AK

Trusted Service Practice Statement

Version 1.0 – Effective date 05.05.21

AUÐKENNI EHF -Trust Services Practice Statement

Change control			
Published	**Version**	**Changes**	**Approval**
01.11.2019	0.9	First draft version.	
16.03.2021	1.0	Publication	Security Committee

TABLE OF CONTENTS

1. INTRODUCTION

This document describes the general practices and procedures common to all trust services offered by Auðkenni ehf (AK).

This document is created according to the ETSI EN 319 400 series and describes general practices common to all trust services offered by AK. This document is unclassified and can be freely distributed. The descriptions of security and technical solutions are therefore at a relatively general level.

The Certification Policy and related Certification Practice Statement describe parts specific to each trust service.

Pursuant to the IETF RFC 3647 [4] this document is divided into nine parts. To preserve the outline specified by RFC 3647 [4], section headings that do not apply have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them.

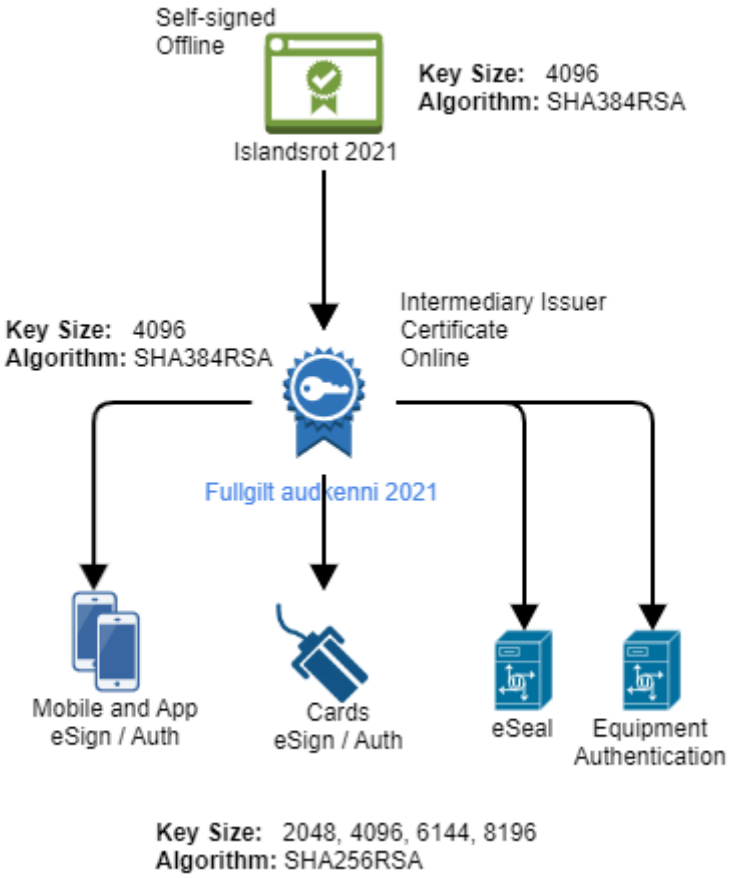
This document applies to all types of certificate issuance at Auðkenni, including certificates on SIM cards, certificates on other smart cards, certificates on remote systems and certificates for computer equipment (eSeal).

Certificates on SIM cards, remote systems and cards have two key pairs, one for authentication and one for signing.

1.1 Overview

AK operates a Public Key infrastructure to provide reliable Trust Services. AK uses intermediate certificates issued by the root Certificate Authority ISLANDSROT.

Following figure shows the Islandsrot 2021 (Iceland root) chain:



Auðkenni Trust Services Practices Statement (TSPS) presents the criteria established by Auðkenni to provide electronic Trust Services, which enhance trust and confidence in electronic transactions. TSPS describes Auðkenni practices of providing non-qualified Trust Services and Qualified Trust Services in conformity with the eIDAS regulation and legal acts of Iceland nr. 55/2019 [1], ETSI EN 319 401 General Policy Requirements for Trust Service Providers [2], and other related service-based standard requirements.

This TSPS describes practices necessary for the achievement of the security level approved by AK management. AK has achieved and maintains ISO/IEC 27001:2013 certification from BSI. The statement of applicability includes more detailed description of security measures.

In the event of conflict between TSPS and the practice statements of specific services, the provisions of the practice statements of specific services shall prevail.

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 [10]. The exact meaning of these words is modified in accordance with the requirements in 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 „Auðkenni Trust Services Practice Statement". The document goes into effect when it is published and out of force when superseded by a new version.

1.3 PKI Participants

1.3.1 Trust Service Provider

AK is a Trust Service Provider (TSP). The roles of AK as TSP are defined in relevant service-based Policy and/or Practice Statement.

Obligations and warranties of AK are described in clause 9.6.1 of this TSPS.

1.3.2 Registration Authorities

Registration Authority (RA) and its roles are defined in relevant service-based Policy and/or Practice Statement. The Registration Authority (RA) operates in accordance with the terms in this document.

Obligations and warranties of RA are described in clause 9.6.2 of this TSPS.

1.3.3 Subscribers

In this document subscriber can be either a natural person or a legal person.

Obligations and warranties of Subscriber are described in the clause 9.6.3 of this TSPS.

1.3.4 Relying Parties

Relying party is for example a bank, merchant, or the recipient of a message signed with a certificate.

Obligations and warranties of Relying Party are described in the clause 9.6.4 of this TSPS.

1.3.5 Other Participants

The mobile operators are responsible to provide SIM cards for key storage and the secure infrastructure for safe and secure communication with SIM cards used for certificates.

The provider for remote certificates is responsible for the secure key storage on remote servers and the secure infrastructure for safe and secure use of remote certificates.

1.4 Certificate Usage

1.4.1. Appropriate Certificate Uses

Certificates issued in accordance with this TSPS are used for authentication or digital signing. Appropriate Certificate Uses are also specified in the CP and CPS.

1.4.2 Prohibited Certificate Uses

Everything that is not explicitly allowed is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This TSPS is administered by Auðkenni ehf.

1.5.2 Contact Person

Chief Executive Officer
Auðkenni ehf
ID: 521000-2790
Borgartún 31, 105 Reykjavík
Tel +354 530 0000
Email: audkenni@audkenni.is http://www.audkenni.is

1.5.3 Person Determining TSPS Suitability for the Policy

Auðkenni Chief Security Officer determines the suitability of this TSPS with the Policy.

1.5.4 TSPS Approval Procedures

Amendments which do not change the meaning of this TSPS, 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 of substantial changes, the new TSPS version is clearly distinguishable from the previous ones and the version number is enlarged by one. The amended TSPS along with the enforcement date, which cannot be earlier than 10 days after publication, is published on AK website.

This TSPS shall be reviewed annually.

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

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
App	Mobile application that works as a QSCD. Used on smart devices only.
Authentication	Unique identification of a person (natural or legal) by checking the alleged identity.
Authentication Certificate	Certificate is intended for Authentication.
Certificate	Public key, together with some other information, laid down in the Certificate Profile [**Error! Reference source not found.**], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of Auðkenni's structure responsible for issuing and verifying electronic Certificates with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a community and/or PKI implementation with common security requirements.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certification Service	In the context of this document, service related to issuing Certificates, managing revocation, modification and re-key of the Certificates.
Distinguished name	Unique Subject name in the infrastructure of Certificates.
Fullgilt auðkenni	An intermediary certificate, the Certificates of which enabling electronic identification and electronic signature are connected to the SIM-card of Mobile phone or plastic cards or app.
Integrity	A characteristic of an array: information has not been changed after the array was created.
Object Identifier	An identifier used to uniquely name an object (OID).
PIN code	Activation code for a Private Key.
Practice Statement	a statement of the practices that a TSP employs in providing a Trust Service.
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.
PUK code	The unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation [**Error! Reference source not found.**].
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 Regulation [**Error! Reference source not found.**].
Qualified Certificate for Electronic Signatures	Qualified Certificate for Electronic Signatures according to eIDAS Regulation [**Error! Reference source not found.**].
Qualified Electronic Signature Creation Device (QSCD)	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation [**Error! Reference source not found.**].
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Relying Party	Entity that relies upon the information contained within a Certificate or Certificate status information provided by Auðkenni.
Secure Cryptographic Device	Device which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Subject	Natural or legal person, or an organization or a device which the certificates are issued to.
Subscriber	Subscriber is a natural or legal person that is a subscriber at the CA for one or more subjects. Subscriber can also be a subject.

Terms and Conditions	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 [**Error! Reference source not found.**] upon receipt the Certificates.

1.6.2 Acronyms

Acronym	Definition
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
CSR	Certificate Signing Request
DMZ	Demilitarized Zone
eIDAS	Regulation (EU) No 910/2014 [**Error! Reference source not found.**] 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.
ETSI	European Telecommunications Standards Institute
FA	Fullgilt auðkenni. Certificate used to issue certificates to subscribers. This is an intermediary root under Íslandsrót.
HSM	Hardware Security Module
MO	Mobile Operator
NCP+	Normalized Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [**Error! Reference source not found.**]
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
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 phones
TSPS	Trust Service Provider Statement

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

AK makes the repository of documents on its website repo.audkenni.is available 24/7.

2.2 Publication of Certification Information

AK publishes all relevant information in its public repository repo.audkenni.is

2.2.1 Publication and Notification Policies

This TSPS is published in AK's public information repository.

TSPS along with the enforcement dates is published at least ten days prior taking effect.

2.2.2 Items not Published in the Practice Statement

Refer to clause 9.3.1 of this TSPS.

2.3 Time or Frequency of Publication

This TSPS and any subsequent amendments are made publicly available after approval.

AK will make all efforts to have the repository available 24/7. Upon system failure or other kinds of outages AK will restore proper functionality without delay.

2.3.1 Directory Service

AK publishes information on certificates via webservices available on demand.

The purpose of the webservice is to provide the Subscribers, Relying Parties and other persons access to the certificates registry to make inquiries about certificates.

These services are OCSP, CRL and LDAP.

2.4 Access Controls on Repositories

Information published in AK's repository is public and not considered confidential information.

AK has implemented security measures and enforced access control to prevent unauthorized access to add, delete, or modify entries into its repository. Publishing into AK's repository is restricted to authorized employees of AK.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Specified in relevant service-based Policy and/or Practice Statement.

3.2 Initial Identity Validation

Specified in relevant service-based Policy and/or Practice Statement.

3.3 Identification and Authentication for Re-Key Requests

Specified in relevant service-based Policy and/or Practice Statement.

3.4 Identification and Authentication for Revocation Request

Specified in relevant service-based Policy and/or Practice Statement.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

Specified in relevant service-based Policy and/or Practice Statement.

4.1.2 Enrolment Process and Responsibilities

Specified in relevant service-based Policy and/or Practice Statement.

4.1.3 Annual Control of QSCD

AK monitors certification status of QSCDs in use and annually checks that QSCD is recognized by verifying validity of Common Criteria Certificate issued for the QSCD or that it is continuously valid in the European Commission's list of Secure Signature Creation Devices, Qualified Signature and Seal Creation Devices notified by the member states.

If the validity in the European Commission's list of Secure Signature Creation Devices, Qualified Signature and Seal Creation Devices notified by the member states is expired due to the modification, then AK will

investigate the cause of the modification from the responsible member state or/and designated certification body. If the QSCD certification is expired or invalidated, then AK will take following actions:

- notify immediately its supervisory body and conformity assessment body;
- revoke of any affected Trust Service Token;
- Inform all affected subscribers and relying parties;
- All certificates linked to the QSCD will be revoked if the certification is invalidated.

The CA key pair generation is performed in a physically secure environment by personnel in trusted roles. All CA key management is performed according the formal Key Ceremony.

4.2 Certificate Application Processing

Specified in relevant service-based Policy and/or Practice Statement.

4.3 Certificate Issuance

Specified in relevant service-based Policy and/or Practice Statement.

4.4 Certificate Acceptance

Specified in relevant service-based Policy and/or Practice Statement.

4.5 Key Pair and Certificate Usage

Specified in relevant service-based Policy and/or Practice Statement.

4.6 Certificate Renewal

Specified in relevant service-based Policy and/or Practice Statement.

4.7. Certificate Re-Key

Specified in relevant service-based Policy and/or Practice Statement.

4.8 Certificate Modification

Specified in relevant service-based Policy and/or Practice Statement.

4.9 Certificate Revocation and Suspension

Specified in relevant service-based Policy and/or Practice Statement.

4.10 Certificate Status Services

Specified in relevant service-based Policy and/or Practice Statement.

4.11 End of Subscription

Specified in relevant service-based Policy and/or Practice Statement.

4.12 Key Escrow and Recovery

Specified in relevant service-based Policy and/or Practice Statement.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

In the field of security management, AK guides itself by the generally recognized standards, e.g. ISO/IEC 27001 [5], and other standards if required by regulations and law.

AK's security management policy documents include the security controls and operating procedures for AK facilities, systems and information assets providing the services. AK carries out and revises risk assessment

regularly in order to evaluate business risks and determine the necessary security requirements and operational procedures. AK management approves risk assessment and accepts the residual risks identified.

AK management establishes the information security policy, which forms a basis for consistency and completeness of information security and management support.

AK Security Committee approves policies and practices related to information security for the overall AK services. AK management communicates information security policies and procedures to employees and relevant external parties who are impacted by it. In addition, AK management sets out AK approach to manage information security objectives for Trust Services, including auditable procedures for internal control.

AK has achieved and maintains ISO/IEC 27001:2013 certification.

5.1 Physical Controls

AK is using physically separated space in rented server rooms specifically designed for data center operations. It is the responsibility of the owner of the premises to provide necessary environment for the equipment. A Service Level Agreement is arranged between AK and the owner of the premises to guarantee uninterrupted and secure operation. All core hardware, including central servers and HSMs are stored in the server rooms.

AK stores paper documents with a specialized document storage provider with sufficient security protocols.

All important assets used for the provision of Trusted Services are stored either in specialized server rooms or secure vaults.

5.1.1 Site Location and Construction

AK services are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of Sensitive Information and systems whether covert or overt.

The protection provided is commensurate with the identified risks. AK ensures that physical access to critical services is controlled and that physical risks to its assets are minimized.

5.1.2 Physical Access

AK data centers are protected by a minimum of three tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Access to the highest tier requires the participation of two persons in Trusted Roles.

The employees of AK may gain access to the facilities concerned with Trust Services of AK only based on an approved list. A log is kept for all entries to the data processing center of AK.

The owner of the premises has no independent access to AK servers.

Any persons entering this physically secure area will not remain there without oversight by an authorized person.

Physical access to AK office facilities is with access card. Intrusion alarm is active outside office hours.

5.1.3 Power and Air Conditioning

AK's secure facilities are equipped with:

- power systems to ensure continuous, uninterrupted access to electric power; and
- heating, ventilation, air conditioning systems to control the temperature and relative humidity.

5.1.4 Water Exposures

AK has taken reasonable precautions to minimize the impact of water exposure to the information systems.

5.1.5 Fire Prevention and Protection

AK has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. The fire prevention and protection measures of AK have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

Portable media, appliances and software may be removed from the premises of AK pursuant to the established procedure. Data media containing sensitive information may be stored only in a special fireproof safe designed for storing data media.

5.1.7 Waste Disposal

Media containing Sensitive Information are securely disposed of when no longer required. Paper documents and materials with Sensitive Information are shredded before disposal. Any media with Sensitive Information removed from use (removable media, hard disks etc.) are sanitized when decommissioned or recycled for other use, to prevent data leaks.

5.1.8 Off-Site Backup

AK performs routine backups of critical system data, audit log data, and other Sensitive Information. AK has dual data centers to ensure availability requirements. Databases in dual data centers are synchronized in real time. In addition, routine backups are performed. Backups of the most critical information (e.g. keys and configurations) are kept off-site in secure storage.

5.2 Procedural Controls

5.2.1 Trusted Roles

The following Trusted Roles critical for security have been defined:

- Security Officer: is responsible for the administration of and the implementation of the security practices;
- System Administrators: are responsible for the installation, configuration and maintenance of the information system of AK, including performing the system backup and recovery.
- System Auditor or Evaluator is responsible for periodically reviewing procedures; for that he/she has access to monitor the document archives and information system audit logs;
- RA Officer: is responsible for identification and authentication of subjects of certificates and may be responsible for registration, certificate suspension, termination of suspension and revocation procedures.

Employees in Trusted Role have job descriptions that define the functions and responsibility related to the Trusted Role.

AK ensures that personnel have achieved trusted status, and approval is given before such personnel are:

- Issued access devices and granted access to the required facilities; or
- Issued electronic credentials to access and perform specific functions on AK or other IT systems.

Security operations are managed by AK personnel in Trusted Roles but may be performed by a non-specialist, operational personnel (under supervision), as defined within the roles and responsibility documents. All requirements and rules for or concerning personnel in Trusted Roles apply equally to personnel with the temporary or permanent employment contract.

5.2.2 Number of Persons Required per Task

AK has established, maintains and enforces control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The following activities require a minimum of two employees in Trusted Roles:

- generation of certification keys;
- backup of the certification keys;
- restoration of the certification keys;
- management of HSMs and CA core systems;
- physical visit to data centers.

Backup and restore functions are performed by employees in Trusted Roles.

5.2.3 Identification and Authentication for Each Role

All Trusted Roles are performed by persons assigned into this role by the management and accepted by this person to fulfil this role.

AK has implemented an access control system, which identifies authorizations and registers all AK information system users in a trustworthy manner.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with their personal account, and administrative commands are only available with explicit permission. File system permissions and other features available in the operating system security model are used to prevent any other use.

User accounts are locked as soon as possible when the role change dictates. Access rights are audited annually by system owners.

AK personnel are accountable for their activities and logs are kept for events.

5.2.4 Roles Requiring Separation of Duties

The Trusted Roles of the Security Officer, System Auditor, Software developers and System Administrators are separate functions but, in some cases, staffed by the same persons.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The employees of AK have received adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

The employment contracts signed by the employees of AK provide for the following obligations:

- to maintain the secrecy of confidential information that has come to their knowledge in the course of their performance,
- to prevent them from holding business interests in a company, which may affect their judgment in the supply of the service and
- to ensure that they have not been punished for a willful crime.

All personnel in Trusted Roles are free from any interests that may affect their impartiality regarding Trust Service operations. The conflict of interests is avoided by separation of duties. Personnel in Trusted Roles is

not allowed to accept the certificate application for herself as Subscriber or for the legal person as Subscriber represented by her.

Personnel at subcontractors receive appropriate training to perform their functions if and when they act as personnel in trusted roles.

5.3.2 Background Check Procedures

For all personnel seeking to become personnel in Trusted Roles, the verification of identity is performed through the physical presence of such personnel before the personnel in Trusted Roles can perform AK operational or security functions. Furthermore, officially recognized documents of identification e.g., ID card or passports are checked. Suitability is further confirmed through background checking procedures.

Background verification checks are carried out in accordance with relevant laws, regulations and principles of ethics. The checks are proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. These checks are conducted on all candidates for employment and on contracted partners directly performing the Trust Service providing operations with access to production data.

Background checks about criminal record are refreshed periodically.

5.3.3 Training Requirements

The employees of AK have received adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

AK ensures that all personnel performing managerial duties with respect to the operation of AK receive comprehensive awareness training in:

- security principles and rules in AK;
- AK internal regulations and processes;
- duties they are expected to perform.

5.3.4 Retraining Frequency and Requirements

The requirements of chapter 5.3.3 will be kept current to accommodate changes in AK system. Refresher training will be conducted as required, and AK is testing security awareness of all personnel at least once a year.

5.3.5 Job Rotation Frequency and Sequence

No rotation used.

5.3.6 Sanctions for Unauthorized Actions

AK establishes, maintains and enforces employment policies (as part of AK Information security policy) for the discipline of personnel following unauthorized actions. Disciplinary actions include measures up to and including termination and will be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

AK uses sub-contractors in Trusted Roles specified in the service-based Practice Statement. In this case AK delegates and defines the relevant requirements to the sub-contractor according to its role and tasks. The sub-contractor is responsible for compliance with defined requirements and its personnel acting in Trusted Roles.

5.3.8 Documentation Supplied to Personnel

Persons in Trusted Roles receive the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

These procedures apply to all devices involved in the life cycle management of certificates and CRL.

The audit log is a tool for documenting and retrieving information about events concerning security in the CA and RA systems. The audit log is a distributed set of data located at RA, Certification Authority System, and central storage entities.

The audit log is used to maintain a secure production environment.

The logs are stored securely and in such a way that they can be made available for review in a timely manner.

5.4.1 Types of Events Recorded

AK ensures that all relevant information concerning the operation of the Trust Services is recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of Trust Service Tokens and the audit log of the Trust Service operation.

AK's information systems or the service provider systems leave an audit log of:

- all events relating to the life cycle of keys and certificates managed by AK;
- all significant security events, including changes in the information security policy settings, system start-up and shutdown, system crashes and hardware failures, changes in firewall configuration and rule base and PKI system access attempts, the activities of system users with superuser rights;
- all events relating to the synchronization of the clock to UTC, the detection of loss of synchronization;
- all events related to registration, including requests for certificate re-key and renewal;
- all registration information, including identity proofing:
    - type of document(s) presented by the applicant to support registration;
    - record of unique identification data, numbers, or a combination thereof of identification documents;
    - storage location of copies of applications and identification documents;
    - identity of the entity accepting the application;
    - method used to validate identification documents;
    - name of submitting Registration Authority;
- all requests and reports relating to suspension and termination of suspension;
- all requests and reports relating to revocation, as well as the resulting actions.

5.4.2 Frequency of Processing Log

The logs are created in real time and can be inspected at any time by an operator with enough access rights. CA system and central servers in the operating infrastructure are either automatically monitored on a continuous basis, with alerts for security-sensitive events and traces of hostile behavior, or reviewed by an operator with enough privileges, at least once a day. System administrators are responsible for regular reviewing of system logs and reporting of possible incidents.

Identifying important event types and extracting fields is responsibility of system administrators, security officer and integrators according to their work task.

5.4.3 Retention Period for Audit Log

Audit logs are retained on-site for no less than ten years.

In case of termination AK audit logs are retained and accessible until abovementioned term for retention accordance with clause 5.8 of this TSPS.

5.4.4 Protection of Audit Log

AK uses information security solutions confirming with the standards, which ensure non-recording of private keys, activation codes, access codes (e.g. PIN) or other security critical information in the audit log.

All logs are stored locally and are sent to the central log server. The central log servers implement the logging policy – retention and archiving.

Archived application logs have a cryptographic protection.

Internal development process defines security requirements for logging process and logs, including protection of logs. Logs are copied to a remote system which has its own access control to prevent accidental or deliberate deletion.

Non-electronic audit information is protected from unauthorized viewing, modification, and destruction through organizational means.

Access to the audit log is limited on the role/privilege basis.

Should the audit log concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons whose right of access to them arises from the law.

5.4.5 Audit Log Backup Procedures

AK performs regular backups of critical system data, audit log data, and other sensitive information. Audit log data backup is the part of general back-up system. AK has a defined backup strategy.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network, and operating system level. Non-electronically generated audit data is recorded by AK persons in Trusted Roles.

5.4.7 Notification to Event-Causing Subject

No stipulations.

5.4.8 Vulnerability Assessments

The operation of the Trusted Service is subject to regular vulnerability assessments and whenever a critical part of the operation is changed. The assessment could cover the operational infrastructure, cryptographic equipment, the physical environment, data storage, software, personnel, processes and procedures and communication.

The service provider performs a regular vulnerability scan on public and private IP addresses and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

5.5 Records Archival

5.5.1 Types of Records Archived

Physical or digital archive records about certificate applications, signed agreements, Terms and Conditions, registration information (including evidences of Subscriber and Subject identity verification) and requests or applications for suspension, termination of suspension and revocation are retained.

5.5.2 Retention Period for Archive

Physical or digital archive records about certificate applications, signed agreements, registration information (including evidences of Subscriber and Subject identity verification) and requests or applications for suspension, termination of suspension and revocation are retained at least for 10 years after validity of relevant certificate.

In case of termination AK archive records are retained and accessible until abovementioned term for retention accordance with clause 5.8 of this TSPS.

5.5.3 Protection of Archive

Electronic archives are kept on disks in the data center with regular backups that are kept in a different location. Paper is first scanned and then boxed and archived at a storage facility specific for paper documents.

5.5.4 Archive Backup Procedures

Only the digital archive is backed up.

5.5.5 Requirements for Timestamping of Records

Database entries contain accurate time and date information. The timestamps are not cryptography based.

5.5.6 Archive Collection System (Internal or External)

AK uses an internal archive collection system.

RA-s use archive collection system for physical archive records which are returned to AK for archiving.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized personnel in Trusted Roles are allowed access to the archive.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons whose right of access to them arises from the law.

The integrity of the information is verified during recovery tests. The archive systems with built-in integrity controls are in use.

5.6 Key Changeover

Specified in relevant service-based Policy and/or Practice Statement.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

AK has implemented a business continuity management framework, which covers procedures of risk assessment, incident handling (includes a response to incidents and disasters), recovery and recovery exercises.

AK carries out a regular risk assessment of AK's Trust Services to prevent possible danger to the availability of AK's operations and to minimize the risk of losing control of the Trust Services. The list of situations considered as emergency situations is determined by the risk assessment. The result of the risk assessment includes the requirements for recovery plans and recovery testing scenarios.

The procedures for the handling of information security incidents, emergency situations and critical vulnerabilities are documented in AK Security Handbook. The objective of incident procedures is the immediate response and recovery of availability and the continuous protection of AK services.

In case of private CA key compromise AK will:

- Indicate that Trust Service Tokens and validity or revocation status information issued using this CA key may no longer be valid;
- Revoke any CA certificate that has been issued for AK when AK is informed of the compromise of another CA;
- Inform all affected subscribers and relying parties.

In case of algorithm or associated parameters become insufficient for its remaining intended usage AK will additionally:

- Schedule a revocation of any affected Trust Service Token;
- Inform all affected subscribers and relying parties.

Recovery plans are tested annually.

The critical vulnerability is addressed no later than 48 hours after its discovery; the vulnerability is remediated, or a mitigation plan is created and implemented to reduce the impact of vulnerability or a decision has been made and documented that remediation is not required.

In the event of a major emergency, AK will inform all the Subscribers and Relying Parties immediately (or at least within 24 hours of the crisis committee's decision) of the emergency and proposed solution through public information communication channels.

AK will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies of any breach of security or loss of integrity that has a significant impact on the Trust Service provided.

If breach is likely to involve personal data and is likely to result in high risk to the rights and freedoms of the natural person, AK will notify the Icelandic Data Protection Agency without undue delay, but at least in 72 hours after initial discovery of the personal data breach.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

Corruption of computer resources, software and data is handled according to AK Security Handbook. In the event of a logical disaster, it is possible to roll the system back to the last successful backup, correct any mistakes and then continue operating the system.

5.7.3 Entity Private Key Compromise Procedures

AK private key compromise is handled according to AK Business Continuity Plan.

5.7.4 Business Continuity Capabilities After a Disaster

In order to ensure the business continuity capabilities after a disaster AK organizes periodically a crisis management training. AK Security Handbook defines how crisis management and communication take place in emergency situations.

There is an internal agreement about priorities for systems and services recovery after the emergency or/and service interruption. AK maintains necessary back-up copies and archives to be able to restore data after the emergency. Backups of the most critical information (e.g. keys and configurations) are kept off-site in secure storage. Back-up arrangements are regularly tested to ensure that they meet the business continuity requirements.

AK has dual data centers to ensure the availability of services. AK office and data centers are independent of each other. In case of an emergency in the data centers guidance's, source codes and other necessary materials are available from AK Office. In case of an emergency at AK office, services in data centers will continue to work.

5.8 CA or RA Termination

AK has defined a Termination Plan. The Trust Service is terminated:

- with a decision of the Board of AK;
- with a decision of the Supervisory Body;
- with a judicial decision;
- upon the liquidation or termination of the operations of AK.

AK ensures that potential disruptions to Subscribers and Relying Parties are minimized as a result of the termination of AK's services and it ensures the continued maintenance of information required to verify the correctness of Trust Service Tokens.

Before AK terminates a Trust Service the following procedures will be executed:

- AK informs all Subscribers and other entities with which AK has agreements or other forms of established relations. In addition, this information will be made available to other Relying Parties;
- AK makes the best effort for doing arrangements with other Trust Service Provider to transfer the provision of services for its existing customers;
- AK destroys the CA private keys, including backup copies or keys withdrawn from use in such a manner that the private keys cannot be retrieved;
- AK reinitializes or destroys any hardware appliances related to this service depending on the security regulations;
- AK terminates authorization of all subcontractors to act on behalf of AK in carrying out any functions relating to the process of issuing Trust Service Tokens;
- AK will preserve the integrity and availability of the CRL and only issue last CRL when all certificates in scope have expired or been revoked. In the last CRL issued, the nextUpdate field value will be set as "*99991231235959Z*".

The notice of termination of AK's Trust Service will be published in the public media.

AK does not assume liability for any loss or damage sustained by the user of the service because of such termination if AK has given the notice of termination through public information communication channels at least one month in advance.

In case AK is goes bankrupt or for other reasons is unable to cover the costs by itself, arrangements have been made as further described in the Termination plan.

In case AK goes bankrupt RA services will also be terminated as AK is the sole provider of the RA services.

The Termination Plan is reviewed annually and updated as needed with new information.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

AK uses cryptographic keys for its Trust Services and follows industry best practices for key lifecycle management, key length and algorithms.

6.1.1 Key Pair Generation

Procedure for AK Trust Service key pair generation is carried out according to the detailed Key Ceremony Script that outlines the Key Ceremony Procedure. The creation of AK's Trust Service keys is observed by an observer, which after the creation of the keys signs the key ceremony documents confirming compliance.

The Trust Service key pair generation and the private key storage occur in the HSM, which is used for providing keys that at least meet the requirements established in the security standard FIPS PUB 140-2 Level 3. The HSM protects the key from external compromise and operates in a physically secure environment.

AK has documented procedure for conducting AK Trust Service key pair generation. The script outlines the procedure, describing which roles are participating in the ceremony, which functions to be performed by every role (when, where and how), responsibilities of each role during and after the ceremony and requirements of evidence to be collected of the ceremony. At the end of the ceremony all roles partaking in the ceremony sign the Key Ceremony Script confirming that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. The more detailed procedures for key ceremony, roles, and responsibilities of participants during and after procedure, requirements for report and collected evidences are defined in AK Security Handbook.

Early enough before expiration of its Trust Service certificate, AK generates a new Trust Service certificate for signing subject key pairs and apply all necessary actions to avoid disruptions of any operations that rely on the certificate and to allow all relying parties to become aware of key changeover. Common name of the Trust Service certificate always contains the number of the year which it was created. The new Trust Service certificate is generated and distributed according to this TSPS and service-related practice statements.

The Subscriber Private Key generation is specified in relevant service-based Policy and/or Practice Statement.

6.1.2 Private Key Delivery to Subscriber

Specified in relevant service-based Policy and/or Practice Statement.

6.1.3 Public Key Delivery to Certificate Issuer

Specified in relevant service-based Policy and/or Practice Statement.

6.1.4 CA Public Key Delivery to Relying Parties

All AK Trust Services public keys are distributed in the form of X.509 certificates issued by AK CA. The primary distribution mechanism for AK Trust Service certificates is via AK repository at repo.audkenni.is. AK takes obligation to provide AK Trust Service certificates to Trusted List of Iceland.

6.1.5 Key Sizes

Specified in relevant service-based Policy and/or Practice Statement.

6.1.6 Public Key Parameters Generation and Quality Checking

The Trust Service key pair for all CAs is generated in the HSM certified with FIPS 140-2, level 3 standard according to the profile specified in relevant service-based Practice Statement. Key pair generation is observed by the commission nominated by the CEO of AK.

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

Specified in relevant service-based Policy and/or Practice Statement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

AK private keys are stored in a FIPS 140, level 3 or Common Criteria certified HSM, and it is not possible to export these from the HSM as plain text.

AK verifies that HSM is not tampered with after its reception and installation. This is documented in the HSM life-cycle protocol.

AK verifies that HSM is functioning correctly during usage.

Cryptographic module standards and controls for cryptographic devices which carry the Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

AK Signing keys are only used for issuing certificates, signing revocation requests and issuing CRLs.

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

The access to AK Trust Service keys is divided into two parts that are secured by different persons in Trusted Roles. For activation of the signing key of AK the presence of at least two authorized persons is required in accordance with clause 5.2.2 of this TSPS.

6.2.3 Private Key Escrow

AK Trust Service private keys are held in secure cryptographic devices certified with the FIPS 140-2 level 3 standard. The activation and use of the private key require multi-person control as explained in clause 6.2.2 in this TSPS.

Subscriber Private Keys escrow is specified in relevant service-based Policy and/or Practice Statement.

6.2.4 Private Key Backup

To meet the availability requirements, a backup copy is made of AK Trust Service private keys by securely cloning them into the backup HSM. Key access is divided into two parts that are secured by different persons. The certification keys of AK can be used only when they are activated. For activation of the certification key of AK the presence of at least two authorized persons is required as explained in clause 6.2.2 in this TSPS.

The Subscriber's Private Keys backup is specified in relevant service-based Policy and/or Practice Statement.

6.2.5 Private Key Archival

AK will not archive AK Trust Service private keys after expiration. All copies of AK Trust Service private keys are destroyed after their expiry or revocation so that further use or derivation thereof is impossible.

There is no archive of Subscribers private keys.

6.2.6 Private Key Transfer into or From a Cryptographic Module

All AK Trust Service keys must be generated by and in the cryptographic module. AK generates Trust Service key pairs in the HSM in which the keys will be used.

6.2.7 Private Key Storage on Cryptographic Module

AK Trust Service Private Keys held in the HSM are stored in encrypted form.

The Subscriber's Private Keys storage is specified in relevant service-based Policy and/or Practice Statement.

6.2.8 Method of Activating Private Key

AK Trust Service private keys are activated according to the specifications of the cryptographic module manufacturer. For activation of the certification key of AK the presence of at least two authorized persons is required as explained in clause 6.2.2 of this TSPS.

Method of activating Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

6.2.9 Method of Deactivating Private Key

AK Trust Service private keys are deactivated when an attempt is made to open the security module used for storage of the keys, when the configuration is changed or in other events endangering the security.

Method of deactivating Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

6.2.10 Method of Destroying Private Key

Method of destroying the AK Trust Service private keys and internal control mechanisms depend on the options available to specific secure cryptographic module.

6.2.11 Cryptographic Module Rating

Refer to clause 6.2.1 of this TSPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All certificates issued (including all expired or revoked certificates) are retained and archived as part of AK routine backup procedures. Public keys are archived for subsequent verification of signatures. The retention period is for a minimum of 10 years.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The operational period of a certificate ends upon revocation. The operational period for key pairs is the same as the operational period for the certificates, except that they may continue to be used for signature verification.

In addition, AK stops issuing new certificates at an appropriate date prior to the expiration of the Trust Service certificate such that no Subscriber certificate expires after the expiration of the Trust Service certificate.

If an algorithm or the appropriate key length does not offer enough security during the validity period of the certificate, the concerned certificate will be revoked, and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by AK management.

For Subscriber certificates, the validity period is defined in relevant service-based Policy and/or Practice Statement.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

AK Trust Service private key activation data generation and installation is performed according to the user manual of the HSM.

The Subscriber's Private Key PINs generation and installation is specified in relevant service-based Policy and/or Practice Statement.

6.4.2 Activation Data Protection

HSM is kept in secure storage and only authorized personnel in Trusted Roles have access to it.

The Subscriber's Private Key PINs protection is specified in relevant service-based Policy and/or Practice Statement.

6.4.3 Other Aspects of Activation Data

Specified in relevant service-based Policy and/or Practice Statement.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

AK ensures that the certification system components are secure and correctly operated, with an acceptable risk of failure.

AK certification services system components are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that change must be approved by the Security Officer. The approval is documented for further reference.

All critical software components of AK are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorized software.

All media containing production environment software and data, audit, archive, or backup information are stored within AK with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic). Media management procedures and backup of records and data to different media types protects against obsolescence and deterioration of media within the period that records are required to be retained. Media containing Sensitive Information are securely disposed of when no longer required.

The performance of AK services and IT systems and their capacity is monitored, and changes are done when necessary according to internal change management procedure.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

AK security operations include operational procedures and responsibilities, secure systems planning and acceptance, protection from malicious software, backups, network management, monitoring of audit logs event analysis and follow-up, media handling and security, data, and software exchange.

AK has implemented security measures and enforced access control in order avoid unauthorized access and attempts to add, delete, or modify information in applications related to the services, including certificates and revocation status information. User accounts are created for personnel in specific roles that need access to the system in question. AK's personnel are authenticated before using critical applications related to the services. Multi-factor authentication or split passwords for all accounts capable of directly causing certificate issuance is enforced. All users must log in with their personal account, and administrative commands are only available through personal administration accounts with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to

prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually. Use of System utility programs is managed and restricted to authorized persons only.

6.5.2 Computer Security Rating

AK uses standard computer systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by AK; or an analysis is carried out on behalf of AK to ensure that security is built into the Information Technology's systems.

The software will be approved by the Security Committee and will originate from a trusted source. New versions of software are tested in a testing environment of the appropriate service and their deployment is conducted according to documented change management procedures. Changes to systems are documented.

6.6.2 Security Management Controls

Measures are implemented in the information systems of AK, including all workstations for guaranteeing the integrity of software and configurations, as well as for detecting fraudulent software and restricting it from spreading.

Only the software directly used for performing the tasks is used in the information system.

6.6.3 Life Cycle Security Controls

AK policies, assets and practices (including TSPS) for information security are reviewed by person which is responsible for administering and maintaining them at planned intervals or in case of significant changes to ensure their continuing suitability, adequacy and effectiveness.

The configurations of AK systems are regularly checked for changes that violate AK security policies. A review of configurations of the issuing systems, security support systems, and front-end/internal support systems occurs regularly. The Security Officer approves changes that have an impact on the level of security provided.

AK has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available. The reasons for not applying any security patches will be documented.

AK manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment. A responsible person has been appointed for all important information security assets.

6.7 Network Security Controls

AK network is divided into sub-networks by security requirements. Communication between the network sections is restricted. Only the protocols needed for AK services are allowed through the firewalls.

There are separate and dedicated firewalls in place for enforcing the information security policy. Access to the administrative interfaces of IT equipment is not directly accessible from the public Internet. For the most critical tasks a separate workstation is used.

The front-end systems are in a DMZ protected by a firewall and load balancers. Actual security critical services and corresponding HSMs run in a secure zone that is separated by dedicated firewall and has no direct Internet access.

The CA is in a high security zone separate from all the other networks. AK systems are configured with only these accounts, applications, services, protocols, and ports that are used in the Trust Service operations.

AK ensures that only personnel in Trusted Roles have access to a secure zone and a high security zone.

The cabling and active equipment along with their configuration in AK internal network are protected by physical and organizational measures.

AK operates data centers in separate sites and with separate duplicated external network connection for redundancy to ensure high level availability of the Trust Services. Communication between sites is cryptographically secured.

All data centers are in a common internal secure network carrying the DMZ and secure zone. The transfer of Sensitive Information outside AK internal network is encrypted.

Communication between distinct trustworthy systems is established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

The security of AK internal network and external connections is monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

AK performs a vulnerability scan once monthly on public and private IP addresses identified by AK.

AK undergoes a penetration test on the certification systems at the set up and after the infrastructure or application upgrades or modifications determined significant by AK.

AK records evidence that each vulnerability scan and penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

All RAs access the RA system through a closed secure network. The RA system is run by AK and all RA officers must logon to the system with electronic certificates to authenticate their identity.

6.8 Timestamping

AK does not provide time-stamping service as a qualified Trust Service.

AK does not use timestamping in relation to certification service. Database entries contain accurate time and date information. The time information is not cryptographic based. The maximum allowed time variance in all parts of the certification system is 1 second. This is guaranteed by an internal Reference Clock service, according to which the chronologies of all parts of the certification system are synchronized. The Reference Clock uses GPS as a primary time source which determines correctness of the time in AK's system. Time used to record events is synchronized to UTC at least every 24 hours.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Specified in relevant service-based Policy and/or Practice Statement.

7.2 CRL Profile

Specified in relevant service-based Policy and/or Practice Statement.

7.3 OCSP Profile

Specified in relevant service-based Policy and/or Practice Statement.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The conformity of information system, policies and practices, facilities, personnel, and assets of AK are assessed by a conformity assessment body pursuant to the eIDAS regulation [1], the corresponding legislation and standards or whenever a major change is made to Trust Service operations.

AK's internal auditor carries out an internal audit according to the audit schedule.

8.2 Identity/Qualifications of Assessor

Conformity assessment body is accredited in accordance with Regulation EC no 765/2008 as competent to carry out conformity assessment of qualified Trust Service Provider and qualified Trust Services it provides.

8.3 Assessor's Relationship to Assessed Entity

The auditor of the conformity assessment body shall be independent from AK and AK assessed systems.

The internal auditor shall not audit his/her own areas of responsibility.

8.4 Topics Covered by Assessment

The conformity assessment covers the conformity of information system, policies and practices, facilities, personnel, and assets with eIDAS regulation, respective legislation, and standards.

Conformity assessment body audits the parts of AK information system used to provide Trust Services.

The Conformity Assessment Body and the Internal Auditor also audit these parts of the information system, policies and practices, facilities, personnel, and the assets of sub-contractors that are related to providing AK Trust Services (e.g. including RAs).

8.5 Actions Taken as a Result of Deficiency

In the event of a result showing deficiency in the assessment, the Supervisory Body requires AK to remedy any failure to fulfil requirements within a time limit (if applicable) set by the Supervisory Body. AK makes efforts to stay compliant and fulfil all requirements of the deficiency on time. AK management is responsible to implement a corrective action plan. AK evaluates the significances of deficiencies and prioritizes appropriate actions to be taken at least during the time limit declared by Supervisory Body or reasonable period.

Where personal data protection rules appear to have been breached, the Supervisory Body shall inform the data protection authority of the results of the compliance audit.

8.6 Communication of Results

Audit conclusions or certificate(s) for trust service(s), which are based on audit results of the conformity assessment conducted pursuant to the eIDAS regulation, corresponding legislation and standards, are published on AK's website repo.audkenni.is.

In addition, AK submits the resulting conformity assessment report to the Supervisory Body within at period of three working days of receiving it. AK submits the audit conclusions or certificate(s) for trust service(s) to other interested parties.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Specified in relevant service-based Policy and/or Practice Statement.

9.1.2 Certificate Access Fees

Specified in relevant service-based Policy and/or Practice Statement.

9.1.3 Revocation or Status Information Access Fees

Specified in relevant service-based Policy and/or Practice Statement.

9.1.4 Fees for Other Services

Fees for services are specified in AK's price list or in the Subscriber's or Relying Party's agreement.

9.1.5 Refund Policy

AK handles refund requests on a case-by-case basis.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

AK acquires insurance policy covering various matters including operation interruption insurance and professional liability insurance.

9.2.2 Other Assets

According to relevant agreements AK may give some additional warranties.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to clause 9.2.1 of this TSPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to AK because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from AK about him/herself according to legal acts.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential or intended for internal use is public information. Information considered public in AK is listed in clause 2.2 of this TSPS.

Additionally, non-personalized statistical data about AK's services is also considered public information. AK may publish non-personalized statistical data about its services.

9.3.3 Responsibility to Protect Confidential Information

AK secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information based on a court order or in other cases provided by law.

9.4 Privacy of Personal Information

9.4.1 Personal Data Protection Principles

AK's principles of personal data protection are described in the principles of client data protection. The principles are published on AK's website: www.audkenni.is

By adhering to the above-mentioned principles, AK guarantees compliance with the Personal Data Protection Act [6] as well as non-disclosure of confidential information and adequacy of subscriber's information storage.

9.4.2 Personal Information Processed by AK

The scope of personal information processed by AK is described in the Principles of Client Data Protection [7].

9.4.3 Responsibility to Protect Private Information

AK ensures protection of personal information by implementing security controls as described in chapter 5 of this TSPS.

9.4.4 Notice and Consent to Use Private Information

The exact terms under which the subscriber grants AK his/her notice and consent to use his/her personal information are described in the Principles of Client Data Protection [7].

9.4.5 Disclosure Pursuant to Judicial or Administrative Process

The circumstances under which AK may disclose the subscriber's personal information to third parties are described in the Principles of Client Data Protection [7].

9.4.6 Other Information Disclosure Circumstances

The circumstances under which AK may disclose the subscriber's personal information to third parties are described in the Principles of Client Data Protection [7].

9.5 Intellectual Property Rights

AK obtains intellectual property rights to this TSPS.

9.6 Representations and Warranties

9.6.1 Trust Service Provider Representations and Warranties

AK has contractual obligations with various entities in relation to its services as a TSP. This TSPS and service-based Practice Statements are integral parts of these obligations.

AK shall:

- provide its services consistent with the requirements and the procedures defined in this TSPS and service-based policies and practice statements;
- carry overall responsibility for conformance with the procedures defined in this TSPS and service-based policies and practices statements;
- comply with eIDAS regulation [1] and related legal acts defined in this TSPS and service-based policies and practice statements;
- publish its TSPS and service-based policies and practice statements and guarantee their availability in a public data communications network;
- publish and meet its claims in terms and conditions for subscribers and other Relying parties and guarantee their availability and access in a public data communications network;

- maintain confidentiality of the information which has come to its knowledge in the course of supplying the service and is not subject to publication;
- keep account of the Trust Service Tokens issued by it and their validity and ensure possibility to check the validity of certificates;
- inform the Supervisory Body of any changes to a public key used for the provision of Trust Services;
- notify the Supervisory Body and, where applicable, other relevant bodies of any breach of security or loss of integrity that has a significant impact on the Trust Service provided;
- notify the Icelandic Data Protection Agency of any personal data breach, which is likely to result in high risk to the rights and freedoms of a natural person;
- where the breach of security or loss of integrity or personal data breach is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach;
- preserve all the documentation, records and logs related to Trust Services according to the clauses 5.4 and 5.5;
- ensure a conformity assessment according to requirements and present the conclusion of conformity assessment body to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- have the financial stability and resources required to operate in conformity with this TSPS;
- publish the terms of the compulsory insurance policy and the conclusion of conformity assessment body in a public data communications network.
- AK requires that senior executive, senior staff and staff in trusted roles shall be free from any commercial, financial and other pressures which might adversely influence trust in the services provided.

Any employee of AK shall have a clear criminal record.

AK has documented agreements and contracts with its subcontracting and outsourcing parties provisioning services. AK has defined in these agreements and contracts the liability, relevant requirements and right to audit, subcontracting and outsourcing parties to be ensured that they are bound to implement any requirements and controls required by AK.

In accordance with the relevant legislation, AK does its best to guarantee that all potential service users, especially people with disabilities, can access services provided by AK on an equal basis. AK accepts that its services imply at least some sort of qualitative capabilities and legal capacity, but nonetheless truly aspires to provide trust services and related technical solutions in a non-discriminating way.

9.6.2 RA Representations and Warranties

RA shall:

- provide its services consistent with the requirements and the procedures defined in the contract between AK and RA, in this TSPS and service-based Policies and Practice statements;
- provide its employees with necessary training for supply of high-quality service;
- without undue delay after having become aware of it, notify AK of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

Any RA officer employed by the RA shall have a clear criminal record.

9.6.3 Subscriber Representations and Warranties

The Subscriber shall:

- observe the requirements provided by AK in this TSPS and the respective service-based policies, terms and conditions and/or practice statements;

- supply true and adequate information in the application for the services, and in the event of a change in the data submitted, he/she shall provide the correct data in accordance with the rules established in the service-based policies and practice statements;
- accept that AK may refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;
- be solely responsible for the safekeeping of his/her private key and Trust Service Tokens. The Subscriber shall use his/her private key and Trust Service Tokens in accordance with this TSPS, service-based practice statements and service terms and conditions.

9.6.4 Relying Party Representations and Warranties

A Relying Party shall:

- study the risks and liabilities related to the acceptance of Certificates. The risks and liabilities have been set out in this TSPS, in the appropriate service-based policies and practice statements and in the service terms and conditions.
- verify the validity of Certificates based on services offered by AK using published information on AK's website or applicable service or appropriate cryptographic information.

9.6.5 Representations and Warranties of Other Participants

Specified in relevant service-based Policy and/or Practice Statement.

9.7 Disclaimers of Warranties

AK:

- is liable for the performance of all its obligations specified in clause 9.6.1 to the extent required by the legislation of the Republic of Iceland;
- has compulsory insurance contracts, which cover all AK Trust Services to ensure compensation for damage which is caused as a result of violation of the obligations of AK.

AK is not liable for:

- the secrecy of the private keys of the Subscribers, possible misuse of the certificates or inadequate checks of the certificates or for the wrong decisions of a Relying Party or any consequences due to errors or omission in Trust Service Token validation checks;
- the non-performance of its obligations if such non-performance is due to faults or security problems of the Supervisory Body, the data protection supervision authority or any other public authority or Trusted List;
- non-fulfilment of the obligations arising from the TSPS if such non-fulfilment is occasioned by Force Majeure.

9.8 Limitations of Liability

The upper limit of the liability for any claim is established in the referred policy available at repo.audkenni.is.

9.9 Indemnities

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

9.10 Term and Termination

9.10.1 Term

Refer to clause 2.2.1 of this TSPS.

9.10.2 Termination

This TSPS and/or service-based Practice Statements remain in force until they are replaced by a new version or when they are terminated due to Trust Service or AK's termination.

Upon AK's termination, AK is obliged to ensure the protection of personal and confidential information.

9.10.3 Effect of Termination and Survival

AK communicates the conditions and effect of this TSPS's and/or service-based Practice Statements 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 public information of repository, AK archives for determined period and logs survive termination. All Subscriber applications remain effective until the certificate is revoked or expired, even if this TSPS and/or service-based Practice Statements terminate.

Termination of this TSPS and/or service-based Practice Statements cannot be done before termination actions described in clause 5.8 of this TSPS.

9.11 Individual Notices and Communications with Participants

In general, AK's website will be used to make any type of notification and communication.

Other means of individual notices and communication is specified in relevant service-based Policy and/or Practice Statement.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to clause 1.5.4 of this TSPS.

9.12.2 Notification Mechanism and Period

Refer to clause 2.2.1 of this TSPS.

9.12.3 Circumstances Under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

All disputes between the parties will be settled by negotiations. If the parties fail to reach and amicable agreement, the dispute will be resolved at the court of the location of AK.

The other parties will be informed of any claim or compliant not later than 30 calendar days after the detection of the basis of the claim, unless otherwise provided by law.

The Subscriber or other party can submit their claim or complaint to AK by phone or email.

9.14 Governing Law

This TSPS is governed by the jurisdiction of the Republic of Iceland.

9.15 Compliance with Applicable Law

AK ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- Electronic Identification and Trust Services for Electronic Transactions Act [1]
- Personal Data Protection and data processing Act nr. 90/2018; [6].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

AK contractually obligates each RA and other participants to comply with this TSPS 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 this TSPS, 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 agreement.

9.16.2 Assignment

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

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 TSPS does not waive AK's right to enforce the same provision later or right to enforce any other provision of this TSPS. To be effective, waivers must be in writing and signed by AK.

9.16.5 Force Majeure

The subject of Force Majeure and other parties are responsible for any consequences caused by circumstances beyond his reasonable control, including but without limitation to war (whether declared or not), acts of government or the European Union, export or import prohibitions, breakdown or general unavailability of transport, general shortages of energy, fire, explosions, accidents, strikes or other concerted actions of workmen, lockouts, sabotage, civil commotion and riots.

Communication and performance in the case of Force Majeure are regulated between the parties with the agreements.

Non-fulfilment of the obligations arising from TSPS and/or relevant service-related Policies and/or Practice Statements is not considered a violation if such non-fulfilment is occasioned by Force Majeure. None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this TSPS and/or relevant service-related Policies and/or Practice Statements caused by Force Majeure.

9.17 Other Provisions

Not applicable.

REFERENCES

[1] Electronic Identification and Trust Services for Electronic Transactions Act nr. 55/2019;

[2] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

[3] CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly Trusted Certificates, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.3.pdf;

[4] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, https://www.ietf.org/rfc/rfc3647.txt;

[5] ISO/IEC 27001:2017 Information technology - Security techniques -Information security management systems – Requirements; https://www.audkenni.is/repository/;

[6] Personal Data Protection and data processing Act nr. 90/2018;

[7] Principles of Client Data Protection, published: https://www.audkenni.is/um-audkenni/meðferð-persónuupplýsinga/;

[8] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

[9] ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

[10] Key Words for Use in RFCs to Indicate Requirement Levels, S.Bradner, RFC2119, March 1997