AK

Certification Practice Statement

for

Fullgilt auðkenni 2021

Version 4.5 – Effective date 29.09.2025

Change control		
Published	**Version**	**Changes**
01.11.2019	0.1	First draft version.
	1.0	First publication for Fullgilt auðkenni. Added here for consistency of version numbering.
	2.0	Second version for Fullgilt auðkenni. Added here for consistency of version numbering.
16.3.2021	3.0	1st Publication for Fullgilt auðkenni 2021
21.9.2021	3.1	Changes to version history, previous version numbers added for consistency. Approval column removed. Suspension possibility removed. Crypto Stick is defined as a future service. Changed max allowed outage in c. 4.10.2
23.10.2022	4.0	Added information about Automated Biometric Identity Verification (ABIV) in App. Added information about Time-Stamping Unit (TSU). Minor fixes to text.
15.09.2023	4.1	AK's address updated. Minor fixes to text, grammatical error fixed, cosmetic changes, harmonization in use of terms etc.
29.10.2023	4.2	Reference errors corrected. Minor addition to chapter 6.1.1.2.
11.01.2024	4.3	Minor fixes to text. Clarification added specifying that certain services are currently not available. Statement added to chapter 4.10.3.
03.06.2024	4.4	Added information about Automated Biometric Identity Verification (ABIV) in App for minors.
19.09.2025	4.5	Update of text in chapter 3.2.3 and 4.1.2.2 to include paperless process at RA. Update of text in chapter 3.2.3 regarding SIM card change via website. Update of text in chapter 4.1.2.2 regarding application in the App. Version numbers of ETSI standards updated. Minor fixes to text.

TABLE OF CONTENTS

1 INTRODUCTION 6
1.1 Overview 6
1.2 Document Name and Identification 7
1.3 PKI Participants 7
1.4 Certificate Usage 8
1.5 Policy Administration 9
1.6 Definitions and Acronyms 9
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 11
2.1 Repositories 11
2.2 Publication of Certification Information 11
2.3 Time or Frequency of Publication 11
2.4 Access Controls on Repositories 12
3 IDENTIFICATION AND AUTHENTICATION 12
3.1 Naming 12
3.2 Initial Identity Validation 12
3.3 Identification and Authentication for Re-Key Requests 15
3.4 Identification and Authentication for Revocation Request 16
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 16
4.1 Certificate Application 16
4.2 Certificate Application Processing 18
4.3 Certificate Issuance 18
4.4 Certificate Acceptance 19
4.5 Key Pair and Certificate Usage 20
4.6 Certificate Renewal 20
4.7 Certificate Re-Key 20
4.8 Certificate Modification 21
4.9 Certificate Revocation and Suspension 22
4.10 Certificate Status Services 24
4.11 End of Subscription 25
4.12 Key Escrow and Recovery 25
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 25
5.1 Physical Controls 25
5.2 Procedural Controls 25

5.3 Personnel Controls 25
5.4 Audit Logging Procedures 25
5.5 Records Archival 26
5.6 Key Changeover 26
5.7 Compromise and Disaster Recovery 26
5.8 CA or RA Termination 26
6 TECHNICAL SECURITY CONTROLS 27
6.1 Key Pair Generation and Installation 27
6.2 Private Key Protection and Cryptographic Module Engineering Controls 31
6.3 Other Aspects of Key Pair Management 39
6.4 Activation Data 39
6.5 Computer Security Controls 40
6.6 Life Cycle Technical Controls 41
6.7 Network Security Controls 41
6.8 Time-Stamping 41
7 CERTIFICATE, CRL, AND OCSP PROFILES 42
7.1 Certificate Profile 42
7.2 CRL Profile 42
7.3 OCSP Profile 42
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 42
9 OTHER BUSINESS AND LEGAL MATTERS 42
9.1 Fees 42
9.2 Financial Responsibility 43
9.3 Confidentiality of Business Information 43
9.4 Privacy of Personal Information 43
9.5 Intellectual Property rights 43
9.6 Representations and Warranties 43
9.7 Dislaimers of warranties 44
9.8 Limitations of Liability 44
9.9 Indemnities 45
9.10 Term and Termination 45
9.11 Individual Notices and Communications with Participants 45
9.12 Amendments 45
9.13 Dispute Resolution Provisions 45
9.14 Governing Law 45
9.15 Compliance with Applicable Law 46

9.16 MISCELLANEOUS PROVISIONS 46
9.17 OTHER PROVISIONS 46
10 REFERENCES 46

1 INTRODUCTION

1.1 OVERVIEW

This document is the Certification Practice Statement (CPS) which describes the practices used to comply with the AK Certificate Policy for Fullgilt auðkenni 2021 (CP) [1]. The full CA hierarchy is described in the TSPS.

The certification service for Qualified Electronic Signature Certificate described in this CPS has qualified status in the Trusted List of Iceland.

The CP is compliant with ETSI EN 319 401 [11], ETSI EN 319 411-2 Policy: QCP-n-qscd, QCP-l-qscd, QCP-l [6] and ETSI EN 319 411-1 Policy: NCP+ and NCP [7]. AK always ensures compliance with the latest versions of the referred documents.

In case of conflicts the documents are considered in the following order (prevailing ones first):

- ETSI EN 319 411-2 V2.6.1 (2025-06);
- ETSI EN 319 411-1 V1.5.1 (2025-04);
- ETSI EN 319 401 V3.1.1 (2024-06);
- CP; and
- this CPS.

The Certificates issued by FA under this CPS 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 content and format of the present document complies with the requirements of the IETF RFC 3647 [2] framework.

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

This document is named "AK Certification Practice Statement for Fullgilt auðkenni 2021."

This CPS 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) cps(6) } This can also be written as {2.16.352.1.2.1.1.6}. The OID for this CPS is fixed and will not change with new versions of this document.

The following OID are used as described in the table:

Service Type	OID	QCP-n-qscd	NCP+	NCP
Cards natural person	2.16.352.1.2.10.1	0.4.0.194112.1.2	0.4.0.2042.1.2	NA
Cards natural person + legal person	2.16.352.1.2.10.2	0.4.0.194112.1.2	0.4.0.2042.1.2	NA
Mobile	2.16.352.1.2.11.1	0.4.0.194112.1.2	0.4.0.2042.1.2	NA
App on Smartphone – Qualified	2.16.352.1.2.12.1	0.4.0.194112.1.2	0.4.0.2042.1.2	NA
App on Smartphone – Non-Qualified	2.16.352.1.2.12.2	NA	0.4.0.2042.1.2	NA
		QCP-l-qscd	**QCP-l (NCP+)**	**NCP**
eSeal – QSCD	2.16.352.1.2.13.1	0.4.0.194112.1.3 Future service	NA	NA
eSeal – Advanced	2.16.352.1.2.13.2	NA	0.4.0.194112.1.1 0.4.0.2042.1.2	NA
eSeal – Advanced soft	2.16.352.1.2.13.3	NA	NA	0.4.0.194112.1.1 0.4.0.2042.1.1
Equipment Authentication	2.16.352.1.2.14.1	NA	NA	0.4.0.2042.1.1
TSU	2.16.352.1.2.14.2	NA	0.4.0.2042.1.2	NA

1.3 PKI PARTICIPANTS

The participants applying the services provided within the framework of the current CPS are the following:

- Auðkenni ehf. – The Certification Authority;
- Customers of Auðkenni (Subscribers and Subjects);
- Relying Parties; and
- Registration Authority – Auðkenni and subcontractors.

1.3.1 Certification Authorities

AK operates as a Certification Authority that issues Certificates for Mobile, Cards, App on Smartphone; eSeals, and TSU signature verification (public) key certificates.

The certification service provided by AK includes by default all the procedures related to the life cycle of the pairs of keys and Certificates, which are described in this CPS.

The Certificates are issued by the intermediate CA Fullgilt auðkenni 2021.

1.3.2 Registration Authorities

AK operates as a Registration Authority and runs a registration system for enrollment procedures for end-user certificates applicants. AK performs enrollment and has contracts with subcontractors that perform enrollment procedures using the AK Registration system. A list of RA subcontractors can be found at Auðkennis website.

All RAs can register applications for Certificates on SIM, App on Smartphones and Cards. Only AK can issue Certificates for eSeals. All subcontractors use the same RA system provided by AK.

In case of electronic authentication and automated biometric identity verification RA duties are performed by the App.

Customers can call +354-530-0000 24/7 to get assistance or to revoke Certificates. After office hours there is a phone answering that offers customers to get emergency assistance. The customer is then transferred to a 24-hour help desk.

1.3.3 Subscribers

Refer to chapter 1.3.3 of the CP for Fullgilt auðkenni 2021 [1].

1.3.4 Relying Parties

A Relying Party is a natural or legal person who decides to rely on the Certificates issued by AK.

1.3.5 Other Participants

Other participants are different sub-contractors or government entities that provide different parts of the CA and RA operations for Auðkenni.

Other participants are:

- Hosting provider 1
  - Emergency help line outside regular office hours.
  - Provides hosting, physical security, uninterrupted power, cooling, and related services.
- MO
  - Provide SIM-cards able to generate Certificates issued by FA. Cards are provided by SIM-card manufacturers.
  - Facilitate communication between CA and Subscribers when using Certificates on Mobile.
- Hosting provider 2
  - Provides App server services.
  - Provides Automated Biometric Identity Verification.
- Answering service
  - First level support and answering service.
- Software and hardware service providers
  - CA system
  - RA system
  - SIM-card providers
  - OCSP vendor
  - HSM vendor
  - Middleware for SIM-cards and other cards
  - Card provider
- Crypto Stick provider

1.4 CERTIFICATE USAGE

Refer to chapter 1.4 of the CP.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

This CPS is administered by Auðkenni.

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 CPS Approval Procedures

Amendments which do not change the meaning of this CPS, 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 is increased by one.

In case the CP is amended, the CPS is reviewed as well to verify the need for amendments.

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

This CPS shall be reviewed annually.

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

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Terminology

In this CPS, the following terms have the following meaning.

Term	Definition
App	Mobile application that works as a QSCD. Used on Smartphones 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 its biometric characteristics.
Card	QSCD on a plastic card.
Certificate	Public key, together with some other information, laid down in the Certificate Profile [2], 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 or 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 intermediary certificate, the Certificates of which enabling electronic identification and electronic signature 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 eIDAS [8].
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 [8].
Qualified Certificate for Electronic Signatures	Qualified Certificate for Qualified Electronic Signatures according to eIDAS [8].
Qualified Electronic Signature Creation Device (QSCD)	A Secure Signature Creation Device that meets the requirements laid down in eIDAS [8].
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	Natural or legal person 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	A 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 [9] 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
AES	Advance encryption standard
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 [8] 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 Regulation, implemented into Icelandic law by act no. 55/2019
eMRTD	Electronic Machine-Readable Travel Document. Identity or travel document 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
HMAC	Hash-based messaged authentication codes
HSM	Hardware Security Module
KWK	Key-wrap-keypair
MO	Mobile Operator
MRZ	Machine-Readable Zone
NCP+	Normalized Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [7]
NFC	Near field communication
OCSP	Online Certificate Status Protocol
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.
RA	Registration Authority
SCM	SIM-card Manufacturer
SIM	SIM-card used in Mobile
TLS	Transport Layer Security
TSPS	Trust Service Practice Statement
TSU	Time-Stamping Unit

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Refer to chapter 2.1 of AK TSPS [3].

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Refer to chapter 2.2 of AK TSPS [3].

2.2.1 Publication and Notification Policies

This CPS is published on AK's website: repo.audkenni.is.

Profiles for Certificates on Mobile, App on Smartphone, Cards, eSeals, and TSU Certificates as well as the Terms and Conditions together with the enforcement dates are published on AK's website repo.audkenni.is no less than ten days prior to taking effect.

AK provides the capability to allow third parties to check and test Certificates it issues.

Test Certificates clearly indicate that they are for testing purposes. Test certificates are available at repo.audkenni.is.

2.2.2 Items not Published in the Certification Practice Statement

Refer to chapter 2.2.2 of the CP.

Refer to chapter 9.3.1 of AK TSPS [3].

2.3 TIME OR FREQUENCY OF PUBLICATION

Refer to chapter 2.2.1 of this CPS.

2.4 ACCESS CONTROLS ON REPOSITORIES

Refer to chapter 2.4 of AK TSPS [3].

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Type of Names

Type of names assigned to the Subscriber is described in the Certificate Profiles for the different Certificates.

3.1.2 Need for Names to be Meaningful

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

Meaning of names in different fields of the Certificates is described in the Certificate Profiles for the different Certificates.

3.1.3 Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

Refer to chapter 3.1.5 of the CP.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

Refer to chapter 3.2.1 of the CP.

3.2.2 Authentication of Organization Identity

RA verifies the organizational identity by consulting the official government company registry or by looking up information from other government or other trusted 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

The Subscriber's identity is verified either pursuant to current legislation based on physical presence, according to article 24.1.c of eIDAS, or according to article 24.1.d of eIDAS for ABIV.

For physical presence:

- The authorized employee must verify the identity of the Subscriber based on an identity or travel document, e.g., passport, driver's license or identity card accepted by AK.
- Information to be inserted into the Certificate is fetched from the National Registry.
- The authorized employee verifies compliance between the information from the identity document with the information from the National Registry.
- The authorized employee must perform further verification in case the Subscriber has an active Certificate, by sending an additional authentication to one or more of the Subscriber's contact information and the Subscriber needs to verify.
- The authorized employee must either upload a copy of the submitted identity document or verified biometric data based on the information read from the chip in the identity document via ABIV into the RA system.
- The authorized employee must prepare an application in connection with the delivery of the Certificate.
- The Subscriber must sign the application; In case the Subscriber is a legal entity a Subscriber's representative has already signed the application, the Subject signs for receiving the Certificate.
- AK must archive the copy made of the Subscriber's identity document together with the signed application for at least 10 years after the validity of the relevant Certificate.

In the case of a minor, AK checks from reliable source the identity of the Subject's legal representative and legal representative's right of representation. The Subject's legal representative signs the application for Certificate on App with a Qualified Electronic Signature issued by AK and compliant with eIDAS and confirms the correctness and integrity of the information presented to AK. The identification of the minor and legal representative is performed in accordance with identification chapter 3.2.3 of this CPS.

For self-registration:

- Based on Qualified Certificate issued according to eIDAS
    - SIM card change via website
        - Only Qualified Certificates issued through physical presence can be used to apply for a Certificate through Self-Registration process.
        - MO registers new SIM card for Subscriber and notifies the RA system.
        - Subscriber logs on to mitt.audkenni.is website using a Qualified Certificate issued by FA.
        - Subscriber applies for a new Certificate for the new SIM card.
        - The Subscriber is shown the Application and accepts or denies it by selecting the appropriate button.
        - Information to be inserted into the Certificate is fetched from the National Registry and compared with the Certificate used to login.
        - RA system verifies the identity of the Subscriber from the Qualified Certificate used to log on.
        - RA system validates the Qualified Certificate checking that it has not been revoked and makes sure the identification evidence is connected to the current application.
        - Subscriber signs the application with a Qualified Electronic Signature using the current SIM card thereby proving identity.
        - The RA system initiates the issuance of the Certificate for the new SIM card.
        - The RA system stores the signed application and other evidence for at least 10 years after the validity of the relevant Certificate.

- Based on ABIV via App
    - The Subscriber starts the App and selects to apply for a Qualified Certificate using biometric verification.
    - The Subscriber's unequivocal consent for the ABIV process is acquired.
    - The Subscriber's identity is verified based on the information read from the chip in the identity document presented by the Subscriber for identity validation.
    - The authenticity of the chip is verified based on the authentication mechanism supported by the chip and by verifying data read from the MRZ or CAN number in the identity document. Validity check of the information read from the identity document is based on an authoritative source.

- Biometric verification of the Subscriber is based on the facial image retrieved from data on the chip with NFC technology and the facial image captured in the liveness session during registration via the App.
- During the liveness session, the liveness of the Subscriber's facial image is verified.
- App receives the success or failure result for the identity verification from the hosting provider. If failure the process stops.
- Information to be inserted into the Certificate is fetched from the National Registry based on the user's identification number.
- The Subscriber is shown the Terms and Conditions and accepts or denies them by selecting the appropriate button in the App.
- The Subscriber is asked to select PIN1 and PIN2 to associate with the new Certificates.
- The Subscriber is asked to verify identity information i.e., identification number and name.
- Once the Subscriber has verified the information the Subscriber is asked to enter PIN1 and PIN2 for verification.
- The App initiates the issuance of the Certificate.
- The App creates an application and asks the user to sign with the newly issued Certificate using PIN2. The issued Certificate can only be used to sign the application. If the application is not signed the App automatically initiates a revocation of the Certificate and stops the process. If the application is signed, then the restriction is removed from the Certificate.
- The RA system stores the signed application and other evidence for at least 10 years after the validity of the relevant Certificate.

- Based on ABIV via App for minors
  - The Subject (the minor) starts the App and selects to apply for a Qualified Certificate using biometric verification.
  - The Subject's unequivocal consent for the ABIV process is acquired. The consent for the ABIV process is confirmed by the Subject's legal representative as well through the signing of the application.
  - The Subject is required to confirm that it has read and understood the Terms and Conditions on the use of the account.
  - The Subject's identity is verified based on the information read from the chip in the identity document presented by the Subject for identity validation.
  - The authenticity of the chip is verified based on the authentication mechanism supported by the chip and by verifying data read from the MRZ in the identity document. Validity check of the information read from the identity document is based on an authoritative source.
  - The Subject is asked to select PIN1 and PIN2.
  - Keys are generated.
  - The App creates an application which the Subject´s legal representative is required to sign with a qualified Certificate, accept the General Terms and Conditions and confirm the consent for the ABIV process. The Subject cannot move forward with the process until the application has been signed by a legal representative.
  - The App generates a link to sign the application, which the Subject is required to share with its legal representative(s). Only registered legal representatives can sign the application. AK verifies the right of representation of the Subject's legal representative and keeps evidence for that.
  - Once the application has been signed, biometric verification of the Subject is based on the facial image retrieved from data on the chip with NFC technology and the facial image captured in the liveness session during registration via the App.
  - During the liveness session, the liveness of the Subject's facial image is verified.
  - App receives the success or failure result for the identity verification from the hosting provider. If failure the process stops.
  - Information to be inserted into the certificate is fetched from the National Registry based on the Subject's identification number.
  - The Subject is asked to verify identity information i.e., identification number and name.
  - Once the Subject has verified the information the Subject is asked to enter PIN1 and PIN2 for verification.

- The App initiates the issuance of the Certificate.
- The Subject is required to confirm the information in the certificate.
- The App finalizes the issuance of the Certificate.
- The RA system stores the signed application and other evidence for at least 10 years after the validity of the relevant Certificate.

3.2.3.1 Card

The Subscriber must apply for Certificate on Card at Auðkennis website before arriving at the RA. The Subscriber goes through the normal RA validation procedure for a Certificate as described in chapter 3.2.3.

Self-registration is not possible for Certificates on Cards.

3.2.3.2 App on Smartphone

The Subscriber installs the App on Smartphone and goes through the normal RA procedures to apply for a Certificate as described in chapter 3.2.3.

3.2.3.3 Mobile

MO provides a non-personalized SIM-card to their customer. The customer then goes through normal RA procedures to apply for a Certificate as described in chapter 3.2.3.

3.2.3.4 eSeal and Equipment Authentication

Process of chapter 3.2.2 is used.

3.2.3.5 TSU

Process of chapter 3.2.2 is used.

3.2.4 Non-Verified Subscriber Information

Non-verified information IS NOT allowed in the Certificate.

3.2.5 Validation of Authority

For Certificates on Mobile, App on Smartphone and Cards the Subscriber can only apply personally. AK checks whether the Subscriber has legal capacity. If a minor applies for a Certificate, AK verifies the right of representation of the minor's legal representative and keeps evidence for that.

When applying on behalf of an organization the representative must be authorized to sign on behalf of the organization. Authorization is checked through the official company registry or by looking up information from other official sources and matching the information from the applicant.

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

Refer to chapter 4.9.3 of this CPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

Certificate Subject or Subscriber can submit a Certificate Application. Refer further to chapter 4.1.1 of the CP.

4.1.2 Enrolment Process and Responsibilities

The Subscriber WILL apply for Certificates via RA, self-registration website, via App on Smartphone (CURRENTLY NOT AVAILABLE) or via ABIV.

Enrolment SHALL be according to chapter 4.1.2 in the CP.

4.1.2.1 Card

For Certificates on Cards the Subscriber must apply at Auðkennis website before arriving at the RA. Subscriber will be shown the finalized application including a linked reference to Terms and Conditions and asked to sign the application, thus confirming the terms. RA provides the Subject with a Card (QSCD) at the time of validation. The Subject goes through the physical identification process described in chapter 3.2.3 of this CPS. A signed copy of the application is stored. RA verifies that issued QSCD has been previously registered in its database and can check the data in the request against the data in a reliable source using an automatic procedure.

Once the application is signed the RA system issues a key generation command to the Card and then issues the Certificate. The identification process is performed as described in chapter 3.2.3 of this CPS.

4.1.2.2 App on Smartphone

For App on Smartphone Certificate the Subscriber can apply via:

- RA office
- App on Smartphone

To **apply via an RA office** the Subscriber must show up physically at the RA, start the application via the App on Smartphone by showing a code provided by the App to the RA officer. Afterward the Subscriber goes through the physical identification process in chapter 3.2.3. The Subscriber is presented with the Terms and Conditions and signs an application either via App or on paper. The application for App on Smartphone includes the Subscriber's identification data, email address or mobile phone number. The RA system issues a key generation command and then issues the Certificate. A signed paper application is sent to AK where it is scanned and uploaded into the RA system. The signed application is stored in the paper archives or case of electronic copy in database archives.

To **apply via the App on Smartphone** the Subscriber must authenticate via ABIV as described in chapter 3.2.3.

The App receives the success or failure result for the identity verification from the hosting provider. If there is a failure the process stops. Information to be inserted into the Certificate is fetched from the National Registry based on the user´s identification number. The Subscriber is shown the Terms and Conditions and accepts or denies them by selecting the appropriate button in the App. The Subscriber is asked to select PIN1 and PIN2 to associate with the new Certificates. The Subscriber is asked to verify identity information and asked to enter PIN1 and PIN2 for verification. Then the App initiates

the issuance of the Certificate, as further described in chapter 3.2.3, signs an application with the newly issued Certificate using PIN2. The RA system stores the signed application and other evidence. The identification process is performed in accordance with the self-registration process in chapter 3.2.3 of the CPS.

In the case of a minor, AK checks from reliable source the identity of the Subject's legal representative and legal representative's right of representation. The Subject's legal representative signs the application for Certificate on App with a Qualified Electronic Signature issued by AK and compliant with eIDAS and confirms the correctness and integrity of the information presented to AK. The identification of the minor and legal representative is performed in accordance with identification chapter 3.2.3 of this CPS.

4.1.2.3 Mobile

The customer has a QSCD from the MO. Keys are generated on the QSCD and the Private Key never leaves the QSCD.

RA verifies that issued QSCD has been previously registered in its database and can check the data in the request against the data in a reliable source using an automatic procedure.

In case of positive evaluation, Certificates are issued by the CA.

4.1.2.3.1 RA On site Application

The Subscriber applies for a certificate at the RA, is presented with the Terms and Conditions and signs an application. The enrolment process is according to chapter 4.1.2 of the CP.

4.1.2.3.2 RA Electronic Application – CURRENTLY NOT AN OPTION

Subscriber logs into the mitt.audkenni.is portal and applies for a Certificate to be associated with the QSCD. The Subscriber must log in with a Qualified Certificate issued by FA through physical presence. Once logged in the Subscriber can apply for a new Certificate for the QSCD.

The Subscriber is presented with the Terms and Conditions and digitally signs the application with a Qualified Electronic Signature, and RA issues a command to generate two key pairs on the QSCD. Upon creation of the keys AK uses corresponding Public Keys for Certification. Private Keys never leave the QSCD.

RA archives the Subscriber's electronically signed application.

4.1.2.4 eSeal and Equipment Authentication

The Subscriber SHALL apply online at Auðkennis website. Online application presents the Subscriber with the Terms and Conditions, verifies all identification numbers of the legal entity, the authorized person and the technical person, and cross [checks with official sources. The RA verifies the legal capacity of the authorized person of the application by checking official registers and other reliable sources.

The authorized person and technical contact receive an email with a link to confirm the email address. The authorized person is then required to sign the application. The RA requires the application to be signed by the authorized person electronically with a qualified signature issued by AK. The signature in the contract is verified being qualified, valid, and not revoked.

In case the customer creates the keys in own HSM the customer must confirm that the keys have been created using FIPS 140-2 level 3 or Common Criteria [13] certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode. The customer sends the CSR during the application process.

In case that AK creates the keys, the keys will be created in a QSCD (Crypto Stick) or in an HSM and delivered in a secure manner. The use of Crypto Stick is a future service.

For non-qualified Equipment Authentication, the Subscriber submits a CSR as part of the online application. The RA never receives a copy of the keys, and 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.

4.1.2.5 TSU

Subscriber SHALL apply online at Auðkennis website. Online application presents the Subscriber with the Terms and Conditions, verifies all identification numbers of the legal entity, the authorized person and the technical person, and cross

checks with official sources. The RA verifies the legal capacity of the authorized person of the application by checking official registers and other reliable sources.

The authorized person and technical contact receive an email with a link to confirm the email address. The authorized person is then required to sign the application. The RA requires the application to be signed by the authorized person electronically with a qualified signature issued by AK. The signature in the contract is verified being qualified, valid, and not revoked.

In case the customer creates the keys in own HSM the customer must confirm that the keys have been created using FIPS 140-2 level 3 or Common Criteria certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

The customer sends the CSR during the application process. Annual Control of QSCD

Refer to chapter 4.1.3 of TSPS [3].

4.2 CERTIFICATE APPLICATION PROCESSING

For Certificates on Cards, Mobile and App on Smartphone the Subscriber and / or Subject is identified in accordance with chapter 3.2.3 of this CPS.

4.2.1 Performing Identification and Authentication Functions

For eSeal certificates the Subscriber is identified in accordance with chapter 3.2.2 of the CPS.

4.2.2 Approval or Rejection of Certificate Applications

Refer to chapter 4.2.2 of the CP.

AK notifies Subscriber of the refusal to issue a Certificate.

4.2.3 Time to Process Certificate Applications

Refer to chapter 4.2.3 of the CP.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

4.3.1.1 Card

After checking the authenticity and integrity of the Certificate application received from the RA, CA automatically issues the corresponding Certificates. Certificates are loaded onto the Card by the RA.

4.3.1.2 App on Smartphone

After verifying the data contained in the CSR, AK automatically issues Certificates corresponding to the application.

4.3.1.3 Mobile

After AK has verified that the issued QSCD has been previously registered in AK's database, CA automatically issues corresponding Certificates.

4.3.1.4 eSeal and Equipment Authentication

After AK has verified that the QSCD used to create the keys is FIPS-140-2 Level 3 or Common Criteria certified, CA issues corresponding Certificates. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

For non-qualified Equipment Authentication, no further checks are required before the CA issues Certificates.

4.3.1.5 TSU

After AK has verified that the HSM used to create the keys is FIPS-140-2 Level 3 or Common Criteria certified, CA issues corresponding Certificates. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

4.3.2.1 Card

The Subscriber or Subject are immediately notified by the RA officer at time of registration and Subscriber receives email notification.

4.3.2.2 App on Smartphone

The Subscriber is immediately notified of the results by the App as the whole process is done online in real time.

4.3.2.3 Mobile

CA notifies the Subscriber of the new Certificate issuance. All notification is through the RA system at time of registration, through SMS messages to the Subscriber or the RA officer gives verbal notice to the Subscriber.

4.3.2.4 eSeal and Equipment Authentication

The Subscriber is notified by the RA of registration through email.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 Card

The Subscriber confirms familiarization and accepts the Terms and Conditions by signing an application. The signed application is stored in the RA system.

This is deemed Certificate acceptance.

4.4.1.2 App on Smartphone

The Subscriber verifies the correctness of the data shown to him during application and consequently the CA issues the Certificates. After the issuance of the certificate the Subscriber verifies again the correctness of the data shown to him. This is deemed Certificate acceptance.

4.4.1.3 Mobile

The Subscriber confirms familiarization and accepts the Terms and Conditions by signing an application. The signed application is stored in the RA system.

This is deemed Certificate acceptance.

4.4.1.4 eSeal and Equipment Authentication

The Subscriber picks up the Crypto Stick at the RA office. This is deemed Certificate acceptance.

In case the Subscriber creates the key pair in own equipment the download, from AK servers, of the Certificate by the Subscriber is deemed Certificate acceptance.

For non-qualified Equipment Authentication, the download of the certificate by the Subscriber is deemed Certificate acceptance.

4.4.1.5 TSU

As the Subscriber creates the key pair in own equipment the download, from AK servers, of the Certificate by the Subscriber is deemed Certificate acceptance.

4.4.2 Publication of the Certificate by the CA

The status of the Certificates is made available through OCSP and CRL. Subscribers can access their own Certificates for Certificates on Mobile and Certificates on App through mitt.audkenni.is portal. All Certificates are available through API service.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

4.4.3.1 Card

CA notifies the RA of the issued Certificate.

4.4.3.2 App on Smartphone

The Certificates are automatically published to the App System by CA.

4.4.3.3 Mobile

CA notifies the RA of the issued Certificate.

4.4.3.4 eSeal and Equipment Authentication

CA notifies the RA of the issued Certificate.

4.4.3.5 TSU

CA notifies the RA of the issued Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber's Private Key and Certificate Usage

Subscriber is required to use the Private Key and Certificate lawfully and in accordance with:

- the CP;
- this CPS; and
- the Terms and Conditions.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Party is required to use the Subscriber's Public Key and Certificate lawfully and in accordance with:

- the CP;
- this CPS; and
- the Terms and Conditions.

4.6 CERTIFICATE RENEWAL

Renewal IS NOT allowed.

4.7 CERTIFICATE RE-KEY

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

Re-key IS NOT allowed.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Re-key IS NOT allowed.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Re-key IS NOT allowed.

4.8 CERTIFICATE MODIFICATION

Certificate modification IS NOT allowed.

4.8.1 Circumstances for Certificate Modification

Certificate modification IS NOT allowed.

4.8.2 Who May Request Certificate Modification

Certificate modification IS NOT allowed.

4.8.3 Processing Certificate Modification Requests

Certificate modification IS NOT allowed.

4.8.4 Notification of New Certificate Issuance to Subscriber

Certificate modification IS NOT allowed.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Certificate modification IS NOT allowed.

4.8.6 Publication of Modified Certificate by the CA

Certificate modification IS NOT allowed.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate modification IS NOT allowed.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

Refer to chapter 4.9.1 of the CP.

4.9.2 Who Can Request Revocation

Refer to chapter 4.9.2 of the CP.

4.9.3 Procedure for Revocation Request

For Certificates on Cards, Mobile and App on Smartphone the Subject or Subscriber can request revocation:

- By using mitt.audkenni.is website.
- By going to the Auðkenni RA office during business hours.
- By calling the help line.
- By deleting the account in App on Smartphone (only certificates on App).
- By disconnecting the mobile phone number (certificates on Mobile only).

In the case of legal persons, the Subscriber can request revocation for Cards, eSeal and Equipment Authentication certificates via the fyr.audkenni.is website by logging in with electronic certificates.

The identity of the applicant for revocation is verified according to the *Revocation Procedures [12]* The application for revocation of Certificates should include the following information:

- The name of the Subscriber and Subject (if different).
- Identification number of the Subscriber and Subject (if different).
- For Mobile
    - Phone number.
- For App
    - Device identification (account number).
- For Card
    - Serial number of the Certificate.
- For eSeal
    - Serial number of the Certificate.
- For Equipment Authentication
    - Serial number of the Certificate.
- For TSU
    - Serial number of the Certificate.
- Grounds for revocation.

The person filing an application for revocation is identified according to the *Revocation Procedures [12]* and the legality to request revocation is established by the RA. If positive identification is not reached within 24 hours from request the revocation request is rejected otherwise if the request fulfils the requirements for revocation, the request is accepted and is processed immediately.

After RA receives an application for revocation, the procedure for processing the request is the following for all products:

- the Certificate is marked as revoked in the certificate database;
- a new CRL is published according to chapter 4.9.7 of this CPS;
- the documentation on which the application for revocation was based is archived;

- the Subscriber is notified of revocation of the Certificate via;
  - For Mobile
    - SMS sent to Subject's phone and email if email information exists.
  - For App
    - Message in App and email if email information exists.
  - For Card
    - Email sent to Subject and Subscriber.
  - For eSeal and Equipment Authentication
    - Email sent to Subscriber.
  - For TSU
    - Email sent to Subscriber.
- OCSP is updated immediately after the application for revocation is recorded in the RA system and no longer responds with "GOOD".

The revocation of the Certificate is recorded in the certificate database of CA. The Subscriber has a possibility to ascertain based on the CRL or OCSP that the Certificate has been revoked.

Revoked Certificate cannot be reinstated.

When the phone number is disconnected from a SIM-card (QSCD) the Mobile Certificate on the SIM-card is revoked automatically. If the Subscriber is issued a new QSCD for the same phone number or changes MO, the previous Mobile Certificates are immediately revoked without further input from the Subscriber. No application for revocation is necessary.

4.9.4 Revocation Request Grace Period

If the Subscriber suspects that the security of the Certificate has been put in danger the Subscriber is required to request revocation immediately.

4.9.5 Time Within Which CA Must Process the Revocation Request

CA processes an application for revocation immediately after the RA has verified the correctness and completeness of the corresponding application as well as applicant's authority to request revocation, within 24 hours, at the latest. The status of the certificate SHALL be changed within 60 minutes from the confirmation of revocation.

4.9.6 Revocation Checking Requirements for Relying Parties

The mechanisms available to a Relying Party to check the status of Certificates on which it wishes to rely have been established in the Terms and Conditions.

4.9.7 CRL Issuance Frequency

The value of the next Update field of CRL is set to 18 hours after issuance of CRL.

CRL is signed by FA. CRL is offered for all products.

4.9.8 Maximum Latency for CRLs

CRL expires 24 hours from issuance. AK monitors the expiry time of the most recent CRL. If a new CRL is not published 6 hours before expiry of the previous one, an alarm is raised.

4.9.9 On-Line Revocation/Status Checking Availability

OCSP service serves as a primary source for the Certificate status information and contains Certificate status information until the Certificate expires.

4.9.10 On-Line Revocation Checking Requirements

The mechanisms available to a Relying Party for checking the status of the Certificate on which it wishes to rely have been established in the Terms and Conditions.

4.9.11 Other Forms of Revocation Advertisements Available

The CRL list is available at crl.audkenni.is.

4.9.12 Special Requirements Related to Key Compromise

Not applicable.

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

AK offers CRL and OCSP services for checking certificate status.

The URL of the CRL service is included in the Certificate in accordance with the Certificate Profile.

The URL of the OCSP service is included in the Certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile for Cards, the Certificate Profile for App, Certificate Profile for eSeals, Certificate Profile for TSU, and the Certificate Profile for Mobile.

For Qualified Certificates, the revocation status will be made available beyond the validity period of the Certificate. Revoked Certificates are not removed from the CRL. The OCSP service only responds with "GOOD" for Certificates that are issued and not for revoked or suspended Certificates.

4.10.2 Service Availability

AK ensures availability of OCSP and CRL Certificate Status Services 24/7. CRL is for information purposes only and is issued every 18 hours. Relying Parties will have to decide which service they use knowing the difference. The maximum allowed outage is 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

In case of App on Smartphone the TSP manages part of the Subject´s Private Key. At the time of use of the Subject´s Private Key the TSP assures that the Certificate is valid at the time by making an OCSP request.

4.11 END OF SUBSCRIPTION

The maximum validity period of the Certificate is described in the different Certificate Profiles.

The subscription ends at the latest when the Certificate expires. The Subscriber (or AK) may end a subscription for the Certificate by revoking the Certificate without replacing it.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

AK does not provide the Subscriber with key escrow and recovery services.

Storing the components of the split private key of Certificates on App in the App server is not considered a key escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

Refer to chapter 5.1 of AK TSPS [3].

5.2 PROCEDURAL CONTROLS

Refer to chapter 5.2 of AK TSPS [3].

5.3 PERSONNEL CONTROLS

Refer to chapter 5.3 of AK TSPS [3].

5.4 AUDIT LOGGING PROCEDURES

Refer to chapter 5.4 of AK TSPS [3].

Audit log of events related to preparation of QSCD is kept.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

Refer to chapter 5.5.1 of AK TSPS [3].

All records from the issuance process and from requests for revocation are retained by RAs and archived in accordance with relevant regulations.

5.5.2 Retention Period for Archive

Refer to chapter 5.5.2 of AK TSPS [3].

5.5.3 Protection of Archive

Refer to chapter 5.5.3 of AK TSPS [3].

5.5.4 Archive Backup Procedures

Refer to chapter 5.5.4 of AK TSPS [3].

5.5.5 Requirements for Time-Stamping of Records

Refer to chapter 5.5.5 of AK TSPS [3].

5.5.6 Archive Collection System (Internal or External)

Refer to chapter 5.5.6 of AK TSPS [3].

RAs may use an internal archive collection system for physical archive records.

AK collects physical records from RA and scans them for storage and archives them. Physical records are stored with an external storage service provider. Electronic records are archived in AK systems.

5.5.7 Procedures to Obtain and Verify Archive Information

Refer to chapter 5.5.7 of AK TSPS [3].

5.6 KEY CHANGEOVER

The Public Key of the CA does not change. The Public Key for the OCSP responder is sent inside the OCSP response, through which a change of key is known.

If necessary, details of a key changeover are considered each time. The common name of the CA always contains “Fullgilt auðkenni”.

5.7 COMPROMISE AND DISASTER RECOVERY

Refer to chapter 5.7 of AK TSPS [3].

5.8 CA OR RA TERMINATION

Refer to chapter 5.8 of AK TSPS [3].

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

Refer to chapter 6.1 of AK TSPS [3].

6.1.1 Key Pair Generation

Refer to chapter 6.1.1 of AK TSPS [3].

6.1.1.1 Card

The Private Keys are generated by the QSCD compliant Card. Only Cards on the EU QSCD list are allowed. The keys never leave the Card. The Subject keys are protected by the activation PIN codes that the Subject selects by entering them on a secure PIN pad during the registration process. Subjects can change the PIN codes with the Card middle ware provided that the Subject knows the current PIN code.

6.1.1.2 App on Smartphone

App on Smartphone Key Pair Terminology

App Key Pair is generated with multiple components for additional protection and cryptographic properties. The following terminology is used to describe the technical security controls:

Public Key - is the public verification key in public-key cryptography. This corresponds to the regular RSA Public Key. The relation between the *Public Key* and a *Subscriber's identity* is attested by a Certificate. Public Key has the following components**:**

- *App's share of the Public Key* and
- *Server's share of the Public Key*.

App's share of the Public Key - is generated in the App, along with the generation of the *App's share of the Private Key*'.

Server's share of the Public Key - is generated in the App server, along with the generation of the *Server's share of the Private Key*'.

Private Key - is the confidential component of the key pair in public-key cryptography. *Private Key is* used for creating electronic signatures. In the App system, the value of *Private Key* itself is never generated, and the *Private Key* exists only in the form of its components. *Private Key* has the following components:

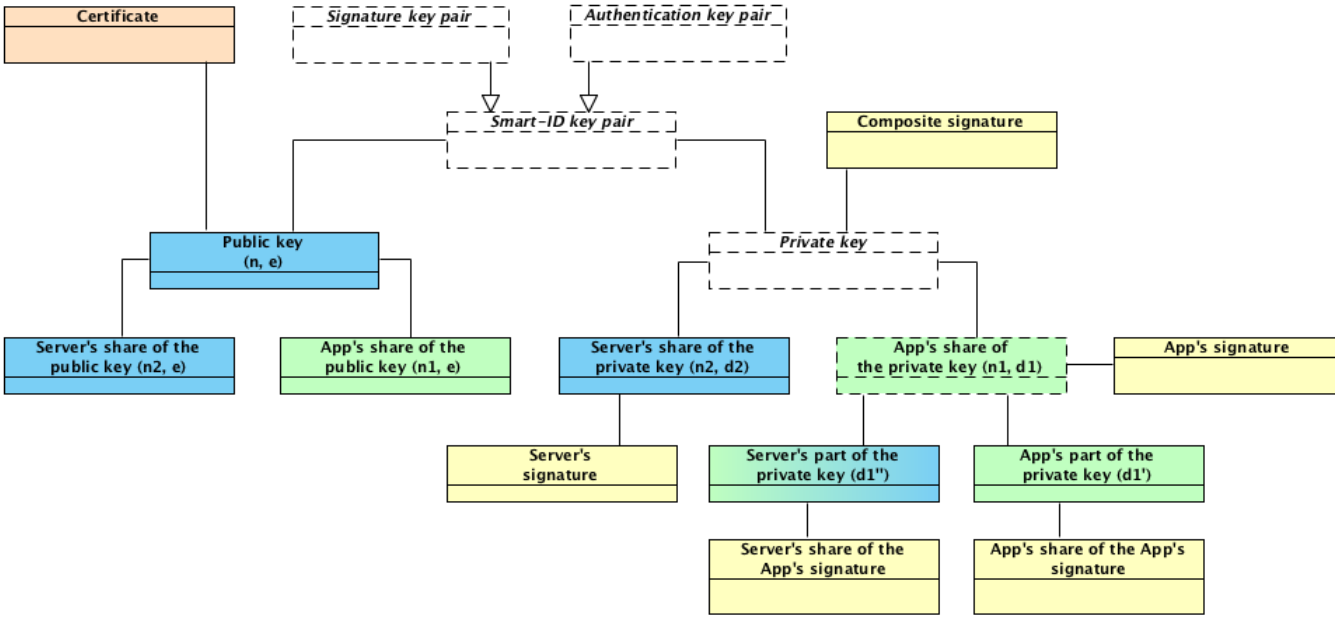
- *App's share of the Private Key*, which is a regular RSA Private Key. It is further divided to the following components:
  - *App's part of the Private Key* and
  - *Server's part of the Private Key*
- *Server's share of the Private Key*, which is a regular RSA Private Key.

App's share of the Private Key - is the component of the Private Key that is generated in the App. The share is divided into two parts immediately after generation and the share itself is deleted.

App's part of the Private Key - is the component of the Private Key, which is generated in the App and stored in the App and is protected with the Subscriber's PIN-code. The Subscriber is obligated to keep this part of the Private Key under the Subscriber's sole control.

Server's part of the Private Key - is the component of the Private Key, which is generated in the App and securely transmitted to the server. *Server's part of the Private Key* is stored in the server's database and protected with Key-Wrapping-Key, which in turn, is protected by the HSM.

Server's share of the Private Key - is the component of the Private Key, which is generated in the HSM and protected by the HSM.



6.1.1.2.1 App Key Pair Generation

Subscriber Key Pair is generated during the App registration process in the App and in the App server. The following components are generated.

Generation of *App's share of the Private Key* and *App's share of the Public Key*

App's share of the Private Key and *App's share of the Public Key* is a 3072-bit RSA key pair. The App generates the key pair according to FIPS 186-4 with the PRNG, which corresponds to NIST SP 800-90A Rev. 1. After dividing the *App's share of the Private Key* to components, the Private Key of the RSA key pair is deleted.

Generation of *App's part of the Private Key*

The *App's part of the Private Key* is a 3072-bit random number. The App generates *the App's part of the Private Key* randomly with the PRNG, which corresponds to NIST SP 800-90A Rev. 1.

Generation of *Server's part of the Private Key*

The *Server's part of the Private Key* is a 3072-bit number, which is computed from the private exponent of the *App's share of the Private Key* and *App's part of the Private Key*. The App computes the *Server's part of the Private Key* and transmits the *Server's part of the Private Key* securely to the App server.

Generation of *Server's share of the Private Key* and *Server's share of the Public Key*

Server's share of the Private Key and *Server's share of the Public Key* is a 3072-bit RSA keypair. App server generates the keypair inside the App HSM module.

Generation of *Subscriber's Public Key*

Subscriber's Public Key is a 6144-bit RSA Public Key. The Public Key is computed by the App server from the *App's share of the Public Key* and *Server's share of the Public Key*. This way all the App keypair components are tied together with the *Public Key*.

6.1.1.3 Mobile

The Private Keys are generated by the QSCD compliant SIM-card. Only SIM-cards on the EU QSCD list are allowed on the QSCD verified SIM-card. The keys never leave the SIM-card. The Subscriber keys are protected by the activation PIN codes that the Subscriber selects by entering them on the device during registration process. Subscribers can change the PIN codes with the SIM Toolkit App.

6.1.1.4 eSeal and Equipment Authentication

For Qualified eSeals the keys must be generated in a FIPS 140-2 Level 3 or Common Criteria certified HSM. The Subscriber is obligated to keep the Private Key under the Subscriber's sole control.

The Subscriber is obligated to only use the Private Key for cryptographic functions within the QSCD.

For non-qualified Equipment Authentication, the Subscriber MAY generate the keys within a secure cryptographic device.

6.1.1.5 TSU

For TSU the keys must be generated in a FIPS 140-2 Level 3 or Common Criteria certified HSM. The Subscriber is obligated to keep the Private Key under the Subscriber's sole control. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

6.1.1.6 Card

The Subject's Private Keys are generated in the chip of the Card.

6.1.1.7 App on Smartphone

Subscriber's *Private key* is composed of multiple components.

6.1.1.7.1 Delivery of App's part of the private key

The *App's part of the Private Key* is generated inside the Subscriber's Mobile and is never transmitted outside of this device.

6.1.1.7.2 Delivery of Server's part of the private key

The *Server's part of the Private Key* is generated inside the Subscriber's Mobile and is securely transmitted to the App server. The transmission is handled in the following way:

1. The key-transmission-key (KTK) key pair is generated inside the App HSM module. The KTK is a 3072-bit RSA key pair.
2. The Public Key of the KTK is embedded in the binary distribution of the App.
3. During the registration procedure, the App and App server generate Diffie-Hellman key pairs and perform the Diffie-Hellman key exchange protocol to derive the transmission-encryption-key (TEK). The length of TEK key is 256 bits, it consists of 128-bit AES key and 128-bit HMAC key, concatenated.
4. The *Server's part of the Private Key* is sent to the App server with the following protection:
    a. The key is encoded and encrypted with the Public Key of the KTK (according to the RFC 7516), so that it can only be decrypted by the App server.
    b. The submission request is encrypted, and integrity protected with the shared TEK key.
    c. The communication is performed within the TLS channel, for additional confidentiality and authenticity.
5. The App server uses the established TEK key to decrypt the request and HSM to decrypt *the Server's part of the Private Key* and stores it securely in the database, wrapped with another long-term key-wrap-keypair (KWK). The KWK is generated and protected by the App HSM module.

6.1.1.7.3 Delivery of Server's share of the private key

The *Server's share of the Private Key* is generated inside the App HSM module and is always protected by the HSM module.

6.1.1.8 Mobile

Subscriber's Private Keys are generated in the chip of the SIM-card. Confidentiality and non-usage are warranted by the MO handing over non-personalized QSCD to the Subscriber.

6.1.1.9 eSeal and Equipment Authentication

The Subscriber creates his own Private Keys and only hands over the CSR.

6.1.1.10 TSU

The Subscriber creates his own Private Keys and only hands over the CSR.

6.1.2 Public Key Delivery to Certificate Issuer

6.1.2.1 Card

The RA system communicates with the Card and receives the Public Key over a secure channel. The Public Key is then sent to the CA system via a secure channel for signing.

6.1.2.2 App on Smartphone

Subscriber's *Public key* is computed inside the App server from the *App's share of the Public Key* and *Server's share of the Public Key* and then transmitted to Certificate Issuer inside the PKCS#10 Certificate Signing Request (CSR). The CSR is signed by the Subscriber for authenticity. The transmission is protected by TLS communication channel for additional confidentiality and authenticity.

Subscriber's *Public Key* is composed of multiple components. The delivery of individual components is as follows:

6.1.2.2.1 Delivery of App's share of the Public Key from App-to-App server

The *App's share of the Public Key* is generated in the App and then transmitted to the App server during the Subscriber's registration process. The Public Key is transmitted over the TLS communication channel for confidentiality and authenticity.

6.1.2.2.2 Delivery of Server's share of the Public Key from App HSM to App server

The *Server's share of the Public Key* is generated inside the App HSM module and then transmitted to App server. The Public Key is transmitted over the secured communication channel for confidentiality and authenticity.

6.1.2.3 Mobile

The RA system communicates with the SIM-card and receives the Public Key over a secure channel. The Public Key is then sent to the CA system via a secure channel for signing.

6.1.2.4 eSeal and Equipment Authentication

Qualified eSeals:

In case the Subscriber creates their own keys the Subscribers only sends the CSR to AK RA as part of the application. AK RA sends Public Key via a secure channel to the CA for signing.

In case AK creates the keys, the AK RA sends the Public Key via secure channel to the CA for signing.

Non-Qualified Equipment Authentication:

The Subscriber creates their own key pairs. AK RA sends Public Key in a secure way to CA for signing.

6.1.2.5 TSU

The Subscriber creates their own keys and only sends the CSR to AK RA as part of the application. AK RA sends Public Key via a secure channel to the CA for signing.

6.1.3 CA Public Key Delivery to Relying Parties

Refer to chapter 6.1.4 of AK TSPS [3].

6.1.4 Key Sizes

6.1.4.1 Card

Subject keys are 2048 and 4096 bits RSA keys.

6.1.4.2 App on Smartphone

1. *App's share of the Private Key* is a 3071 or 3072 bit RSA Private Key.
2. *App's part of the Private Key* is a 3071 or 3072 bit number.
3. *Server's part of the Private Key* is a 3071 or 3072 bit number.

4. *Server's share of the Private Key* is a 3071 or 3072 bit RSA Private Key.
5. *App's share of the Public Key* is a 3071 or 3072 bit RSA Public Key.
6. *Server's share of the Public Key* is a 3071 or 3072 bit RSA Public Key.
7. *Public key* is a 6142, 6143 or 6144 bit RSA Public Key.

6.1.4.3 Mobile

Subscriber keys are 2048 bits when RSA is used.

6.1.4.4 eSeal and Equipment Authentication

Subscriber keys are 2048 and 4096 bits when RSA is used.

6.1.4.5 TSU

Subscriber keys are 2048 and 4096 bits when RSA is used.

6.1.5 Public Key Parameters Generation and Quality Checking

6.1.5.1 Card

The quality of Public Keys is guaranteed by using secure random number generators built into the QSCD. User-generated keys are not accepted.

6.1.5.2 App on Smartphone

Quality of Public Keys is guaranteed by using secure random number generators by the App and App HSM module and following the specified algorithms in FIPS 186-5. Before issuing a Certificate, key is checked for duplicates and some basic analytic checks are applied (e.g., e > 1 for RSA). More thorough checks are run over the database of issued Certificates regularly.

6.1.5.3 Mobile

The quality of Public Keys is guaranteed by using secure random number generators built into the QSCD. User-generated keys are not accepted.

6.1.5.4 eSeal and Equipment Authentication

For qualified eSeal the keys must be generated by a FIPS 140-2 Level 3 or Common Criteria certified HSM either in the Subscriber equipment or on a secure Token (Crypto Stick) provided by AK. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

For non-qualified Equipment Authentication user-generated keys are accepted.

6.1.5.5 TSU

For TSU the keys must be generated by the Subscriber in a FIPS 140-2 Level 3 or Common Criteria certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

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

Refer to chapter 6.1.7 of AK TSPS [3].

Key usage purposes are described in chapter 7.1 of this CPS.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

Cryptographic devices used to generate Subject keys are securely stored and distributed.

6.2.1.1 Card

Refer to chapter 6.2.1 of AK TSPS [3].

The chips used to store Subject's Private Keys are QSCD according to eIDAS [8].

6.2.1.2 App on Smartphone

Refer to chapter 6.2.1 of AK TSPS [3].

App on Smartphone App cryptographic library standards

The App on the Android and iOS platforms correspond to FIPS 186-4.

App on Smartphone server cryptographic library standards

The App server is using App HSM module for cryptographic operations. HSM module corresponds to FIPS 140-2 Level 3. HSM is certified to be compliant with the QSCD requirements according to eIDAS [8].

6.2.1.3 Mobile

Refer to chapter 6.2.1 of AK TSPS [3].

The chips used to generate, and store Subscriber's Private Keys are QSCD according to eIDAS [8].

6.2.1.4 eSeals and Equipment Authentication

For Qualified eSeals:

The Subscriber is required to create and store keys in a FIPS-140-2 Level 3 or Common Criteria certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

For Non-Qualified Equipment Authentication:

The Subscriber is not required to create and store keys in a certified HSM.

6.2.1.5 TSU

The Subscriber is required to create and store keys in a FIPS-140-2 Level 3 or Common Criteria certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

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

6.2.2.1 Card

Refer to chapter 6.2.2 of AK TSPS [3].

No Multi-Person control is applied to Subject's Private keys.

6.2.2.2 App on Smartphone

Multi-Person Control of *App's part of the Private Key*

No Multi-Person control is applied to *App's part of the Private Key.*

Multi-Person Control of *Server's part of the Private Key*

The access means to the KWK key, which is used to protect the *Server's part of the Private Key*, is divided into two parts that are secured by different persons in Trusted Roles. For activation of the KWK key the presence of at least two authorized persons is required in accordance with chapter 5.2.2 of AK TSPS [3].

Multi-Person Control of *Server's share of the Private Key*

The access means to the *Server's share of the Private Key* is divided into two parts that are secured by different persons in Trusted Roles. For activation of such keys, after the reboot of the App System, the presence of at least two authorized persons is required in accordance with chapter 5.2.2 of AK TSPS [3].

6.2.2.3 Mobile

Refer to chapter 6.2.2 of AK TSPS [3].

No Multi-Person control is applied to the Subscriber's Private Keys.

6.2.2.4 eSeal and Equipment Authentication

Refer to chapter 6.2.2 of AK TSPS [3].

No Multi-Person control is applied to Subscriber's Private Keys.

6.2.2.5 TSU

Refer to chapter 6.2.2 of AK TSPS [3].

6.2.3 Private Key Escrow

AK does not offer Key Escrow services to Subscribers.

6.2.4 Private Key Backup

6.2.4.1 Card

Refer to chapter 6.2.4 of AK TSPS [3].

The Subject's Private Keys cannot be extracted or restored from the chip and are not backed up anywhere.

6.2.4.2 App on Smartphone

Refer to chapter 6.2.4 of AK TSPS [3].

In general, App System does not provide Private Key backup services. AK makes the following exceptions to the following components of the Subscriber's Private Key to support high availability of the App System.

6.2.4.2.1 No backup of App's part of the Private Key

The encrypted value of *the App's part of the private key* is stored inside the App private storage area. It is not backed up and not copied from the storage area.

In case Subscriber needs to recover from the malfunctioning Mobile or user error, Subscriber needs to complete the registration process again.

6.2.4.2.2 Backing up of encrypted value of Server's part of the Private Key

The encrypted value of *Server's part of the Private Key*, protected with the KWK, is stored inside the App database.

The App database is regularly synchronized to another data center and regularly copied to the backup storage.

6.2.4.2.3 Backing up of KWK of Server's part of the Private Key

The *Server's part of the Private Key* is encrypted with the KWK, which is protected by the App HSM module.

The HSM module is regularly synchronized to another data center and regularly backed up to backup storage.

6.2.4.2.4 Backing up Server's share of the Private Key

The *Server's share of the Private Key* is protected by the App HSM module.

The App HSM module is regularly synchronized to another data center and regularly backed up to backup storage.

6.2.4.3 Mobile

Refer to chapter 6.2.4 of AK TSPS [3].

Subscriber's Private Keys cannot be extracted or restored from the chip and are not backed up.

6.2.4.4 eSeal and Equipment Authentication

Refer to chapter 6.2.4 of AK TSPS [3].

Subscriber's Private Keys are under control of the Subscriber.

For Qualified eSeal, the Subscriber is required to generate and store the Certificates in a FIPS 140-2 Level 3 or Common Criteria certified HSM or a QSCD when QCP-l-QSCD or QCP-l with NCP+ policy. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

For non-Qualified Equipment Authentication, the Subscriber is NOT required to generate and store the Certificates in a FIPS 140-2 Level 3 or Common Criteria certified HSM.

6.2.4.5 TSU

Refer to chapter 6.2.4 of AK TSPS [3].

The Subscriber's Private Keys are under control of the Subscriber.

The Subscriber is required to generate and store the keys in a FIPS 140-2 Level 3 or Common Criteria certified HSM. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

6.2.5 Private Key Archival

6.2.5.1 Card

Refer to chapter 6.2.5 of AK TSPS [3].

The Subject's Private Keys cannot be extracted or restored from the chip and are not archived.

6.2.5.2 App on Smartphone

Refer to chapter 6.2.5 of AK TSPS [3].

Components of the Subscriber's *Private Key* are not archived.

6.2.5.3 Mobile

Refer to chapter 6.2.5 of AK TSPS [3].

The Subscriber's Private Keys cannot be extracted or restored from the chip and are not archived.

6.2.5.4 eSeal and Equipment Authentication

Refer to chapter 6.2.5 of AK TSPS [3].

The Subscriber's Private Keys are under control of the Subscriber.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

6.2.6.1 Card

Refer to chapter 6.2.6 of AK TSPS [3].

The Subject's Private Keys for Card are never transferred. They are generated on the QSCD at the time of registration.

6.2.6.2 App on Smartphone

Refer to chapter 6.2.6 of AK TSPS [3].

Private Key transfer into or from the cryptographic module is not done, otherwise than described in the chapter 6.1.2 of this CPS.

6.2.6.3 Mobile

Refer to chapter 6.2.6 of AK TSPS [3].

The Subscriber's Private Keys for Mobile are never transferred. They are generated on the QSCD at the time of registration.

6.2.6.4 eSeal and Equipment Authentication

Refer to chapter 6.2.6 of AK TSPS [3].

The Subscriber's Private Keys for eSeal are never transferred. In the case of Qualified eSeal, the keys are generated either by the Subscriber in their own FIPS 140-2 level 3 or Common Criteria certified HSM equipment or by AK on a Crypto Stick. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

In case of non-qualified Equipment Authentication, the keys are created by the Subscriber.

6.2.6.5 TSU

Refer to chapter 6.2.6 of AK TSPS [3].

The Subscriber's Private Keys are never transferred. The keys are generated by the Subscriber in their own FIPS 140-2 level 3 or Common Criteria certified HSM equipment. FIPS 140-2 Level 3 certified HSM shall be in FIPS mode.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 Card

Refer to chapter 6.2.7 of AK TSPS [3].

Private Keys of the Subject are stored on the chip of the Card.

6.2.7.2 App on Smartphone

Refer to chapter 6.2.7 of AK TSPS [3].

6.2.7.2.1 Storage of App's part of the Private Key

App's part of the Private Key is a random large integer number. For storage, it is encrypted with the 128-bit AES key, derived from the Subscriber's PIN. The encrypted *App's part of the Private Key* is then stored on the private area of the App on the Mobile storage.

The AES key is generated from the Subscriber's PIN with the PBKDF2 function (according to RFC 2989). The AES key and the Subscriber's PIN is never stored by the App. The AES encryption algorithm is used in the CBC mode and without any padding.

6.2.7.2.2 Storage of Server's part of the Private Key

The Server's part of the Private Key is a random large integer number. For storage in the App database, it is encrypted with the 128-bit key-wrapping-key (KWK). The KWK is a 128-bit AES key, which is protected by the App HSM module.

6.2.7.2.3 Storage of Server's share of the Private Key

Server's share of the Private Key is the Private Key of the RSA key pair. It is generated inside the App HSM module and protected by the HSM module.

6.2.7.3 Mobile

Refer to chapter 6.2.7 of AK TSPS [3].

Private Keys of the Subscriber are stored on the chip of the Mobile.

6.2.7.4 eSeal and Equipment Authentication

Refer to chapter 6.2.7 of AK TSPS [3].

Private Keys under control of the Subscriber.

6.2.8 Method of Activating Private Key

6.2.8.1 Card

Refer to chapter 6.2.8 of AK TSPS [3].

The Subject's Private Keys are protected by PIN codes. The following rules apply:

- There is a separate PIN for each Private Key.
- The Subject must enter the activation code of the Authentication Certificate (PIN1) at least once after the Card has been inserted into the card reader device.
- The Subject must enter the activation code of the Qualified Electronic Signature Certificate (PIN2) before every single operation done with the corresponding Private Key.
- The usage of all Private Keys protected by a single PIN will be blocked after five (5) consecutive incorrect tries for authentication and after three (3) consecutive incorrect tries for signature.
- PIN CANNOT be unblocked.
- User can change the PIN.

The length of the activation codes cannot be shorter than:

- 4 digits for the Authentication Key (PIN1).
- 6 digits for the Signature Key (PIN2).

6.2.8.2 App on Smartphone

Refer to chapter 6.2.8 of AK TSPS [3].

In order to give signatures with Subscriber's *Private Key*, all components of the Private Key must be activated.

6.2.8.2.1 Activating App's part of the Private Key

The App's part of the Private Key is protected by Subscriber's PIN and Subscriber needs to enter the PIN to the App for each transaction. The value of PIN is never stored by the App.

Subscriber's PIN is chosen by the Subscriber during the registration process of the App.

The following rules apply:

1. PIN1 to protect the authentication key pair must be 4 to 12 digit long.
2. PIN2 to protect the signature key pair must be 5 to 12 digit long.
3. In case the Subscriber enters the wrong PIN 3 times in a row, the keypair is locked from usage for next three hours.
4. In case the Subscriber enters the wrong PIN 6 times in a row, the keypair is locked from usage for next 24 hours.
5. In case the Subscriber enters the wrong PIN 9 times in a row, the keypair is blocked and the Certificate is revoked.

6.2.8.2.2 Activating Server's part of the Private Key

Server's part of the Private Key is protected by KWK, which in turn, is protected by the App HSM module. To activate the KWK, the operator needs to enter the operator keycard into the HSM and enter the operator password to the HSM. Once activated by the operator, the KWK is activated until the App System is stopped.

Further, the activation of the *Server's part of the Private Key* for completing the signature with the Subscriber's *Private Key* is the subject of authentication and access control procedure performed on the App server. The access is granted only after successful validation of the possession-based authentication factor (one-time password, presented by the App over the secure channel) and successful validation of the knowledge-based authentication factor (signature share computed from the data to be signed, Subscriber's PIN and the *App's part of the Private Key*, presented by the Subscriber and the App over the secure channel. So, this means that activation of *Server's part of the Private Key* requires that Subscriber has activated the *App's part of the Private Key* by entering correct PIN code according to chapter 6.2.8.2.1 of this CPS.

The authentication factors are only usable for specific data to be signed, and they would need to be re-submitted for the next operation with Subscriber's *Private Key*.

6.2.8.2.3 Activating Server's share of the Private Key

Server's share of the Private Key is an RSA private key, which is generated and protected by the App HSM module. To allow App system to access the HSM, the operator needs to enter the operator keycard into the HSM and enter the operator password to the HSM. HSM connection is active until the App System is stopped.

The activation of the *Server's share of the Private Key* for completing the signature with the Subscriber's *Private Key* is the subject of authentication and access control procedure performed on the App server. The access is granted only after successful validation of the possession-based authentication factor (one-time password, presented by the App over the secure channel) and successful validation of the knowledge-based authentication factor (App's signature computed from the data to be signed, Subscriber's PIN (presented by the Subscriber), the *App's part of the Private Key* and *Server's part of the Private Key*. So, this means that activation of *Server's share of the Private Key* requires that Subscriber has activated the *App's part of the Private Key* by entering correct PIN code according to chapter 6.2.8.2.1 of this CPS.

The authentication factors are only usable for specific data to be signed, and they would need to be re-submitted for the next operation with Subscriber's *Private Key*.

6.2.8.3 Mobile

Refer to chapter 6.2.8 of AK TSPS [3].

The Subscriber's Private Keys are protected by PIN codes. The following rules apply:

- There is one PIN for both Private Keys corresponding to a Certificate with a unique Distinguished Name.
- The Subscriber must enter the activation code of the Authentication Certificate (PIN) before every single operation with the corresponding Private Key.
- The Subscriber must enter the activation code of the Qualified Electronic Signature Certificate (PIN) before every single operation done with the corresponding Private Key.
- The usage of all Private Keys protected by a single PIN will be blocked after 5 consecutive incorrect tries.
- Locked PIN cannot be unlocked.

The length of the activation codes is limited to:

- 4 – 8 digits for the Authentication Key and Signature Key (PIN); Same PIN for both.

6.2.8.4 eSeal and Equipment Authentication

Refer to chapter 6.2.8 of AK TSPS [3].

The Subscriber's Private Keys are under control of the Subscriber. If Private Keys are stored on an AK provided Crypto Stick the keys are protected by a PIN code selected by the Subscriber at time of registration.

6.2.8.5 TSU

Refer to chapter 6.2.8 of AK TSPS [3].

The Subscriber's Private Keys are under control of the Subscriber.

6.2.9 Method of Deactivating Private Key

6.2.9.1 Card

Refer to chapter 6.2.9 of AK TSPS [3].

The Private Key is deactivated by disconnecting power or resetting the Card.

The Subject can deactivate a Private Key by entering the PIN codes incorrectly 5 consecutive times.

6.2.9.2 App on Smartphone

Refer to chapter 6.2.9 of AK TSPS [3].

Deactivation of any component of the Subscriber's *Private Key* also means that the Subscriber cannot give signatures anymore and needs to activate that component again.

6.2.9.2.1 Deactivating App's part of the Private Key

The user entered PIN-code is only used for a single key pair operation. The PIN and derived AES key is deleted from the App memory after the operation is completed or when the App server responds with 'Wrong PIN' error message.

6.2.9.2.2 Deactivating Server's part of the Private Key

The *Server's part of the Private Key* is only decrypted for a single key pair operation by the server, and the clear-text value is immediately deleted from the App server memory after the operation is completed or when the App server responds with 'Wrong PIN' error message.

6.2.9.2.3 Deactivating Server's share of the Private Key

Server's share of the Private Key is protected by the App HSM module. Access to the keys is lost after the App HSM or App server is stopped.

6.2.9.3 Mobile

Refer to chapter 6.2.9 of AK TSPS [3].

The Private Key is deactivated by disconnecting power or resetting the Card.

The Subscriber can deactivate a Private Key by entering all the PIN incorrectly 5 consecutive times.

6.2.9.4 eSeal and Equipment Authentication

Refer to chapter 6.2.8 of AK TSPS [3].

The Private Key is under the control of the Subscriber. In the case of Crypto Stick provided by AK the Private Key can be deactivated by resetting the Crypto Stick or by entering the wrong PIN more than five times.

For non-qualified Equipment Authentication, the Subscriber can delete the keystore.

6.2.9.5 TSU

Refer to chapter 6.2.8 of AK TSPS [3].

The Private Key is under the control of the Subscriber.

6.2.10 Method of Destroying Private Key

6.2.10.1 Card

Refer to chapter 6.2.9 of AK TSPS [3].

The Subject's Private Keys can be destroyed by physically destroying the chip.

6.2.10.2 App on Smartphone

Refer to chapter 6.2.10 of AK TSPS [3].

Destroying any component of the Subscriber's *Private key* also means that the Subscriber cannot give signatures anymore and needs to complete the registration process again.

6.2.10.2.1 Destroying App's part of the Private Key

The Subscriber can destroy the *App's part of the Private Key* from the App during the App account closing (for example, by closing the App account and the App or in the App portal, by uninstalling the App, by destroying the Mobile, etc.).

6.2.10.2.2 Destroying Server's part of the Private Key

Server's part of the Private Key is deleted in the App server during the App account closing (for example, by closing the App account in the App or in the App portal, after multiple wrong PIN codes entered, detection of cloned device, etc.).

6.2.10.2.3 Destroying Server's share of the Private Key

Server's share of the Private Key is deleted in the App HSM module during the account closing (for example, by closing the App account in the App or in the App portal, after multiple wrong PIN codes entered, detection of cloned device, etc.).

6.2.10.3 Mobile

Refer to chapter 6.2.9 of AK TSPS [3].

The Subscriber's Private Keys can be destroyed by physically destroying or damaging the chip of the Card.

6.2.10.4 eSeal and Equipment Authentication

Refer to chapter 6.2.8 of AK TSPS [3].

The Subscriber's Private Keys are under control of the Subscriber. In the case of a Crypto Stick provided by AK the Subscriber's Private Keys can be destroyed by physically destroying or damaging the chip.

For non-qualified Equipment Authentication, the Subscriber can delete the keystore.

6.2.10.5 TSU

Refer to chapter 6.2.8 of AK TSPS [3].

The Subscriber's Private Keys are under control of the Subscriber.

6.2.11 Cryptographic Module Rating

Refer to chapter 6.2.1 of this CPS.

Card, App, Mobile SIM-cards, and Crypto Stick are defined as QSCD by eIDAS.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

Refer to chapter 6.3.1 of AK TSPS [3].

All the Subscriber's Public Keys are kept in database of AK and may be archived after expiration of the CA that has issued the Certificates.

6.3.2 6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Refer to chapter 6.3.2 of AK TSPS [3].

For Subscriber Certificates, the validity period is defined in chapter 7.1 of this CPS.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

6.4.1.1 Card

Refer to chapter 6.4.1 of AK TSPS [3].

The Subscriber picks the PIN codes at the time of enrollment. PIN codes are never printed or recorded anywhere by AK.

In case the Subscriber is a legal entity the Subject picks the PIN code.

6.4.1.2 App on Smartphone

Refer to chapter 6.4.1 of AK TSPS [3].

The App generates random activation codes and provides the Subscriber option to choose his own activation codes as well.

Activation data is used as the input seed to the encryption key derivation function (PBKDF2) and the resulting key is used to encrypt the locally stored *App's part of the private key*. The activation codes themselves are never stored in the App nor in the App service provider.

6.4.1.3 Mobile

Refer to chapter 6.4.1 of AK TSPS [3].

The Subscriber picks the PIN code at the time of enrollment. PIN codes are never printed or recorded anywhere.

6.4.1.4 eSeal and Equipment Authentication

Refer to chapter 6.4.1 of AK TSPS [3].

The Subscriber decides on his/her own activation code and is responsible for keeping it secure. In the case of Crypto Stick provided by AK the Subscriber picks the PIN code at the time of enrollment.

6.4.1.5 TSU

Refer to chapter 6.4.1 of AK TSPS [3].

The Subscriber decides on his/her own activation code and is responsible for keeping it secure.

6.4.2 Activation Data Protection

6.4.2.1 Card

Refer to chapter 6.4.2 of AK TSPS [3] and 6.4.1.1 of this CPS.

6.4.2.2 App on Smartphone

Refer to chapter 6.4.2 of AK TSPS [3].

The initial activation data is generated by the App or chosen by the Subscriber.

After that, activation codes themselves are never stored in the App nor with the App's service provider.

The Subscriber must memorize the activation codes and never share them with anyone.

6.4.2.3 Mobile

Refer to chapter 6.4.2 of AK TSPS [3] and 6.4.1.3 of this CPS.

6.4.2.4 eSeal and Equipment Authentication

Refer to chapter 6.4.1 of AK TSPS [3].

The Subscriber is responsible for keeping the activation code secure.

6.4.2.5 TSU

Refer to chapter 6.4.1 of AK TSPS [3].

The Subscriber is responsible for keeping the activation code secure.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

Refer to chapter 6.5.1 of AK TSPS [3].

The Subscriber is responsible for applying reasonable protections on its device.

6.5.2 Computer Security Rating

Refer to chapter 6.5.2 of AK TSPS [3].

The Subscriber is responsible for applying reasonable protections on its device.

6.6 LIFE CYCLE TECHNICAL CONTROLS

Refer to chapter 6.6 of AK TSPS [3].

The Subscriber is responsible for applying reasonable protections on its device.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Card

Refer to chapter 6.7 of AK TSPS [3].

Subject is responsible for applying reasonable protections for its Card.

6.7.2 App on Smartphone

Refer to chapter 6.7 of AK TSPS [3].

The App and App server communicates with each other over the TLS channel. Server enforces known good encryption cipher-suites on the TLS channel. The App implements the certificate pinning to verify the authenticity of channel endpoint. Server implements the App authentication to verify the authenticity of channel endpoint.

The App and App server further use the established transmission-encryption-key (TEK) to secure the network requests and responses. The App and server generate Diffie-Hellman key pairs and perform the Diffie-Hellman key exchange protocol, to derive the TEK. The length of TEK key is 256 bits, it consists of 128-bit AES key and 128-bit HMAC key, concatenated.

The Subscriber is responsible for applying reasonable protections on its device.

6.7.3 Mobile

Refer to chapter 6.7 of AK TSPS [3].

The Subscriber is responsible for applying reasonable protections on its device.

6.7.4 eSeal and Equipment Authentication

Refer to chapter 6.7 of AK TSPS [3].

The Subscriber is responsible for applying reasonable protections on its device.

6.8 TIME-STAMPING

Refer to chapter 6.8 of AK TSPS [3].

Not applicable to Subscribers.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificate profile is described in the different Certificate Profiles [4] published in AK's public information repository repo.audkenni.is.

7.2 CRL PROFILE

The CRL profile is described in the Certificate Profile for CRL [4], published in AK's public information repository repo.audkenni.is.

7.3 OCSP PROFILE

The OCSP profile is described in the Certificate Profile for OCSP [4], published in AK's public information repository repo.audkenni.is.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Refer to chapter 8 of AK TSPS [3].

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

The fee for the Certificate issuance is according to the published price list.

9.1.2 Certificate Access Fees

The fee for the Certificate access is according to the published price list.

9.1.3 Revocation or Status Information Access Fees

The fee for the Certificate revocation and status information access is according to the published price list. CRL and OCSP information are publicly available 24/7 pursuant to chapter 4.9.9. Revocation status information for qualified signatures is free of charge for individual use.

9.1.4 Fees for Other Services

The fee for other services is according to the published price list.

9.1.5 Refund Policy

Refer to chapter 9.1.5 of AK TSPS [3].

Financial settlements are according to the agreement between parties.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Refer to chapter 9.2.1 of AK TSPS [3].

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to chapter 9.2.1 of AK TSPS [3].

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Refer to chapter 9.3 of AK TSPS [3].

9.4 PRIVACY OF PERSONAL INFORMATION

Refer to chapter 9.4 of AK TSPS [3].

9.5 INTELLECTUAL PROPERTY RIGHTS

AK obtains intellectual property rights to this CPS.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

Refer to chapter 9.6.1 of AK TSPS [3].

AK runs a CA system and is a Trust Service Provider. AK is responsible for:

- the proper identification and data verification of a natural person and/or business entity for the purpose of Certificate issuance,
- issuance of Certificates in a secure manner to preserve their authenticity and accuracy, and
- compliance with its obligations.

AK ensures that:

- the supply of the certification service is in accordance with the relevant legislation;
- ensures, when applicable, verification that the Subscriber of a Seal is in possession of a Private Key whose pertaining Public Key is delivered for certification;
- the supply of the certification service is in accordance with this CPS and the CP;
- it keeps account of the Certificates issued by it and of their validity;
- it provides the possibility to check the validity of Certificates 24 hours a day;
- the CA certification keys are protected by hardware security modules (i.e., HSM) and are under sole control of AK;
- the CA certification keys used in the supply of the certification service are activated based on shared control;
- it provides security with its internal security procedures;
- it accepts and registers batches of QSCDs presented by MO; and
- it accepts, registers, and processes the applications for revocation of Certificates presented by the Subscriber, MO or competent authority.

9.6.2 RA Representations and Warranties

Refer to chapter 9.6.2 of AK TSPS [3].

AK runs an RA registration system and uses subcontractors to perform RA duties. All applications for certificates go through the RA system. The RA system accepts Subscriber applications and revocations.

AK also runs an RA portal for customers. The portal accepts applications for new Certificates and revocation requests. All transactions in the RA portal require a valid Certificate with Qualified Electronic Signature.

9.6.3 Subscriber Representations and Warranties

Refer to chapter 9.6.3 of AK TSPS [3].

The Subscriber:

- in the registration process, presents itself in the manner stipulated in chapter 3. and in chapter 4.1.2.2 hereof,
- carefully uses and stores electronic signature or seal creation device, Private Keys, and activation data, in accordance with this CPS;
- takes adequate protection measures against any unauthorized access and use of electronic signature or seal creation device, Private Key, and activation data, in accordance with chapter 6. hereof;
- requires, as soon as possible, the revocation of the Certificate in case of Private Key compromise, the loss or damage of electronic signature or seal creation device, Private Key, and activation data, in accordance with chapter 4.9. hereof;
- uses the Certificate and the accompanying Private Key in accordance with the laws and other regulations of the Republic of Iceland and in accordance with chapters 1.4.1 and 1.4.2 hereof;
- uses the Certificate and the accompanying Private Key in cases when the Subscriber possesses the key pair and manages it, in accordance with chapter 4.5.1 hereof;
- acts in accordance with all other provisions of this CPS that refer to Subscriber obligations; and
- is bound by the Terms and Conditions [9] after signing the application for a Certificate.

9.6.4 Relying Party Representations and Warranties

Refer to chapter 9.6.4 of AK TSPS [3].

9.6.5 Representations and Warranties of Other Participants

App provider ensures that:

- it adheres to the key generation and storage procedures under its control and described in this CPS;
- it adheres to provisions of fees described in this CPS; and
- it transfers the correct Certificate and correct Certificate status information.

MO is responsible for providing SIM-cards that have QSCD status and AK application.

Hosting provider providing Automated Biometric Identity Verification SHALL follow the requirements stipulated in the agreement concluded with AK for the issuance of eIDAS EU Qualified certificate.

9.7 DISLAIMERS OF WARRANTIES

Refer to chapter 9.7 of AK TSPS [3].

9.8 LIMITATIONS OF LIABILITY

Refer to chapter 9.8 of AK TSPS [3].

9.9 INDEMNITIES

Indemnities between the Subscriber and AK are regulated in the Terms and Conditions.

9.10 TERM AND TERMINATION

9.10.1 Term

Refer to chapter 2.2.1 of this CPS.

9.10.2 Termination

Refer to chapter 9.10.2 of AK TSPS [3].

9.10.3 Effect of Termination and Survival

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

At a minimum, all responsibilities related to protecting personal and confidential information, also maintenance of AK archives for determined period, and logs, survive termination. All Subscriber agreements remain effective until the Certificate is revoked or expired, even if this CPS is terminated.

Termination of this CPS cannot be done before termination actions described in chapter 5.8 of this CPS.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The Subscriber is obliged to become familiarized with the Terms and Conditions before agreeing to and signing it.

The Subscriber's individual notices are communicated via the Subscriber's personal contact information, to the extent provided. The contact may be via email address, regular mail, or phone number.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Refer to chapter 1.5.4 of this CPS.

9.12.2 Notification Mechanism and Period

Refer to chapter 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 chapter 9.13 of AK TSPS [3].

The Subscriber or other party can submit their claim or complaint at the email address fyrirspurnir@audkenni.is.

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

Refer to chapter 9.15 of AK TSPS [3].

Additionally, AK ensures compliance with the Data Protection and processing of personal data Act no. 90/2018. [10]

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

AK contractually obligates each RA to comply with the CP and applicable industry guidelines. AK also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from the CP, then the agreement with that party prevails, but solely with respect to that party. Third parties may not rely on or bring action to enforce such an agreement.

9.16.2 Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of AK. Unless specified otherwise in a contract with a party, AK 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 (Attorney's Fees and Waiver of Rights)

AK may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. AK's failure to enforce a provision of this CPS does not waive AK'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 AK.

9.16.5 Force Majeure

Refer to chapter 9.16.5 of AK TSPS [3].

9.17 OTHER PROVISIONS

Not applicable.

10 REFERENCES

1. AK CP – AK Certificate Policy for Fullgilt auðkenni 2021; repo.audkenni.is.
2. RFC 3647 – Request for Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
3. AK TSPS - AK Trust Service Practice Statement; repo.audkenni.is.
4. AK CPR - Certificate, CRL and OCSP Profiles: repo.audkenni.is.
5. Key Words for Use in RFCs to Indicate Requirement Levels, S.Bradner, RFC2119, March 1997.
6. ETSI EN 319 411-2 V2.6.1 (2025-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service.

7. ETSI EN 319 411-1 V1.5.1 (2025-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements.
8. Electronic Identification and Trust Services for Electronic Transactions Act no. 55/2019.
9. Terms and Conditions for electronic certificates issued by Audkenni's intermediary certificates, published: repo.audkenni.is.
10. Act no. 90/2018 on Data Protection and processing of personal data.
11. ETSI EN 319 401 V3.1.1 (2024-06) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
12. Revocation Procedures. Part of AK security handbook.
13. Common Criteria – ISO/IEC Standard 15408-1/2/3:2005 – Information technology – Security techniques – Evaluation criteria for IT security