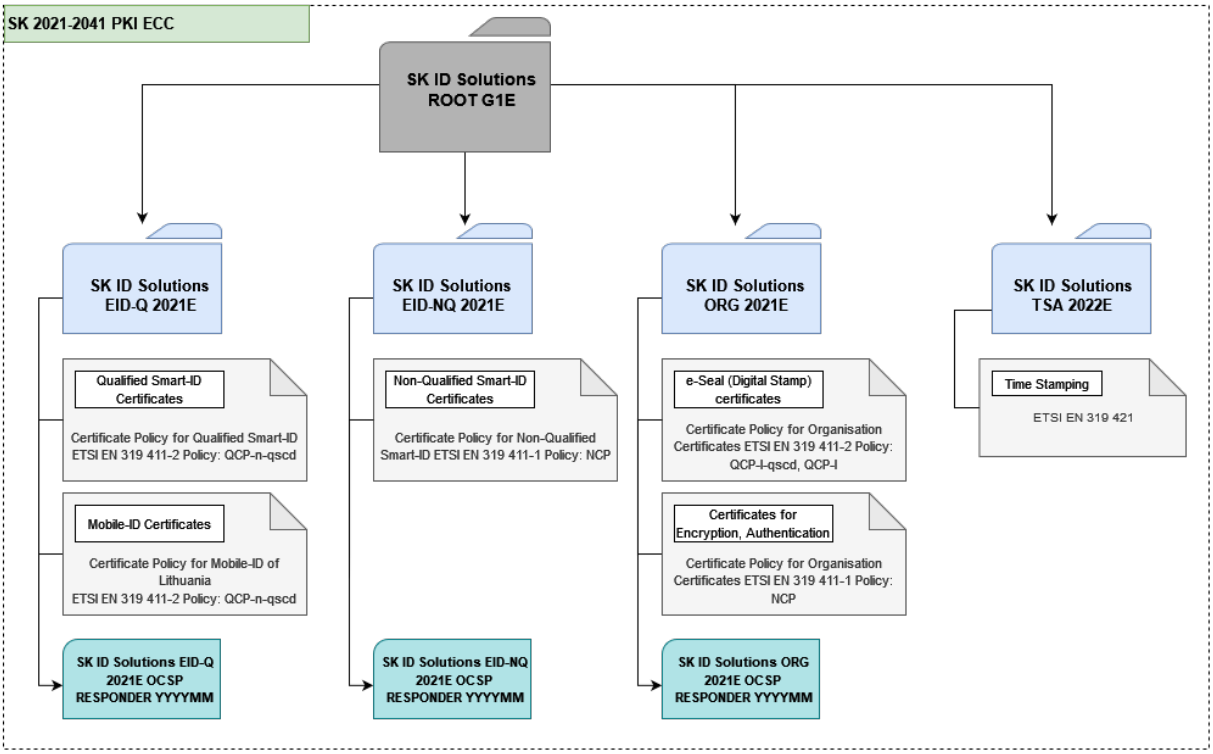
1.1. Overview

This CPS describes the practices used to operate SK ID Solutions ROOT G1 (ROOT G1) to issue intermediate CA certificates.

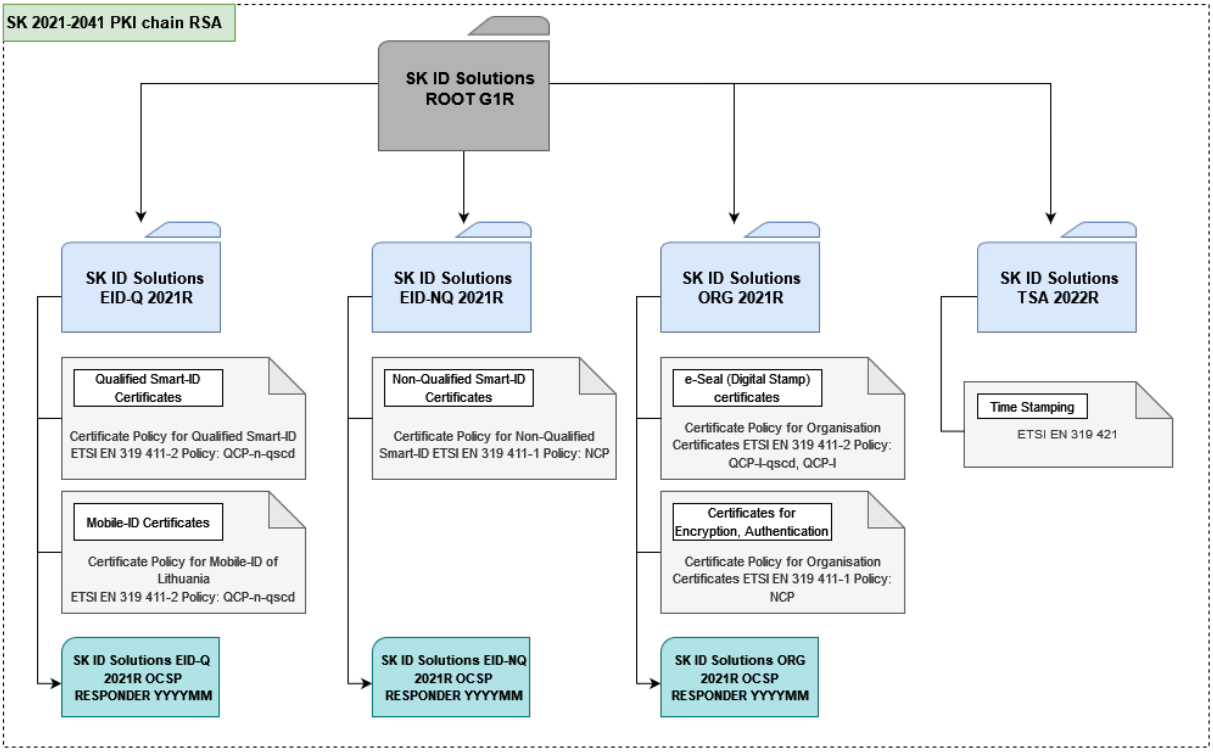
The operation of SK ID Solutions ROOT G1 is compliant to ETSI EN 319 411-2 [8].

Intermediate CA certificates will be issued from two SK ID Solutions ROOT G1 chains – SK ID Solutions ROOT G1E (ECC) and SK ID Solutions ROOT G1R (RSA). End entity certificates will be issued from one CA chain at a time. SK ID Solutions ROOT G1E will be primary and SK ID Solutions ROOT G1R will be secondary CA chain. The relations between SK ID Solutions ROOT G1E and SK ID Solutions ROOT G1R and their subordinate CAs and the CPs are shown on the following figures.

SK ID Solutions ROOT G1E chain, valid 2021-2041:



SK ID Solutions ROOT G1R chain, valid 2021-2041:



1.2. Document Name and Identification

This document is called “SK ID Solutions AS – Certification Practice Statement for SK ID Solutions ROOT G1.”

1.3. PKI Participants

1.3.1. Certification Authorities

SK operates as a CA.

The certification service of SK covers all procedures described in this CPS related to lifecycle of keypairs and certificates.

SK does not use third parties to issue and maintain certificates issued by SK ID Solutions ROOT G1.

SK ID Solutions ROOT G1 is identified by the following certificates:

1) SK ID Solutions ROOT G1E

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
4a:66:8b:d6:e6:e2:0b:71:61:5a:e9:42:22:12:77:fb
Signature Algorithm: sha512ECDSA
Issuer: C=EE, O=SK ID Solutions AS, 2.5.4.97=NTREE-10747013, CN=SK ID Solutions ROOT G1E
Validity
Not Before: Oct 4 2021 11:45:06 UTC
Not After : Oct 4 2041 11:45:06 UTC
Subject: C=EE, O=SK ID Solutions AS, 2.5.4.97=NTREE-10747013, CN=SK ID Solutions ROOT G1E
Subject Public Key Info:
Public Key Algorithm: ECDSA_P521
Public-Key: ECC (521 bit)
04:00:DF:B3:37:44:0D:44:7D:29:2F:AA:33:20:4A:85
48:18:AA:01:2A:15:95:C8:28:8B:6F:9E:A5:0E:9F:53
F8:09:E5:96:F2:4A:73:6D:8D:C7:F1:AA:A8:B7:B1:6F
97:1C:AD:C8:5C:DD:A4:C0:C2:26:CD:6C:7F:3F:B4:B8
66:14:5F:00:93:49:8B:AA:8F:9B:2C:83:9D:72:04:D7
B8:D4:BA:A5:41:70:F6:70:A5:AA:77:72:A4:0D:0F:71
40:DF:FC:20:B3:7A:FF:76:70:47:C9:00:F8:33:68:A1
7F:78:F8:20:3C:BF:00:D9:7A:22:22:36:0F:86:79:D2
29:38:41:47:D8
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid: 86:74:4F:3A:EB:38:F2:B0:A7:EE:ED:B9:85:9B:9D:83:09:45:31:6B
X509v3 Subject Key Identifier:
86:74:4F:3A:EB:38:F2:B0:A7:EE:ED:B9:85:9B:9D:83:09:45:31:6B
X509v3 Key Usage: critical
Certificate Signing, Off-line CRL Signing, CRL Signing
X509v3 Basic Constraints: critical
CA:True, pathlen:none
Signature Algorithm: sha512ECDSA
30:81:87:02:41:7e:a5:82:c3:74:98:ec:1d:ce:e1:bd
6d:1d:94:83:e4:ea:b8:99:2a:bd:cf:0d:ee:be:de:dd
cf:6a:af:94:75:be:0e:1b:0d:f2:cc:9a:31:08:a4:1b
9c:b5:0b:b6:53:7a:c1:e3:ba:c2:ea:41:9f:dd:57:fb
05:fa:41:b0:b2:fe:02:42:00:af:c9:b4:fd:54:b1:62
e4:9b:10:9a:9e:7b:8a:18:e2:07:f0:28:1c:28:85:dd
5b:fc:fb:fd:34:0b:7e:bc:a0:74:93:20:67:94:e3:cc
b3:07:5e:85:f7:80:a4:93:36:90:ae:64:47:9a:98:46
01:cd:df:07:28:b0:e7:29:85:95
-----BEGIN CERTIFICATE-----

MIICtDCCAhagAwIBAgIQSmaL1ubiC3FhWulCIhJ3+zAKBggqhkjOPQQDBDBmMQsw
CQYDVQQGEwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRh
DA5OVFJFRS0xMDc0NzAxMzEhMB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJPT1Qg
RzFFMB4XDTIxMTAwNDExNDUwNloXDTQxMTAwNDExNDUwNlowZjELMAkGA1UEBhMC
RUUxGzAZBgNVBAoMElNLIElEIFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOTlRSRUUt
MTA3NDcwMTMxITAfBgNVBAMMGFNLIElEIFNvbHV0aW9ucyBST09UIEcxRTCBmzAQ
BgcqhkjOPQIBBgUrgQQAIwOBhgAEAN+zN0QNRH0pL6ozIEqFSBiqASoVlcgoi2+e
pQ6fU/gJ5ZbySnNtjcfxqqi3sW+XHK3IXN2kwMImzWx/P7S4ZhRfAJNJi6qPmyyD
nXIE17jUuqVBcPZwpap3cqQND3FA3/wgs3r/dnBHyQD4M2ihf3j4IDy/ANl6IiI2
D4Z50ik4QUfYo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAd
BgNVHQ4EFgQUhnRPOus48rCn7u25hZudgwlFMWswHwYDVR0jBBgwFoAUhnRPOus4
8rCn7u25hZudgwlFMWswCgYIKoZIzj0EAwQDgYsAMIGHAkF+pYLDdJjsHc7hvW0d
lIPk6riZKr3PDe6+3t3Paq+Udb4OGw3yzJoxCKQbnLULtlN6weO6wupBn91X+wX6
QbCy/gJCAK/JtP1UsWLkmxCannuKGOIH8CgcKIXdW/z7/TQLfrygdJMgZ5TjzLMH
XoX3gKSTNpCuZEeamEYBzd8HKLDnKYWV
-----END CERTIFICATE-----

2) SK ID Solutions ROOT G1R

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
74:65:cc:9b:18:4f:0e:ed:61:5a:ea:b5:e6:cf:4b:29
Signature Algorithm: sha384WithRSAEncryption
Issuer: C=EE, O=SK ID Solutions AS, 2.5.4.97=NTREE-10747013, CN=SK ID Solutions ROOT G1R
Validity
Not Before: Oct 4 2021 11:51:17 UTC
Not After : Oct 4 2041 11:51:17 UTC
Subject: C=EE, O=SK ID Solutions AS, 2.5.4.97=NTREE-10747013, CN=SK ID Solutions ROOT G1R
Subject Public Key Info:
Public Key Algorithm: RSA
Public-Key: (4096 bit)
Modulus:
00:be:e6:9d:1c:98:8f:8b:72:77:c8:6f:75:8d:d1:2a
f6:d1:08:36:bb:d2:a5:17:f9:b8:ba:19:5d:3c:d5:8e
34:42:5a:4d:bd:b6:62:07:f4:37:d5:b3:31:3a:e1:cc
67:da:a6:32:4b:49:c8:04:b8:77:72:d7:68:eb:2f:ac
94:f7:91:58:3d:5a:4f:7e:48:9d:3b:d6:93:13:e2:32
9d:7a:51:51:d1:ee:29:20:cd:bc:0f:02:ec:7d:0f:67
df:69:02:c8:e4:db:48:bc:f4:71:9f:11:9d:95:16:dd
89:3c:a9:7d:8e:46:71:6d:9f:fa:2c:70:95:b8:11:60
81:3a:1d:e1:62:52:0a:f0:c1:32:0e:a3:6b:e4:c0:72
ad:9f:44:c3:92:de:6c:36:31:78:ea:9a:d4:a7:ab:79
35:d5:ac:5f:11:99:66:29:b9:71:ae:b8:c7:a7:e6:e8
d9:b4:18:da:17:62:e5:4a:c6:ff:72:15:f8:3e:d6:a9
81:46:4a:2c:75:5f:3e:35:65:a4:19:71:d4:80:0a:71
00:96:a2:b0:7f:be:a4:1e:78:1a:86:cc:b8:a6:94:6e
c5:89:20:35:22:87:58:31:00:a7:71:7a:9c:63:f6:7f
9d:b4:13:48:d9:11:25:de:b1:1d:5c:c2:54:9b:fa:12
a9:56:ea:55:67:6a:4e:a7:27:9b:82:c8:84:e5:56:3d
ff:a0:3c:4e:0e:23:5e:dd:27:35:e3:fb:cf:bb:86:2f
8d:7d:54:f4:db:0d:b8:2e:15:66:24:9c:6a:b4:d2:6e
0a:61:8b:f4:d6:98:59:17:dc:2b:f2:6f:56:9b:04:d2
52:6c:de:d1:ed:1e:00:9f:8f:56:97:6f:2e:37:ce:e1
ee:6b:bb:1f:27:5c:08:5d:14:ae:a9:b5:92:32:eb:c8

ae:d8:d0:0a:46:0f:9b:fa:53:79:11:a4:85:ef:6a:a0
ab:ff:e4:d5:98:10:a2:0e:fb:f0:68:cb:f1:95:9f:8f
a5:43:89:32:c7:18:b5:69:bc:8a:3a:2e:ba:9e:40:78
5a:a7:41:61:73:8d:98:c5:ee:cb:0b:ee:ee:c6:7f:6f
31:b9:65:23:f3:23:89:39:6a:4a:b0:c9:64:81:36:33
e0:6b:ab:a1:8b:11:71:b8:d6:3b:14:db:8e:4f:5a:99
18:87:7c:ca:10:3b:71:23:30:10:aa:dd:f6:54:71:17
e8:9a:07:3d:c6:1b:b4:dd:18:ff:3f:eb:02:90:52:35
91:90:d0:68:2e:47:1f:a2:ad:9e:f3:b9:17:82:0d:aa
04:25:38:83:ee:69:a6:06:95:a0:82:a9:e1:a8:58:6f
d9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid: 95:0D:B7:64:18:C2:A6:9B:66:76:D8:FC:FC:9A:5A:24:BC:28:D6:CD
X509v3 Subject Key Identifier:
95:0D:B7:64:18:C2:A6:9B:66:76:D8:FC:FC:9A:5A:24:BC:28:D6:CD
X509v3 Key Usage: critical
Certificate Signing, Off-line CRL Signing, CRL Signing
X509v3 Basic Constraints: critical
CA:True, pathlen:none
Signature Algorithm: sha384WithRSAEncryption
00:3b:c1:5c:25:ca:ec:10:66:57:41:ab:13:e0:fb:53
37:50:e1:bc:1b:40:06:ff:62:35:1f:2b:11:e4:bd:93
46:d3:8f:86:39:15:9d:a4:19:e7:98:1e:c7:16:dd:2f
5f:c4:cd:fb:d7:c9:e4:6c:24:dd:18:22:57:d9:43:36
6b:0f:96:67:da:4d:2e:3c:0d:52:eb:a6:c5:71:3c:c9
d9:d7:d1:32:d7:ed:4a:33:50:b0:47:ee:82:28:61:42
79:6b:a3:85:4f:f6:5f:27:85:9f:11:3e:d6:5d:aa:48
63:3c:a5:da:b4:37:54:99:e3:a0:72:ea:e6:ee:8f:aa
19:d4:f2:42:78:d6:d8:af:8e:cb:6d:9a:56:d5:27:52
ca:28:ca:db:bf:62:68:3a:fd:fd:13:83:6e:91:aa:e5
2b:fb:c9:d0:20:d6:28:62:21:ce:2b:ac:4b:f5:23:d5
dc:67:43:8b:58:cd:a9:0c:96:78:b7:b2:e3:5c:80:09
7b:6a:d3:12:84:85:0f:d5:58:c3:0d:f7:08:b3:45:7c
45:47:c3:55:71:2e:c8:5b:02:53:61:58:c5:37:93:c1
ce:cd:03:c5:78:ce:ab:4d:29:51:e0:91:4a:09:90:36
89:33:71:0c:ca:c7:32:51:fd:04:89:b0:71:31:4b:7f
b8:32:c6:99:c1:c6:fd:aa:77:7f:23:71:1b:c7:b0:b4
1e:38:93:2d:43:27:a2:d1:e8:1a:2a:da:27:88:92:13
39:4d:d1:eb:62:57:59:df:d8:ba:e8:a7:7b:b2:c1:57
71:48:03:ce:b7:10:23:fc:15:94:22:a7:8e:76:e1:56
7b:0d:c8:1f:d6:e8:5c:dd:22:a6:33:4f:3c:0c:0b:80
58:86:c8:89:43:d0:2e:13:23:c3:26:e7:ad:a7:c4:73
76:0e:7d:cd:d8:22:0b:5c:ea:4c:c9:08:5b:17:b9:29
d9:ee:ff:d4:33:bc:1d:76:95:7c:93:01:2d:71:18:a1
16:b7:b5:cc:dc:cc:e1:3d:98:d8:68:1d:04:1e:b5:dd
a5:de:fd:93:46:0f:f6:0c:58:20:82:c8:49:ad:b4:ad
69:7d:e4:86:e2:61:25:51:e8:bb:e0:89:93:89:57:7f
52:c8:f2:87:6d:10:c4:08:bd:ae:cf:db:34:66:06:64
bb:40:75:ca:bc:14:c2:c2:f8:61:6f:1d:35:1c:3b:22
75:73:1f:f1:28:30:03:55:92:1b:8d:40:38:85:f7:fc
c6:41:7d:ff:e5:f7:17:e6:d2:59:68:3d:ef:cb:d9:98
24:02:79:77:fb:e1:70:63:aa:1d:b2:37:b3:65:b6:ef
e7
-----BEGIN CERTIFICATE-----

MIIFuTCCA6GgAwIBAgIQdGXMmxhPDu1hWuq15s9LKTANBgkqhkiG9w0BAQwFADBm
MQswCQYDVQQGEwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYD
VQRhDA5OVFJFRS0xMDc0NzAxMzEhMB8GA1UEAwwYU0sgSUQgU29sdXRpb25zIFJP
T1QgRzFSMB4XDTIxMTAwNDExNTExN1oXDTQxMTAwNDExNTExN1owZjELMAkGA1UE
BhMCRUUxGzAZBgNVBAoMElNLIElEIFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOTlRS
RUUtMTA3NDcwMTMxITAfBgNVBAMMGFNLIElEIFNvbHV0aW9ucyBST09UIEcxUjCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAL7mnRyYj4tyd8hvdY3RKvbR
CDa70qUX+bi6GV081Y40QlpNvbZiB/Q31bMxOuHMZ9qmMktJyAS4d3LXaOsvrJT3
kVg9Wk9+SJ071pMT4jKdelFR0e4pIM28DwLsfQ9n32kCyOTbSLz0cZ8RnZUW3Yk8
qX2ORnFtn/oscJW4EWCBOh3hYlIK8MEyDqNr5MByrZ9Ew5LebDYxeOqa1KereTXV
rF8RmWYpuXGuuMen5ujZtBjaF2LlSsb/chX4PtapgUZKLHVfPjVlpBlx1IAKcQCW
orB/vqQeeBqGzLimlG7FiSA1IodYMQCncXqcY/Z/nbQTSNkRJd6xHVzCVJv6EqlW
6lVnak6nJ5uCyITlVj3/oDxODiNe3Sc14/vPu4YvjX1U9NsNuC4VZiScarTSbgph
i/TWmFkX3Cvyb1abBNJSbN7R7R4An49Wl28uN87h7mu7HydcCF0Urqm1kjLryK7Y
0ApGD5v6U3kRpIXvaqCr/+TVmBCiDvvwaMvxlZ+PpUOJMscYtWm8ijouup5AeFqn
QWFzjZjF7ssL7u7Gf28xuWUj8yOJOWpKsMlkgTYz4GuroYsRcbjWOxTbjk9amRiH
fMoQO3EjMBCq3fZUcRfomgc9xhu03Rj/P+sCkFI1kZDQaC5HH6KtnvO5F4INqgQl
OIPuaaYGlaCCqeGoWG/ZAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0P
AQH/BAQDAgEGMB0GA1UdDgQWBBSVDbdkGMKmm2Z22Pz8mlokvCjWzTAfBgNVHSME
GDAWgBSVDbdkGMKmm2Z22Pz8mlokvCjWzTANBgkqhkiG9w0BAQwFAAOCAgEAO8Fc
JcrsEGZXQasT4PtTN1DhvBtABv9iNR8rEeS9k0bTj4Y5FZ2kGeeYHscW3S9fxM37
18nkbCTdGCJX2UM2aw+WZ9pNLjwNUuumxXE8ydnX0TLX7UozULBH7oIoYUJ5a6OF
T/ZfJ4WfET7WXapIYzyl2rQ3VJnjoHLq5u6PqhnU8kJ41tivjsttmlbVJ1LKKMrb
v2JoOv39E4NukarlK/vJ0CDWKGIhziusS/Uj1dxnQ4tYzakMlni3suNcgAl7atMS
hIUP1VjDDfcIs0V8RUfDVXEuyFsCU2FYxTeTwc7NA8V4zqtNKVHgkUoJkDaJM3EM
yscyUf0EibBxMUt/uDLGmcHG/ap3fyNxG8ewtB44ky1DJ6LR6Boq2ieIkhM5TdHr
YldZ39i66Kd7ssFXcUgDzrcQl/wVlCKnjnbhVnsNyB/W6FzdIqYzTzwMC4BYhsiJ
Q9AuEyPDJuetp8Rzdg59zdgiC1zqTMkIWxe5Kdnu/9QzvB12lXyTAS1xGKEWt7XM
3MzhPZjYaB0EHrXdpd79k0YP9gxYIILISa20rWl95IbiYSVR6LvgiZOJV39SyPKH
bRDECL2uz9s0ZgZku0B1yrwUwsL4YW8dNRw7InVzH/EoMANVkhuNQDiF9/zGQX3/
5fcX5tJZaD3vy9mYJAJ5d/vhcGOqHbI3s2W27+c=
-----END CERTIFICATE-----

1.3.2. Registration Authorities

Not applicable.

1.3.3. Subscribers

SK is the Subscriber in the context of this CPS.

1.3.4. Relying Parties

A Relying Party is a natural or legal person who takes a decision relying on the certificate issued by SK.

1.3.5. Other Participants

Not applicable.

1.4. Certificate Usage

Only subordinate CAs are issued according to this CPS.

1.5. Policy Administration

1.5.1. Organisation Administering the Document

This CPS is administered by SK.

SK ID Solutions AS

Registry code 10747013

Pärnu mnt 141, 11314 Tallinn

Tel +372 610 1880

Fax +372 610 1881

Email: info@skidsolutions.eu

https://www.skidsolutions.eu/

1.5.2. Contact Person

Head of Trust Services

Email: info@skidsolutions.eu

1.5.3. Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4. CPS Approval Procedures

Amendments which do not change the meaning of the CPS, such as corrections of misspellings, translation and updating of contact details, are documented in the Versions and Changes section of the present document and the fraction part of the document version number is enlarged.

In case of substantial changes, the new CPS version is clearly distinguishable from the previous ones. The new version bears a serial number enlarged by one. The amended CPS along with the enforcement date is published electronically on SK's website.

1.6. Definitions and Acronyms

1.6.1. Terminology

In this CPS the following terms have the following meaning.

Term	Definition
Certification Practice Statement	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the profile and minimum requirements for the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) certificates.
Certification Service	Issuing certificates, managing suspension, termination of suspension, revocation, modification and re-key.
Directory Service	Certificate validity information publication service.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile [3], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Private Key	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	The key pair that may be publicly disclosed by the holder of corresponding private key and that is used by 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.
Relying Party	Entity that relies upon either the information contained within a certificate.
eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [5]
OCSP	Protocol for checking certificate validity
Root CA	Highest level certification authority, whose certificate is bundled with application software and that issues certificates to subordinate CA-s.
SK CA	Certification authority of SK, whose certificate is signed by Root CA or another subordinate CA.
Supervisory body	An institution, designated by Member State to carry out supervision according to eIDAS Regulation [5] over trust services and trust service providers on the territory of Member State.
Trust Service	Described in eIDAS Regulation [5] as an electronic service offered for a fee and that covers - creation, verification and validity confirmation of electronic signatures, electronic seals or electronic time stamps, electronic registration services and certificates related to these services; - creation, verification and validity confirmation of certificates for website authenication - maintaining the certificates related to electronic signatures, stamps or services related to them
Trust Service Provider	Organisation that provides at least one Trust Service

1.6.2. Acronyms

Acronym	Definition
CA	Certification Authority
ROOT G1	SK ID Solutions ROOT G1
CPS	Certification Practice Statement for SK ID Solutions ROOT G1
CRL	Certificate Revocation List
HSM	Hardware Security Module
SK	SK ID Solutions AS, provider of the certification services
SK PS	SK ID Solutions AS Trust Services Practice Statement [1]

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

Refer to clause 2.1 of SK PS [1].

2.2. Publication of Certification Information

Refer to clause 2.2 of SK PS [1].

2.2.1. Publication and Notification Policies

This CPS is published on SK's website: https://www.skidsolutions.eu/en/repository/CPS/.

2.2.2. Items not Published in the Certification Practice Statement

Refer to clause 9.3.1 of SK PS [1].

2.3. Time or Frequency of Publication

Refer to clause 1.5.4 of SK PS [1].

2.4. Access Controls on Repositories

Refer to clause 2.4 of SK PS [1].

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of Names

Types of names assigned to the Subscriber are described in the Certificate Profile [3].

3.1.2. Need for Names to be Meaningful

Meanings of names on different fields of the certificate are described in the Certificate Profile [3].

3.1.3. Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting various name forms are described in the Certificate Profile [3].

3.1.5. Uniqueness of Names

SK guarantees that multiple certificates with identical distinguished names are not valid at the same time.

3.1.6. Recognition, Authentication, and Role of Trademarks

Not allowed.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Possession of Private Key is guaranteed by internal procedures of SK. Procedures are carried out by persons named by CEO of SK and observed by external auditor.

3.2.2. Authentication of Organisation and Domain Identity

Not applicable.

3.2.3. Authentication of Individual Identity

CEO of SK defines a commission of at least 4 persons to carry out key generation and certification procedures. The head of commission is nominated also by CEO.

An independent auditor is observing the key generation procedures and identifies the personnel carrying out the procedure and verifies their authorisation.

3.2.4. Non-Verified Subscriber Information

Not allowed.

3.2.5. Validation of Authority

CEO of SK nominates personnel carrying out the procedures of key generation and certification.

3.2.6. Criteria for Interoperation

SK ID Solutions ROOT G1 does not cross-certify other Root CA-s.

3.3. Identification and Authentication for Re-Key Requests

Not applicable.

3.4. Identification and Authentication for Revocation Request

Refer to clause 3.2.3 of this CPS.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

CEO of SK approves certificate applications.

4.1.2. Enrolment Process and Responsibilities

CEO of SK approves the application for key generation and certification and nominates list of persons to carry out the procedure, contents, time and place of the procedure.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

Refer to clause 3.2.3 of this CPS.

4.2.2. Approval or Rejection of Certificate Applications

All certificate applications that have not been enforced with the decree issued by CEO of SK are rejected.

4.2.3. Time to Process Certificate Applications

CEO of SK defines the time to process the application.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

The certificate is issued manually from an off-line part of SK's information system based on the decree of CEO of SK. Decree establishes the procedure to be carried out and the commission mandated by CEO to carry it out.

The certificate is valid from the moment specified in the certificate.

After issuance of a certificate, a new CRL is issued and a fresh backup of the database is made.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

The procedure is documented in a way that shows the activities done and the certificate issued. The document on the issuance is signed by members of the commission.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Dedicated member of the commission verifies that the issued certificate is correct.

4.4.2. Publication of the Certificate by the CA

The certificate is published on webpage of SK: https://www.skidsolutions.eu/en/repository/certs/

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Refer to clause 4.4.2 of this CPS.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

The Subscriber is required to use the Private Key and the certificate in accordance with CPS of the CA to be certified.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Party is required to use the Subscriber's Public Key and the certificate in accordance with CPS of the CA to be certified.

4.6. Certificate Renewal

Not applicable.

4.7. Certificate Re-Key

Not applicable.

4.8. Certificate Modification

4.8.1. Circumstances for Certificate Modification

Certificate Modification is allowed to correct mistakes in previous certificate.

4.8.2. Who can request Certificate Modification

CEO of SK can request Certificate Modification.

4.8.3. Processing Certificate Modification Requests

Refer to clause 4.2 of this CPS.

4.8.4. Notification of New Certificate Issuance to Subscriber

Refer to clause 4.3.2 of this CPS.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Refer to clause 4.4.1 of this CPS.

4.8.6. Publication of the Modified Certificate by the CA

Refer to clause 4.4.2 of this CPS.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Refer to clause 4.4.2 of this CPS.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Refer to clause 4.9.1.2 of CA/Browser Baseline Requirements for Issuing and Management of Publicly-Trusted Certificates [4].

4.9.2. Who Can Request Revocation

Request for revocation is submitted to CEO of SK.

4.9.3. Procedure for Revocation Request

The application for revocation can be submitted only to CEO of SK.

The application is checked for correctness and validity according to presented evidence and other available information.

After revoking the certificate SK issues immediately a new CRL which contains the serial number of the revoked certificate.

4.9.4. Revocation Request Grace Period

Not applicable.

4.9.5. Time Within Which CA Must Process the Revocation Request

SK will process the revocation request within 5 working days after receiving the application.

4.9.6. Revocation Checking Requirements for Relying Parties

Relying Party must verify the validity of a certificate before trusting it.

4.9.7. CRL Issuance Frequency

CRL is issued once every 90 days, with the value of the next Update field set to 97 days after issuance of CRL.

4.9.8. Maximum Latency for CRLs

CRL is published no later than 1 working day after issuance.

4.9.9. On-Line Revocation/Status Checking Availability

Refer to clause 4.10.1 of this CPS.

4.9.10. On-Line Revocation Checking Requirements

Relying Party is obliged to check the status of a certificate.

4.9.11. Other Forms of Revocation Advertisements Available

Information about revocation of a certificate can be requested by e-mail at info@skidsolutions.eu or by phone +372 6101880.

4.9.12. Special Requirements Related to Key Compromise

A security incident must be opened in case of key compromise.

4.9.13. Circumstances for Suspension

Not applicable.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

SK offers CRL and OCSP services for checking certificate status. Services are accessible over HTTP protocol. The status of a certificate can be verified using OCSP protocol at http://ocsp.sk.ee/CA and using CRLs at http://c.sk.ee/SK_ROOT_G1E.crl and http://c.sk.ee/SK_ROOT_G1R.crl. The URLs of the services are included in the certificates on the CRL Distribution Point (CDP) and Authority Information Access (AIA) fields respectively in accordance with the Certificate Profile [3].

4.10.2. Service Availability

SK ensures availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99.44% availability overall per year with a scheduled downtime that does not exceed 0.28% annually.

4.10.3. Operational Features

None.

4.11. End of Subscription

Not applicable.

4.12. Key Escrow and Recovery

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Refer to clause 5 of SK PS [1].

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

Refer to clause 6.1 of SK PS [1].

6.1.1. Key Pair Generation

Refer to clause 6.1.1 of SK PS [1].

6.1.2. Private Key Delivery to Subscribers

Not applicable.

6.1.3. Public Key Delivery to Certificate Issuer

The public key is delivered using removable media and the auditor verifies its integrity.

6.1.4. CA Public Key Delivery to Relying Parties

Refer to clause 6.1.4 of SK PS [1].

6.1.5. Key Sizes

According to this CPS key sizes are in accordance with ETSI TS 119 312 [9]. Key size for each CA to be certified is defined on a case-by-case basis.

6.1.6. Public Key Parameters Generation and Quality Checking

Refer to clause 6.1.6 of SK PS [1].

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Key usage purposes are described in the Certificate Profile [3].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Refer to clause 6.2.1 of SK PS [1].

6.2.2. Private Key (n out of m) Multi-Person Control

Refer to clause 6.2.2 of SK PS [1].

6.2.3. Private Key Escrow

Refer to clause 6.2.3 of SK PS [1].

6.2.4. Private Key Backup

Refer to clause 6.2.4 of SK PS [1].

6.2.5. Private Key Archival

Refer to clause 6.2.5 of SK PS [1].

6.2.6. Private Key Transfer Into or From a Cryptographic Module

Refer to clause 6.2.6 of SK PS [1].

6.2.7. Private Key Storage on Cryptographic Module

Refer to clause 6.2.7 of SK PS [1].

6.2.8. Method of Activating Private Key

Refer to clause 6.2.8 of SK PS [1].

6.2.9. Method of Deactivating Private Key

Refer to clause 6.2.9 of SK PS [1].

6.2.10. Method of Destroying Private Key

Refer to clause 6.2.10 of SK PS [1].

6.2.11. Cryptographic Module Rating

Refer to clause 6.2.11 of SK PS [1].

6.3. Other Aspects of Key Pair Management

Refer to clause 6.3 of SK PS [1].

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Refer to clause 6.4.1 of SK PS [1].

6.4.2. Activation Data Protection

Refer to clause 6.4.2 of SK PS [1].

6.4.3. Other Aspects of Activation Data

Refer to clause 6.4.3 of SK PS [1].

6.5. Computer Security Controls

Refer to clause 6.5 of SK PS [1].

6.6. Life Cycle Technical Controls

Refer to clause 6.6 of SK PS [1].

6.7. Network Security Controls

Refer to clause 6.7 of SK PS [1].

6.8. Time-Stamping

Refer to clause 6.8 of SK PS [1].

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

The certificate profile is described in the Certificate Profile [3], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/.

7.2. CRL Profile

The CRL profile is described in the Certificate Profile [3], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/.

7.3. OCSP Profile

The OCSP profile is described in the Certificate Profile [3], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Refer to chapter 8 of SK PS [1].

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Not applicable.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Refer to clause 9.2.1 of SK PS [1].

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or Warranty Coverage for End-Entities

Refer to clause 9.2.1 of SK PS [1].

9.3. Confidentiality of Business Information

Refer to clause 9.3 of SK PS [1].

9.4. Privacy of Personal Information

Refer to clause 9.4 of SK PS [1].

9.5. Intellectual Property Rights

Refer to clause 9.5 of SK PS [1].

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

Refer to clause 9.6.1 of SK PS [1].

SK ensures that:

- the certification keys are protected by HSM and are under sole control of SK;
- in case of compromise of certification keys all issued certificates will be revoked;
- all the activated certification keys are on the territory of the Republic of Estonia.
- the certification keys used in the supply of the certification service are activated on the basis of shared control.

9.6.2. RA Representations and Warranties

Not applicable.

9.6.3. Subscriber Representations and Warranties

Not Applicable.

9.6.4. Relying Party Representations and Warranties

Refer to clause 9.6.4 of SK PS [1].

A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in this CPS.

9.6.5. Representations and Warranties of Other Participants

Not applicable.

9.7. Disclaimers of Warranties

Refer to clause 9.7 of SK PS [1].

9.8. Limitations of Liability

Refer to clause 9.8 of SK PS [1].

9.9. Indemnities

Not applicable.

9.10. Term and Termination

9.10.1. Term

Refer to clause 1.5.4 of this CPS.

9.10.2. Termination

Refer to clause 9.10.2 of SK PS [1].

9.10.3. Effect of Termination and Survival

SK communicates the conditions and effect of the termination of this CPS via its public repository. The communication specifies which provisions survive termination.

At a minimum, all responsibilities related to protecting confidential information, also maintenance of SK archives for determined period and logs survive termination.

Termination of this CPS cannot occur before termination actions described in clause 5.8 of SK PS [1].

9.11. Individual Notices and Communications with Participants

Refer to clause 9.11 of SK PS [1].

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to clause 1.5.4 of this CPS.

9.12.2. Notification Mechanism and Period

Refer to clause 2.2.1 of this CPS.

9.12.3. Circumstances Under Which OID Must be Changed

Not applicable.

9.13. Dispute Resolution Provisions

Refer to clause 9.13 of SK PS [1].

9.14. Governing Law

This CPS is governed by the jurisdictions of the European Union and Estonia.

9.15. Compliance with Applicable Law

SK ensures compliance with all requirements to comply with laws to protect data against loss, destroying of forging, and the following requirements:

- eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [5];
- Relevant European standards:
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI): General Policy Requirements for Trust Service Providers [6];
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [7];
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [8].

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

Not applicable.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of SK. Unless specified otherwise in a contract with a party, SK does not provide notice of assignment.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS remains valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

SK may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. SK's failure to enforce a provision of this CPS does not waive SK's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by SK.

9.16.5. Force Majeure

Refer to clause 9.16.5 of SK PS [1].

9.17. Other Provisions

Not applicable.

REFERENCES

[1] SK ID Solutions AS – Trust Services Practice Statement, published: https://www.skidsolutions.eu/en/repository/sk-ps/;
[2] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
[3] Certificate, OCSP and CRL Profile for Intermediate CA Issued by SK, published: https://www.skidsolutions.eu/en/repository/profiles/
[4] CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (V1.8.0), published: https://cabforum.org/baseline-requirements-documents/;
[5] eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
[6] ETSI EN 319 401 Electronic Signatures and Infrastructure (ESI): General Policy Requirements for Trust Service Providers;
[7] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
[8] ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
[9] ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites