AK

Certificate Policy

for

Fullgilt auðkenni 2021

Version 3.6 – correcting previous versions

Effective date: Retroactive, see change control on next page

Change control		
Published	**Version**	**Changes**
01.11.2019	0.1	First draft version.
	1.0	Previous version of CP. Information added to keep consistency in version numbering.
16.03.2021	2.0	Publication
21.9.2021	2.1	Added changes to chapter 1.3.3 regarding National Registry. Approval column removed from Change Control. OID for NCP and NCP+ in Ch. 1.2 Policy name "Fullgilt auðkenni" updated to "Fullgilt auðkenni 2021" Use of Crypto Stick defined as Future service as well as NCP for QCP-l. Changed max allowed outage in c. 4.10.2
23.11.2022	3.0	Added information about Automated Biometric Identity Verification (ABIV) in App. Added information about Time-Stamping Unit (TSU). Changed information about other participants. Minor fixes to text.
15.09.2023	3.1	AK's address updated. Minor fixes to text, grammatical error fixed, cosmetic changes, harmonization in use of terms etc.
29.10.2023	3.2	Reference errors corrected. Minor fixes to text, errors corrected.
11.01.2024	3.3	Clarification added specifying that certain services are currently not available.
03.06.2024	3.4	Chapter 3.2.3 updated to include the option of ABIV in App for minors.
19.09.2025	3.5	Version numbers of ETSI standards updated. Minor fixes to text.
9.12.2025	3.6	**Correction version.** This version shall correct version 2.1 as of 21.09.2021 with regards to issuance date of the ESTI EN 319 401 v1.2.1. The correct issuance date is 2018-04 (not 2018-02). This version shall correct versions 3.0, 3.1, 3.2, 3.3, 3.4 and 3.5 as of their effective date with regards to referenced versions of ETSI EN 319 411-2, ETSI SI EN 319 411-1 and ETSI EN 319 401 (see chapter 10). Versions 3.0, 3.1, 3.2, 3.3, 3.4 and 3.5 should have included the following versions of the standards: • ETSI EN 319 411-2 V2.4.1 (2021-11) • ETSI EN 319 411-1 V1.3.1 (2021-05) • ETSI EN 319 401 V2.3.1 (2021-05) For clarification and avoidance of doubt, all Certificates issued during the validity of versions 3.0, 3.1, 3.2, 3.3, 3.4 and 3.5 were issued in compliance with the above mentioned ETSI standards. Chapter 3.1.5 clarification of Subject´s uniqueness added.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This document is the Certification Policy (CP) that defines procedure and operational requirements that Auðkenni ehf. (AK) adheres to and requires entities to adhere to when issuing and managing Certificates for Fullgilt auðkenni 2021 (FA). FA is an intermediary root owned by Auðkenni, issued by Íslandsrót 2021, used to issue Certificates to end-users. Íslandsrót 2021, the default Icelandic root anchor, is managed by the Ministry of Finance. The full CA hierarchy is described in the TSPS [12]. The Certificate Profiles issued by FA under this Certificate Policy are as follows:

Certificate Policy / Technology	QCP-n-qscd	QCP-l-qscd	QCP-l *NCP+*	QCP-l *NCP*	NCP+	NCP	Signature	Authentication
SIM on Mobile	X				X		X	X
Card	X				X		X	X
App on Smart Device	X				X		X	X
eSeal		Future service	X	X			X	
Equipment authentication						X	X	X
Time-Stamping Unit (TSU)					X		X	X

The Certificate Policy is a "named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements." [4] The content and format of this document complies with the requirements of the IETF RFC 3647 [4] framework. It consists of 9 sections that contain the security requirements, processes and the practices defined by AK to be followed during the provision of services. To strictly preserve the outline specified by IETF RFC 3647, sections where the Certificate Policy does not impose a requirement have the statement "No stipulation".

This document contains the requirements of multiple Certificate Policies. Most of the requirements defined in the document apply to all the Certificate Policies uniformly and are not otherwise mentioned. Where the policies require different requirements, it will be clearly identified which Certificate Policy the given requirement refers to.

Each product, except in the case of eSeals and TSU Certificates, contains two key pairs and thus two Certificates: an Authentication Certificate and a Qualified Electronic Signature Certificate and their corresponding Private Keys. Each Private Key is protected depending on the level of protection based on the quality of the FA Certificate profile. A single person can have several valid Certificate pairs. eSeals have one Certificate that can be used for Seal, Authentication, or both. TSU Certificate is only used to issue Public Key Certificates for other TSPs/TSAs that wish to issue time-stamps. Audkenni does not issue time-stamps.

Issuing and managing Certificates within FA is regulated by the eIDAS Regulation (EU) 910/2014 implemented into Icelandic law with Icelandic act no. 55/2019 [1] which establishes a legal framework for electronic authentication and trust services in Iceland.

This document describes restrictions to Policy for EU Qualified Certificate issued to natural persons or legal persons where the Private Key and the related Certificate reside on a QSCD (QCP-n-qscd and QCP-l-qscd) from ETSI EN 319 401 and ETSI EN 319 411-2 [3], and Normalized Certificate Policy (NCP) requiring a secure cryptographic device (NCP+) from ETSI EN 319 401 and ETSI EN 319 411-1 [2].

The certification service for Qualified Electronic Signature Certificates described in this CP SHALL be a qualified trust service and claimed as such to the trusted list of Iceland.

The keywords "**MUST, MUST NOT, IS REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, CAN** and **OPTIONAL**" in this document must be interpreted as described in [5]. The exact meaning of these words is modified in accordance with the requirements within the text where they occur.

When the words **MUST** and **MANDATORY** are used, this means that the definition is an absolute requirement in the specification.

MUST NOT or **SHALL NOT** means that the definition is absolutely forbidden in the specification.

SHOULD or **RECOMMENDED** means that there may be cases where there are strong reasons to ignore a subject, but in doing so, one must understand and consider the full consequence of choosing another solution.

SHOULD NOT or **NOT RECOMMENDED** means that there may be cases where there are strong reasons to, or it would be useful to, perform a certain task, but in doing so, one must understand and consider the full consequence of performing a task that is described with these words.

CAN or **OPTIONAL** means that the subject/element is optional.

1.2 DOCUMENT NAME AND IDENTIFICATION

Refer to chapter 5.3 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

This document is named "AK Certificate Policy for Fullgilt auðkenni 2021".

This CP is identified by the OID: {joint-iso-itu-t(2) country(16) is(352) organizations-and-institutes(1) audkenni(2) pki(1) public-pki(1) cp(2) } This can also be written as {2.16.352.1.2.1.1.2}. The OID for this CP is fixed and will not change with new versions of this document.

Qualified Electronic Signature Certificate by FA issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-2 [3] chapter 5.3 c) for QCP-n-qscd: 0.4.0.194112.1.2
  - Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
- ETSI EN 319 411-2 [3] chapter 5.3 d) for QCP-l-qscd: 0.4.0.194112.1.3
  - Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)
- ETSI EN 319 411-2 [3] chapter 5.3 b) for QCP-l: 0.4.0.194112.1.1
  - itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)
- This CP.

Authentication Certificates by FA issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-1 [2] chapter 5.3 a) for NCP: 0.4.0.2042.1.1
  - itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)
- ETSI EN 319 411-1 [2] chapter 5.3 b) for NCP+: 0.4.0.2042.1.2
  - itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
- ETSI EN 319 411-1 [2] chapter 5.3 a) for NCP: 0.4.0.2042.1.1
  - itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)
- This CP.

TSU Certificates by FA issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-1 [2] chapter 5.3 b) for NCP+: 0.4.0.2042.1.2
- itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

1.3 PKI PARTICIPANTS

Refer to chapter 5.4 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

1.3.1 Certification Authorities

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

1.3.2 Registration Authorities

AK operates as a Registration Authority (RA) and has contracts with entities that operate as Registration Authorities. Refer to list of RAs at Auðkennis website.

The Registration Authority operated by AK constitutes physical facilities, self-registration website, self-registration via App on Smartphone (CURRENTLY NOT AN OPTION) or via ABIV. In this document RA means all these different facilities.

RA performs Subscriber Authentication and associates the Subscriber to the specific QSCD, eSeal or Non-qualified Certificate in App and initiates creation of keypairs.

For Certificates on SIM-cards, the MO has issued the QSCD to the Subscriber beforehand. Subscriber can decide to register for a Certificate at any time.

AK facilitates the registration / management of the QSCD for the App.

1.3.3 Subscribers

The Subscriber can either be a natural person or legal person dependent on the Certificate Profile. The Subscriber is often the Subject of the Certificate issued under this CP. Only Subscribers and/or Subjects with an ID assigned by the National Registry or the Companies registry can be registered.

1.3.4 Relying Parties

Relying Parties are legal or natural persons who are making decisions based on the Certificate and to authenticate Subscribers and allow Subscribers to sign.

1.3.5 Other Participants

QSCD for Mobile Certificates are procured by MOs. QSCD for Cards and QSCD Crypto Sticks for eSeals are procured by AK from relevant suppliers (SCM, CM). MOs facilitate communication between the Subscriber's device and the QSCD in the case of Mobile Certificates. Crypto Stick is a future service not yet implemented.

The creation of the App keys and storage of keys as well as the Automated Biometric Identity Verification is facilitated by an external party.

1.4 CERTIFICATE USAGE

Refer to chapter 5.5 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

1.4.1 Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes:

Qualified Electronic Signature Certificate is intended for:

- Creating Qualified Electronic Signatures compliant with eIDAS [1].

- In case of App on Smartphone where AK manages part of the QSCD, the Private Key SHALL NOT be used for signing except within the QSCD.

Authentication Certificate is intended for:

- Authentication.

CA Private Keys SHALL NOT be used to sign other types of Certificates except for the following:

- Subscriber Certificates compliant with QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ or NCP.
- OCSP response verification Certificates.
- CRL signing Certificates.
- Internal Certificates for technical needs.

1.4.2 Prohibited Certificate Uses

Subscriber's Certificates issued under this CP SHALL NOT be used for any of the following purposes:

- Unlawful activity (including cyber-attacks and attempt to infringe the Certificate or FA).
- Issuance of new Certificates and information regarding Certificate validity.
- Enabling other parties to use the Subscriber's Private Key.
- Enabling the Certificate issued for electronic signature to be used in an automated way.

Subscriber's Authentication Certificate SHALL NOT be used to create Qualified Electronic Signatures compliant with eIDAS [1].

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

This document is administered by AK.

Organization name: *Auðkenni ehf.*

Registry code: *521000-2790*

Organization address: *Katrínartún 4, 105 Reykjavik, Iceland*

Telephone: *+354 530 0000*

Email: *fyrirspurnir@audkenni.is*

Website: *http://www.audkenni.is/*

1.5.2 Contact Person

Company Executive Officer

Email: *fyrirspurnir@audkenni.is*

1.5.3 Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4 CP Approval Procedures

Amendments which do not change the meaning of this CP, such as spelling corrections, translation activities and contact details updates, are documented in the Versions and Changes section of the present document. In this case the fractional part of the document version number SHALL be increased by one.

In the case of substantial changes, the new CP version SHALL be clearly distinguishable from the previous ones, and the version number SHALL be increased by one. The amended CP along with the enforcement date, which cannot be earlier than 10 days after publication, SHALL be published electronically on AK website.

This CP shall be reviewed annually.

All amendments to this CP SHALL be coordinated with RAs and other subcontractors as applicable.

All amendments changing the meaning of this CP SHALL be approved by the Security Committee.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Terminology

In this CP, the following terms have the following meaning:

Term	Definition
App	Mobile application that works as a QSCD. Used on Smartphone or Smart Devices only.
Authentication	Unique identification of a person (natural or legal) by checking the alleged identity.
Authentication Certificate	Certificate is intended for Authentication.
Automated Biometric Identity Verification	Remote on-boarding process for App on Smartphone where the Subscriber's identity is verified by his/her biometric characteristics.
Card	QSCD on a plastic card.
Certificate	Public Key, together with some other information, laid down in the Certificate Profile[4], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of Auðkenni's structure responsible for issuing and verifying electronic Certificates with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a community and/or PKI implementation with common security requirements.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certification Service	In the context of this document, service related to issuing Certificates, managing revocation, modification, and re-key of the Certificates.
Crypto Stick	USB key with integrated (proprietary) smart card to enable highly secure encryption of e-mails and data, for authentication in networks and for access control.
Distinguished Name	Unique Subject name in the infrastructure of Certificates.
Fullgilt auðkenni 2021	An intermediate Certificate, the Certificates of which enabling electronic identification, electronic signature and electronic seals are connected to the SIM-card of Mobile or Cards or App.
Integrity	A characteristic of an array: information has not been changed after the array was created.
Mobile	A wireless handheld device with SIM-card.
National Registry	Iceland's national registry (Þjóðskrá Íslands).
Object Identifier	An identifier used to uniquely name an object (OID).
PIN code	Activation code for a Private Key.
Private Key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures or authenticate someone.

Public Key	The key of a key pair that may be publicly disclosed by the holder of corresponding Private Key or CA and that is used by Relying Party to verify electronic signatures created with the holder's corresponding Private Key.
Qualified Certificate	A Certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation [1].
Qualified Electronic Signature	Advanced electronic signature that is created by a Qualified Electronic Signature Creation Device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Certificate for Electronic Seals	Qualified Certificate for Electronic Seals according to eIDAS [1].
Qualified Certificate for Electronic Signatures	Qualified Certificate for Electronic Signatures according to the eIDAS [1].
Qualified Electronic Signature Creation Device (QSCD)	A Secure Signature Creation Device that meets the requirements laid down in eIDAS [1].
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Relying Party	Entity that relies upon the information contained within a Certificate or Certificate status information provided by Auðkenni.
Secure Cryptographic Device	Device which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Smartphone / Smart Device	A cellular telephone or a device with an integrated computer and other features not originally associated with telephones, such as an operating system, web browsing and the ability to run software application
Subject	Natural or legal person, or an organization or a device which the Certificates are issued to.
Subscriber	Subscriber is a natural or legal person that is a Subscriber at the CA for one or more Subjects. Subscriber can also be a Subject.
Terms and Conditions	AK's document that describes obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber must be familiar with the document and accept the Terms and Conditions [7] upon receipt the Certificates. The Terms and Conditions are available at repo.audkenni.is

1.6.2 Acronyms

Acronym	Definition
ABIV	Automated Biometric Identity Verification
AK	Auðkenni ehf.
AK CA	The system that processes the CSR from the App. This can be an external service provider such as SK
CA	Certificate Authority
CM	Card manufacturer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [1] 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 and Icelandic act nr. 55/2019
eMRTD	Electronic Machine-Readable Travel Document. Identity or travel documents that has contactless integrated circuit embedded in it usable for biometric identification.
FA	Fullgilt auðkenni 2021. Certificate used to issue Certificates to Subscribers. This is an intermediary root under Íslandsrót 2021.
HSM	Hardware Security Module
MO	Mobile Operator
NCP+	Normalized Certificate Policy requiring a Secure Cryptographic Device
OCSP	Online Certificate Status Protocol
NCP	Normalized Certificate Policy
OID	Object Identifier, a unique object identification code
PIN	Personal identification number
PKI	Public Key Infrastructure

QSCD	Qualified Electronic Signature Creation Device
QCP-n-qscd	Policy for EU qualified Certificate issued to a natural person where the Private Key and the related Certificate reside on a QSCD
QCP-l-qscd	Policy for EU qualified Certificate issued to a legal person where the Private Key and the related Certificate reside on a QSCD
QCP-l	Policy for EU Qualified Certificate issued to a legal person where the Private Key and the related Certificate DO NOT reside on a QSCD.
RA	Registration Authority
SCM	SIM-card Manufacturer
SIM	SIM-card used in Mobile phones
SK	Provider of international e-identity solutions. SK provides support for the App for smart phones and operates ABIV.
TSPS	Trust Service Practice Statement
TSA	Time Stamping Authority
TSU	Time-Stamping Unit

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

Refer to chapter 6.1 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

2.1 REPOSITORIES

AK SHALL make its repository of information available on its webpage. The repository SHALL contain this CP and associated CPS, Terms and Conditions, Trust Service Provider Statement, and other necessary documents.

AK SHALL also make sure that the systems publishing its service Certificates, the Certificate repository and the revocation status information will be available 24/7.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication and Notification Policies

This CP, the Certification Practice Statement [11], the Certificate Profiles [6], as well as the Terms and Conditions [7] with the enforcement dates, SHALL be published on the website repo.audkenni.is no less than 10 days prior to taking effect.

2.2.2 Items not Published in the Certification Practice Statement

Information about service levels, fees and technical details laid out in mutual agreements between AK and RA MAY be left out of CPS.

2.3 TIME OR FREQUENCY OF PUBLICATION

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

2.4 ACCESS CONTROLS ON REPOSITORIES

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

3 IDENTIFICATION AND AUTHENTICATION

Refer to chapter 6.2 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

3.1 NAMING

The Distinguished Name of the Certificate SHALL comply with conventions set in the Certificate Profile [6].

3.1.1 Types of Names

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

3.1.2 Need for Names to be Meaningful

All the values in the Subscriber information section of a Certificate SHALL be meaningful.

3.1.3 Anonymity or Pseudonymity of Subscribers

AK does not allow Certificates with Anonymity or Pseudonymity.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

3.1.5 Uniqueness of Names

AK SHALL ensure that each Subject will be issued a Certificate that uniquely identifies them using Serial Number (SN). SN is a unique number issued to individuals by the National Registry. For each Subject this is a unique number and therefore makes the SN unique for the individual. The issued Certificate also includes a SN that is unique for the issued Certificate that makes it different from all other Certificates.

AK SHALL ensure that the Subject is entitled to use indicated names as recorded in the National Registry or national business registry and AK is entitled to revoke the Certificate in question for the forbidden use of name or data.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable.

3.2 INITIAL IDENTITY VALIDATION

AK can use any communication channel within the limits provided by law, for the verification of the identity of the person or organization requesting the Certificate, and for checking the authenticity of the data provided.

AK may refuse the issuance of the required Certificate at its sole discretion, without any apparent justification.

3.2.1 Method to Prove Possession of Private Key

RA SHALL perform Subscriber Authentication and:

- for Mobile and Card initiate creation of key pairs;
- for App, the App itself initiates the creation of key pairs;
- for eSeal either the customer creates the key pairs in own HSM or AK provides a QSCD and initiates the creation;
- for TSU the customer creates the key pairs in own HSM.

For Mobile Certificates, Subscribers SHALL verify the possession of the QSCD by entering the code received from the RA.

For Certificates on Cards the Private Key is created on the Card at time of registration.

For certificates on App, Subscribers SHALL confirm the possession of Private Key by giving the activation code to the RA. In case of online registration Subject MUST use a Certificate on Mobile to verify possession. In case of self-registration in the App the Subscriber MUST have a Qualified Certificate issued by AK to prove possession (CURRENTLY NOT AN OPTION).

For Qualified eSeals the Subscriber MUST either provide evidence that the key pair was generated using a FIPS 140-2 level 3 or Common Criteria certified HSM [14] or use a secure token (Crypto Stick, future service) provided by AK.

For TSU certificates the Subscriber MUST provide evidence that the key pair was generated using a FIPS 140-2 level 3 or Common Criteria certified HSM [14].

For Non-qualified eSeals the Subscriber IS NOT required to provide evidence of the key pair being generated using a FIPS 140-2 Level 3 or Common Criteria certified HSM [14].

FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

3.2.2 Authentication of Organization Identity

RA SHALL verify organizational identity by consulting the official government company registry or by looking up information from other government or business registers and matching the information. When the Subject is a natural person identified in association with a legal person (Subscriber) evidence of the identity of the Subject will be kept.

3.2.3 Authentication of Individual Identity

Authentication of Subject is carried out by RA as follows.

RA SHALL perform Subject Authentication when the Subject applies for a new Certificate to be issued to a natural person or a natural person is acting on behalf of an Organization or legal person.

RA SHALL Authenticate the Subject:

- via physical presence checks or
- via self-registration using means of electronic authentication and Qualified Electronic Signature compliant with article 24.1.c of eIDAS [1] (CURRENTLY NOT AN OPTION); or
- via self-registration using Automated Biometric Identity Verification.

In case of Automated Biometric Identity Verification, AK ensures authentication by:

- acquiring the Subscriber’s unequivocal consent for the ABIV process
- verifying authenticity of the Subscriber's eMRTD presented for verification
- reading the Subscriber's personal data from the Subscriber's eMRTD presented for verification; performing liveness detection of the Subscriber's facial image; and
- performing match of the Subscriber's facial image captured in the liveness session during registration with the data set on the chip on his/her eMRTD presented for verification.

In case of Automated Biometric Identity Verification for minors, AK ensures authentication by:

- acquiring the Subject’s unequivocal consent for the ABIV process.
- acquiring the Subject’s legal representative consent for the ABIV process as well through the signing of the application;
- verifying authenticity of the Subject's eMRTD presented for verification;
- reading the Subject's personal data from the Subject's eMRTD presented for verification; performing liveness detection of the Subject's facial image; and
- performing match of the Subject's facial image captured in the liveness session during registration with the data set on the chip on his/her eMRTD presented for verification.

For a more detailed description of the authentication process, see chapter 3.2.3 in the CPS.

3.2.4 Non-Verified Subscriber Information

Non-verified information IS NOT allowed in the Certificate.

3.2.5 Validation of Authority

In general, the Subscriber SHALL apply for a Certificate on behalf of itself.

When the Subscriber does not have the legal capacity, a legal guardian SHALL sign the application.

When applying on behalf of an organization the representative MUST be authorized to sign on behalf of the organization.

3.2.6 Criteria for Interoperation

No stipulation

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

Re-key IS NOT allowed.

3.3.2 Identification and Authentication for Re-Key After Revocation

Re-key after revocation IS NOT allowed.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

No stipulation in addition to QCP-n-qscd, QCP-l, QCP-l-qscd, NCP+, and NCP.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Refer to chapter 6.3 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

AK SHALL accept Certificate applications only from the Subscriber or Subject in case the Subscriber is a legal entity.

Certificate application MAY be submitted via RA.

For qualified Certificates on eSeals the Certificate application process SHALL ensure that the Subscriber has possession or control of the Private Key associated with the Public Key presented for certification.

For TSU the Certificate application process SHALL ensure that the Subscriber has possession or control of the Private Key associated with the Public Key presented for certification.

4.1.2 Enrolment Process and Responsibilities

The Subscriber WILL request Certificates via RA.

The enrolment process is as follows.

- RA SHALL Authenticate the Subscriber as stated in chapter 3.2.3 of this CP.
- RA SHALL perform additional checks related to the Subscriber's identity validation.

- RA SHALL verify compliance to the Subscriber's name with the Subscriber's name on its identity document and in the National Registry.
- RA SHALL record Subscriber contact information.
- Upon successful Authentication, the Subscriber SHALL accept the Terms and Conditions [7] and
  - confirm that the QSCD for Certificates on Mobile is in its possession by entering the Activation code provided by the RA,
  - confirm that the QSCD for Certificates on Card is in its possession by selecting PIN codes,
  - confirm that the QSCD for Certificates on App is in its possession by using Mobile Certificate or entering the Activation code provided by the app and recorded by the RA.
  - confirm that the QSCD (Crypto Stick) for Certificates on eSeal is in its possession by selecting PIN codes.
  - confirm that a FIPS-140-2 level 3 or Common Criteria [14] certified HSM is used for TSU Certificates. FIPS 140-2 level 3 certified HSM shall be in FIPS mode.
- For QSCD personalization, RA supplies CA with information that binds the Subject to the Private Keys on the QSCD in the Subject's possession and the corresponding Public Keys, which CA uses for certification.
- RA SHALL apply for Certification at the CA on behalf of the Subscriber.
- RA SHALL archive the agreement signed by the Subscriber and return to the CA.
- CA SHALL verify validity of the QSCD, perform the necessary checks, sign the Public Keys and the Certificate SHALL be made available via mitt.audkenni.is or API service and the OCSP SHALL start responding with „GOOD".

RA is responsible for submitting correct identification data from the National Registry to the CA.

4.2 CERTIFICATE APPLICATION PROCESSING

Certificates on Card, Mobile and App are finished as part of the enrollment process (chapter 4.1.2). Issuance of eSeals is the content of the following chapters.

4.2.1 Performing Identification and Authentication Functions

After receiving a Certificate application, the RA verifies the application information and other information in accordance with Section 3.2.3. The RA MUST create and maintain records enough to establish that it has performed its required verification tasks. RA evaluates the information presented and decides whether it is correct and reliable enough to issue the Certificate. This process is applicable to all types of Certificates.

4.2.2 Approval or Rejection of Certificate Applications

CA SHALL refuse to issue a Certificate if:

- for QCP-n-qscd: the information about QSCD does not exist in the CA database in case of Certificate on Mobile and Certificate on Card;
- for QCP-l-qscd: the QSCD is not provided by AK in case Crypto Stick is used;
- the application data does not validate;
- the Certificate application does not comply with the technical requirements set in applicable documents;
- the Subscriber lacks legal capacity and is not properly represented;
- the data used for identification does not match with the data in a reliable source (National Registry).
- the Subjects ID on the application does not match with the Subjects ID on its identity document;
- the eMRTD is unsuccessfully used for biometric verification and there is a reasonable doubt for its misuse;
- integrity and trustworthiness of the data read from the eMRTD cannot be verified;
- the eMRTD has not been issued by a respective document issuer;
- authenticity of the eMRTD cannot be verified;
- the facial image read from the data set on the chip on eMRTD does not match with the facial image of the Subscriber performing the liveness session;
- the liveness of the Subscriber's facial image cannot be verified;
- the eMRTD is expired or revoked;
- the App security monitoring mechanism has detected threats to the system or Subscriber identity.

If the data contained in a Certificate application needs to be modified, the corresponding amendment SHALL be coordinated with Subscriber.

If the CA refuses to issue a Certificate Subscriber SHALL be notified.

4.2.3 Time to Process Certificate Applications

Certificate applications are processed in a timely manner when all conditions for the application have been fulfilled.

4.3 CERTIFICATE ISSUANCE

Applications for Certificates on Card, Mobile and App are finished as part of the enrollment process (chapter 4.1.2).

4.3.1 CA Actions During Certificate Issuance

Refer to chapter 4.3.1 of CPS.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Subscribers for Certificates issued on Mobile or in App are notified by a message on the Mobile of the issuance.

Subjects for Certificates issued on Cards are notified verbally by the RA.

For e-seals and Equipment Authentication the CA SHALL notify the Subscriber of the new Certificate issuance by email.

For TSU Certificates the CA SHALL notify the Subscriber of the new Certificate issuance by email.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

Refer to chapter 4.4.1 of CPS.

4.4.2 Publication of the Certificate by the CA

Certificates are published by CA in API service. Certificate validity can be checked through Auðkenni OCSP service and CRL.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.5.2 Relying Party Public Key and Certificate Usage

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.6 CERTIFICATE RENEWAL

Renewal IS NOT allowed.

4.7 CERTIFICATE RE-KEY

Certificate Re-Key IS NOT allowed.

4.7.1 Circumstances for Certificate Re-Key

Certificate Re-Key IS NOT allowed.

4.7.2 Who May Request Certification of a New Public Key

Certificate Re-Key IS NOT allowed.

4.7.3 Processing Certificate Re-Keying Requests

Certificate Re-Key IS NOT allowed.

4.7.4 Notification of New Certificate Issuance to Subscriber

Certificate Re-Key IS NOT allowed.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Certificate Re-Key IS NOT allowed.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Certificate Re-Key IS NOT allowed.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate Re-Key IS NOT allowed.

4.8 CERTIFICATE MODIFICATION

Certificate modification IS NOT allowed.

4.8.1 Circumstances for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

If the Subject loses control over one or more of the keys or PIN codes, the Subject SHALL apply for Certificate revocation immediately.

AK (including external RAs) has the right to revoke FA Certificates if one or more of the following occurs:

- the Subscriber or Subject requests revocation;
- AK obtains evidence that Subject has lost control over Private Keys or PIN codes;
- the Subscriber notifies AK that the original Certificate request was not authorized and does not retroactively grant authorization;
- AK obtains evidence that the Subject's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements;
- AK obtains evidence that the Certificate was misused;
- AK is made aware that a Subject has violated one or more of its obligations under the Terms and Conditions [7];
- AK is made aware of a material change in the information contained in the Certificate;
- AK is made aware that the Certificate was not issued in accordance with the CPS and/or CP;
- AK determines that any of the information appearing in the Certificate is inaccurate or misleading;
- AK ceases operations for any reason and has not planned for another CA to provide revocation support for the Certificate;
- AK's right to issue Certificates is revoked or terminated, unless AK has planned to continue maintaining the OCSP repository;
- AK is made aware of a possible compromise of the Private Key of the AK CA used for issuing the Certificate; revocation is required by the CP;
- AK determines that the cryptographic device used is no longer on the EU list of QSCDs or no longer deemed secure.

MO has the right to request revocation of FA Certificates if one or more of the following occurs:

- QSCD is replaced (for example QSCD is damaged, reset, migration to other MO, application for new Certificate);
- Subscriber's or Subject's telecommunication service contract is terminated;
- MO obtains evidence that Subject has lost control over Private Keys or PIN codes (for example SIM-card has been transferred to another person);
- the Subscriber or Subject has violated one or more of its obligations to MO (for example the Subscriber has not fulfilled its financial obligations).

4.9.2 Who Can Request Revocation

Subscriber or Subject MAY request revocation of the Subscriber's Certificates at any time.

MO, RA and CA MAY request revocation for any of the reasons listed in chapter 4.9.1 of this CP.

4.9.3 Procedure for Revocation Request

The procedure for revocation SHALL be as described in AK CPS [11] and Revocation Procedures [13].

4.9.4 Revocation Request Grace Period

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.9.5 Time Within Which CA Must Process the Revocation Request

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.9.7 CRL Issuance Frequency

CRL SHALL be issued no less than every 24 hours.

4.9.8 Maximum Latency for CRLs

Not applicable.

4.9.9 On-Line Revocation/Status Checking Availability

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.9.10 On-Line Revocation Checking Requirements

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.9.12 Special Requirements Related to Key Compromise

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.9.13 Circumstances for Suspension

Suspension IS NOT allowed.

4.9.14 Who Can Request Suspension

Suspension IS NOT allowed.

4.9.15 Procedure for Suspension Request

Suspension IS NOT allowed.

4.9.16 Limits on Suspension Period

Suspension IS NOT allowed.

4.9.17 Circumstances for Termination of Suspension

Suspension IS NOT allowed

4.9.18 Who Can Request Termination of Suspension

Suspension IS NOT allowed.

4.9.19 Procedure for Termination of Suspension

Suspension IS NOT allowed.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.10.2 Service Availability

AK SHALL ensure that its Certificate Status Services are available 24/7 with a maximum allowed outage not to exceed six (6) hours in any one disruption of the OCSP or CRL service and a minimum of 99.0% annual uptime.

4.10.3 Operational Features

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.11 END OF SUBSCRIPTION

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Not allowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Refer to chapter 6.4 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

Further information can be found in the AK Trust Service Provider Statement.

6 TECHNICAL SECURITY CONTROLS

Refer to chapter 6.5 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Private Keys for QCP-n/l-QSCD and QCP-l-NCP+ SHALL be generated in the QSCD or in a FIPS 140-2 Level 3 or CC EAL 4+ certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

For Mobile Certificates, the Private Key SHALL be generated on the SIM-card (QSCD).

For Certificates on Cards the Private Key SHALL be generated on the Card (QSCD)

For eSeals the Private Key SHALL be generated on the Crypto Stick (QSCD) provided by Auðkenni or FIPS-140-2 level 3 or Common Criteria certified HSM [14] at the customer site. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

For TSU certificates the Private Key SHALL be generated in a FIPS-140-2 level 3 or Common Criteria certified HSM [14] at the customer site. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

Non-qualified Certificates do not require QSCD or HSM.

For the App the Key Pair Generation SHALL be as follows:

- The App Server and App SHALL generate RSA key pairs independently.
- The App Server's Private Key SHALL be generated on a FIPS 140-2 Level 3 or CC EAL 4+ certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.
- The App SHALL further divide its Private Key into two parts. The two parts SHALL NOT be distinguished from random numbers.
- The App SHALL send one of these parts to the App Server over a secure communication channel.
- The App SHALL NOT store the key pair sent to the App Server and SHALL store the other part encrypted and protected with activation data.

6.1.2 Private Key Delivery to Subscriber

For Certificates on Mobile, App, and Card the Private Key is always within the QSCD.

For Certificate on eSeal the Private Key is either within the QSCD; within the Subscriber HSM, or Subscriber creates the key within own equipment (not HSM) AK never has the Private Key.

For TSU Certificate the Private Key is within the customer HSM and AK never receives the Private Key.

RA SHALL perform Subscriber Authentication in accordance with chapter 4.1.2 of this CP.

6.1.3 Public Key Delivery to Certificate Issuer

For Certificate on Mobile, App, or Card the RA SHALL hand Public Keys over to CA for registration.

For eSeals and Equipment authentication the Public Key is transferred securely to the CA.

For TSU Certificate the Public Key is transferred securely to the CA.

6.1.4 CA Public Key Delivery to Relying Parties

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.1.5 Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [6].

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

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

Allowed key usage flags SHALL be set as described in the Certificate Profile [6].

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 *Cryptographic Module Standards and Controls*

Keys SHALL be generated by a FIPS 140-2 Level 3 or CC EAL 4+ certified device or a QSCD. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

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

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.3 *Private Key Escrow*

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.4 *Private Key Backup*

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.5 *Private Key Archival*

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.6 *Private Key Transfer into or From a Cryptographic Module*

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.7 *Private Key Storage on Cryptographic Module*

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.8 *Method of Activating Private Key*

Different solutions have different requirements for activating Private Key:

- SIM on Mobile requires one PIN code for both Authentication and Signature (at least 4 digits).
- App on Smartphone requires two PIN codes, one for Authentication (at least 4 digits) and one for Signature (at least 5 digits).
- Cards require two PIN codes, one for Authentication (at least 4 digits) and one for Signature (at least 6 digits).
- eSeals require at least a 4-digit PIN code when stored on Crypto Stick.
- Equipment Authentication activation method is at the discretion of the Subscriber.
- TSU activation method is managed by the Subscriber when using own HSM.

6.2.9 *Method of Deactivating Private Key*

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.10 Method of Destroying Private Key

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.2.11 Cryptographic Module Rating

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the Subscriber Certificates SHALL NOT exceed the validity period stated in the Certificate Profile [6].

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

For Certificates on Mobile and Card there is an activation code used. At time of registration the RA asks the Subscriber to enter the issued code to verify the possession of the QSCD and following that to choose a PIN code to activate the Private Key.

For App Certificates the App creates an activation code that the RA MUST enter to activate the Private Key. If Subscriber has Mobile Certificate, then it can use that to activate.

6.4.2 Activation Data Protection

The Subscriber SHALL memorize the PIN codes and not share them with anyone.

If the PIN codes are not under the control of the Subscriber, the Subscriber SHALL apply for Certification revocation immediately.

Copies of PIN codes SHALL NOT be stored anywhere.

6.4.3 Other Aspects of Activation Data

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.5.2 Computer Security Rating

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.6.2 Security Management Controls

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.6.3 Life Cycle Security Controls

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.7 NETWORK SECURITY CONTROLS

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

6.8 TIME-STAMPING

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

7 CERTIFICATE, CRL, AND OCSP PROFILES

Refer to chapter 6.6 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

7.1 CERTIFICATE PROFILE

The Certificate SHALL comply with the profile described in the Certificate Profile [6].

7.2 CRL PROFILE

The CRL SHALL comply with the profile described in the Certificate Profile [6].

7.3 OCSP PROFILE

The OCSP responses SHALL comply with the profile described in the Certificate Profile [6].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Refer to chapter 6.7 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

9 OTHER BUSINESS AND LEGAL MATTERS

Refer to chapter 6.8 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3].

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

Refer to chapter 9.1.1 of CPS.

9.1.2 Certificate Access Fees

Refer to chapter 9.1.2 of CPS.

9.1.3 Revocation or Status Information Access Fees

Refer to chapter 9.1.3 of CPS.

9.1.4 Fees for Other Services

Refer to chapter 9.1.4 of CPS.

9.1.5 Refund Policy

Refer to chapter 9.1.5 of CPS.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.2.2 Other Assets

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

No stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.5 INTELLECTUAL PROPERTY RIGHTS

AK obtains intellectual property rights to this CP.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

An employee of CA SHALL have a clean criminal record.

9.6.2 RA Representations and Warranties

An employee of RA SHALL have a clean criminal record and receive appropriate training to perform RA duties.

9.6.3 Subscriber Representations and Warranties

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.6.4 Relying Party Representations and Warranties

Relying Party SHALL verify the validity of the Certificate using validation services offered by AK prior to relying on the Certificate.

The Relying Party SHALL consider the limitations stated in the Certificate and SHALL ensure that the transaction to be accepted corresponds to this CP.

9.6.5 Representations and Warranties of Other Participants

An employee of App service SHALL have a clean criminal record.

The Biometric Identity Verification Provider SHALL follow the requirements stipulated in the agreement concluded with AK.

9.7 DISCLAIMERS OF WARRANTIES

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.8 LIMITATIONS OF LIABILITY

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.9 INDEMNITIES

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.10 TERM AND TERMINATION

9.10.1 Term

Refer to chapter 2.2.1 Publication and Notification Policies of this CP.

9.10.2 Termination

This CP SHALL be in force until replaced by a newer version of the CP or when it is terminated due to the CA termination or when the service is terminated, and all the Certificates therefore become invalid.

This CP SHALL, even if replaced by a new version of the CP, remain in force for all Certificates issued while the CP was in force.

9.10.3 Effect of Termination and Survival

AK SHALL communicate the conditions and effect of termination of this CP.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Refer to chapter 1.5.4 of this CP.

9.12.2 Notification Mechanism and Period

Refer to chapter 1.5.4 of this CP.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation.

9.13 DISPUTE RESOLUTION PROVISIONS

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.14 GOVERNING LAW

This CP is governed by the jurisdictions of the Republic of Iceland.

9.15 COMPLIANCE WITH APPLICABLE LAW

AK SHALL ensure compliance with the following requirements:

- Electronic Identification and Trust Services for Electronic Transactions Act no. 55/2019.
- Data Protection and processing of personal data Act no. 90/2018. [8]
- Related European Standards:
  - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [9].
  - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [2].
  - ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates [3].
  - CEN EN 419 211 Protection profiles for secure signature creation device [10].

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.16.2 Assignment

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.16.3 Severability

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.16.5 Force Majeure

No stipulation in addition to QCP-n-qscd, QCP-l-qscd, QCP-l, NCP+ and NCP.

9.17 OTHER PROVISIONS

Not allowed.

10 REFERENCES

1. Electronic Identification and Trust Services for Electronic Transactions, Act no. 55/2019.
2. ETSI EN 319 411-1 V1.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements.
3. ETSI EN 319 411-2 V2.4.1 (2021-11) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
4. RFC 3647 – Request for Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, published: https://www.ietf.org/rfc/rfc3647.txt.
5. Key Words for Use in RFCs to Indicate Requirement Levels, S. Bradner, RFC2119, March 1997.
6. Certificate and OCSP Profiles for FA, published: repo.audkenni.is.
7. Terms and Conditions for Use of Certificates of FA published: repo.audkenni.is.
8. Act no. 90/2018 on Data Protection and processing of personal data.
9. ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
10. CEN EN 419 211 Protection profiles for secure signature creation device.
11. AK Certification Practice Statement published: repo.audkenni.is.
12. AK TSPS – AK Trust Service Practice Statement; repo.audkenni.is.
13. Revocation Procedures. AK Security Handbook.
14. Common Criteria – ISO/IEC Standard 15408-1/2/3:2005 – Information technology – Security techniques – Evaluation criteria for IT security