CERTIFICATE POLICY

ORGANISATION CERTIFICATES

For Digital and Population Data Services Agency

OID: 1.2.246.517.1.10.203

ISO 9001

ISO/IEC 27001

01/01/2020

DOCUMENT MANAGEMENT	
Owner	
Author	Tuire Saaripuu
Checked by	
Approved by	Kankaanrinne Joonas

Certificate policy for Digital and Population Data Services Agency's organisation certificate.

VERSION MANAGEMENT		
version no	action	date/author
v.1.0	Approved version 1.0., an eIDAS-compliant document	3 May 2018
v.1.1	Approved version 1.1, Centre name change.	1 Jan 2020

01/01/2020

Contents

01/01/2020

1 Foreword

This document is based on a technical specification prepared by the ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

2 Introduction

Electronic services require that the source of data be identified in a manner comparable to a handwritten signature on documents. Usually, this can be implemented by using electronic signatures. Certificate service providers, who generally are called certification authorities, produce certificates needed for electronic signatures.

Users of electronic signatures can trust the genuineness of electronic signatures if the certification authority has appropriate procedures and protection measures in place to minimise the operational and economic risks pertaining to public key encryption systems.

Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC shall apply with regard to signature certificates in trust services as of 1 July 2016. The procedural requirements concerning the activities and administrative practices of certification authorities that issue signature certificates under the Regulation are described in this document. The use of a secure signature creation device is described in the procedural requirements specified in this document.

The certificate policy is a document drawn up by the Certification Authority (CA) which describes the practices and principles used in certification. The certification practice statement is a more detailed description of the CA's activities than the certificate policy.

This certificate policy applies to organisation certificates of the Digital and Population Data Services Agency.

The organisation certificate consists of a certificate pair with two different purposes: the authentication and encryption certificate and the signature certificate, which is a signature certificate conformant to the Act on Strong Electronic Identification and Trust Services.

3 Scope

This document specifies the procedure requirements that apply to certification authorities that grant signature certificates and to Digital and Population Data Services Agency, which is the provider of a strong electronic identification means. Procedure requirements are set for the activities and administration practice of certification authorities that grant certificates so that the subscribers, signers certified by the certification authority and the parties trusting the certificate can trust that the certificate can be used to verify electronic signatures.

The provision of the strong electronic identification means offered by Digital and Population Data Services Agency takes place in the same production environment, with similar technical and functional solutions and subject to the same procedures as with the provision of the signature certificate granted by Digital and Population Data Services Agency.

The procedure requirements on the certification authority contain requirements on the provision of registration services, creation of certificates, distribution of certificates, management of certificate revocation, revocation status and, if necessary, the provision of a means of creating a signature. Other functions of the certificate service provider, such as time stamps, attribute certificates and confidentiality-supporting services, are excluded from the scope of this application. This document does not present requirements for the certification authority's certificates, certificate hierarchies or cross-certification. These procedure requirements are limited to apply to the certification of keys used in connection with electronic signatures.

These procedure requirements are specifically targeted at signature certificates granted to the public, where such certificates are used to support electronic signatures according to the Regulation. Certificates granted according to these procedure requirements can be used for authenticating a person acting on behalf of himself/herself or a natural person, legal entity or organisation represented by the person.

These procedure requirements apply to the use of public key encryption in certifying electronic signatures.

Independent, competent bodies may rely on this document when assessing whether the certification authority meets the requirements on the granting of signature certificates.

Certificate holders and parties trusting a certificate are urged to read more detailed information in the certification authority's certification practice statement on how the certification authority in question implements its specific certificate policy.

This document does not, however, specify how independent parties can assess the requirements set forth herein, for example there are no requirements regarding the information made available to independent assessors or the assessors themselves.

4 List of references

This document refers to regulations and specifications presented in the following documents. They are binding with respect to functions described in this document.

- The references used with respect to date of publishing or version numbers are either specific or non-specific.
- For specific references, only the cited version applies.
- For non-specific references, only the latest version of the referenced document applies.

Material related to this document is available at the following location, among others: http://docbox.etsi.org/Reference. ETSI does not guarantee the long-term functionality of the link.

Compelling references:

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

[2] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".

[3] Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5, CA/Browser Forum.

[4] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

Guideline references:

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.3] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

[i.4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the

protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider

Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

Terminology descriptions:

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [1], ETSI

EN 319 411-1 [2], the Regulation (EU) N° 910/2014 [i.1] and the following apply:

EU Qualified Certificate: qualified certificate as specified in Regulation (EU) No. 910/2014 [i.1]

Qualified Electronic Signature/Seal Creation Device: As specified in Regulation (EU) No. 910/2014 [i.1].

5 Definitions and abbreviations

5.1 Definitions

The following concepts and definitions are used in this document:

Activation data: A confidential data (PIN code) that is needed to activate private keys stored in a microchip and to use them in public key methods (e.g. electronic signatures).

Signer: A party marked in a certificate as the holder of the private key related to the public key issued in the certificate

Data used for creating a signature: A unique dataset, such as codes or private encryption keys, that the signer uses in order to create a digital signature. A more detailed description is based on requirements conformant to specifications issued on the basis of the Regulation.

In case of signature certificates based on public key encryption, such as in the scope of application of this document, the data used for the creation of the signature include the private keys. Thus, this document refers to the data used for creating a signature as private key.

Signature creation tool: Appropriately configured software or hardware with which data used for creating a signature are processed. A more detailed description is based on the requirements of the Regulation.

Data used for authenticating a signature: A dataset, such as codes or public encryption keys, used for authenticating a digital signature. A more detailed description is based on the requirements of the Regulation.

In case of signature certificates based on public key encryption, such as in the scope of application of this document, the data used for the authentication of the signature include the public keys. Thus, this document refers to the data used for authenticating a signature as public key.

Attribute: A data element associated with a party, specifying a property of the party, such as group membership or role, or other information pertaining to that party.

Key pair: A pair of interconnected keys, one public and one private, which are used in public key methods. The keys' purpose of use is defined in the certificate (see certificate holder's signature certificate and authentication and encryption certificate).

Asymmetric encryption: A pair of one public key and one private key is used in asymmetric encryption. A message that has been encrypted using a public key can only be opened by the private key of the key pair in question.

Personal identity card: A means of personal identification where the technical part contains the cardholder's organisation certificate.

Public key: The public component of a key pair used in asymmetric encryption in public key methods. The certification authority certifies with its digital signature that the public key belongs to the certificate holder. The public key is part of the data content of the certificate.

Public key infrastructure: A data security infrastructure in which security services are provided by public key methods.

Public key method: A data security service, such as electronic identification, which is provided by using public and private keys, certificates and asymmetric encryption.

Advanced digital signature: A signature that meets the following requirements: it is uniquely associated with

a) its signer

b) it can be used for uniquely identifying the signer

c) it has been created with means that the signer can maintain under its sole control

d) it is associated with the target data in such a way that subsequent altering of the data can be detected

Card reader software: Card reader software is used in workstations as a so-called end-user application. It enables users to use their personal identity cards and certificates stored on it in various user and application environments such as public e-services, secure email and logging on to workstations.

Signature certificate: A certificate that meets the requirements of the Regulation and that has been granted by a certification authority that meets the decreed requirements. The data content of the certificate is determined by the Act on Strong Electronic Identification and Trust Services.

Trusting party: A party that trusts the certificate data and uses the certificate for various data security services such as electronic identification of the certificate holder and authentication of digital signature.

Payment card: Generic term for credit, combination, prepaid and delayed debit cards.

Microchip: A technical platform that is used to store the certificate and private keys, integrated into an identity card, payment card or mobile terminal card.

Organisation certificate: A certificate pair granted by Digital and Population Data Services Agency to a natural person, defined in more detail in this document.

PIN code: Activation data that activates a private key held on a microchip. PIN 1: the basic code for authentication and encryption. PIN 2: a signature code for digital signing.

PUK code: A code that is needed to unblock a locked PIN code.

Registration authority: The registration authority identifies the certificate applicant in accordance with the certificate policy and certification practice statement on behalf of and at the responsibility of the Certification Authority.

RSA algorithm and RSA key: The RSA algorithm is a common public key algorithm. The private and public keys associated with an organisation certificate are RSA keys.

Revocation list: A list of certificates revoked before the end of their validity period and the revocation dates, electronically signed and published by the certification authority. The revocation list specifies the publication dates of the current and next revocation list. Revoked certificates are added to the list.

Revocation service: A technical service provider that receives certificate revocation requests and submits them to the certificate system on behalf of the certification authority.

Digital signature: Digital information that has been associated or logically associates with other digital data and which is used as an authentication method for that data and which is defined in more detail in the Act on Strong Electronic Identification and Trust Services.

E-service ID: An identifier consisting of a series of numbers and a check character that helps identify Finnish citizens and, in accordance with the Municipality of Residence Act, foreign citizens permanently residing in Finland who are entered in the Population Information System.

Digital signature: An advanced digital signature based on a signature certificate, created with a secure signature creation tool.

Secure signature creation tool: A tool for creating a signature, meets the requirements of the Regulation and regulations issued on the basis of the Regulation.

Certificate: Contains the user's public key and other data protected against forging by encrypting them with the private key of the certification authority that granted the certificate. A more detailed description is based on the ITU-T recommendation X.509.

Certificate: A digital certificate that associates the signature authentication data with the signer and authenticates the signer. A certificate contains an OID (object identifier) that identifies the certification practice statement in question.

Certificate system: A technical data system used to create certificates and sign revocation lists.

PKI disclosure statement: A document that contains the main points of the certificate policy and certification practice statement.

Certificate service provider: An organisation, legal entity or natural person that grants certificates or offers other services pertaining to digital signatures and that has been defined in more detail in the Act on Strong Electronic Identification and Trust Services.

This document applies to certificate service providers that grant signature certificates (or provide partial services for granting signature certificates—see item 4.1). This document does not cover other types of functions by the provider of certificate services, such as time stamping or backup key systems.

Certificate policy: A named rule set that indicates the suitability of a specific certificate for a specific organisation and/or suitability class, which is covered by common security requirements. A more detailed description is based on the ITU-T recommendation X.509.

More details on the mutual relationship between certificate policies and the certification practice statement are provided in section 4.3. The certificate policies published by PRC are publicly available. Each certificate policy is identified by an OID.

Certificate register: A register conformant to the Act on Strong Electronic Identification and Trust Services that a certification authority providing signature certificates to the public must maintain. Data must be held for at least 5 years after the expiry of the certificate.

Certificate management system: A data system consisting of certificate systems, data communications, a certificate directory, revocation list service, advice and revocation service, certificate management and card management.

CPS OID is part of the data content of the certificate.

Certification practice statement: A statement of the practices that the certification authority adheres to in granting, administering, revoking and renewing certificates and in exchanging certificate key pairs. Each certification practice statement is identified by an OID.

Certification authority: An organisation that issues certificates, is responsible for their provision and draws up the certificate policy that describes its operation and the associated certification practice statement. One or more parties trust the activities of a certification authority. The certification authority is a certificate service provider that grants certificates. A more detailed description is based on the ITU-T recommendation X.509.

CA certificate: Contains the name, country and public key of the certification authority.

CA's private key: The private key used by the certification authority to sign its issued certificates and published revocation lists.

Certificate applicant: A person who requests an organisation certificate and is reliably identified in conjunction with the request.

Certificate holder: A person whose identity and public key are verified by the CA's digital signature and who holds the private keys linked with the certificate in question.

Certificate applicant/holder: A natural person applying for a certificate, identified in a personal way and who, upon receiving the certificate, is the certificate holder.

Certificate holder's signature certificate: The public key in the certificate verifies the digital signature made by the certificate holder with the corresponding private key. The signature code (PIN 2) is required for the signing.

Certificate holder's authentication and encryption certificate: A certificate used for electronic personal identification and data encryption. The certificate holder uses the private authentication and encryption key for electronic identification and decryption of encrypted data or messages. The use of the key requires a basic PIN code (PIN 1).

Certificate usage and purpose: In this document, certificate usage refers to the use of the certificate and the associated keys. For example, using a certificate in digital signature refers to the use of a private key in signing and to the use of the public key and certificate in verifying the signature.

Trusting party: The recipient of a certificate that acts with trust for the certificate in question and/or digital signatures that have been verified with that signature. A more detailed description is based on the RFC 3647 specification.

Certificate revocation list: A signed list of certificates containing certificates their issuers no longer deem valid. A more detailed description is based on the ITU-T recommendation X.509.

Private key: The private component of a key pair used in asymmetric encryption in public key methods. The private keys of the certificate holder are stored on a microchip to protect them from unauthorised usage.

01/01/2020

5.2 Abbreviations

ISO 27001	ISO IEC 27001
CA	Certification Authority
CSP	Certification Service Provider
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module
EPI	Electronic Personal Identification
HTTP	Hypertext Transport Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PDS	PKI Disclosure Statement
PIN	Personal Identification Number, PIN
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key, PUK code
QCP	Qualified Certificate Policy
RSA	Rivest, Shamir, Adleman, RSA ID, a public key algorithm, asymmetric algorithm
SATU	Electronic service identifier
SIM	Subscriber Identity Module
SSCD	Secure Signature Creation Device: A secure signature creation tool
DPDSA	Digital and Population Data Services Agency

6 Common concepts

6.1 Certification authority

The certification authority creates and issues certificates that the users of certificate services, i.e., certificate applicants and parties trusting the certificates, trust. The certification authority has overall responsibility for the provision of the certificate services defined in section 4.2. The certification authority is uniquely identified in the certificate as the issuer of the certificate. Signature certificates are signed with its private key.

The certification authority may use third parties in its provision of certificate services to provide parts of the service. However, the certification authority is always responsible for the entire service it produces and ensures that the procedure requirements set forth in this document are met. The certification authority may, for example, subcontract all sub-parts of the service, including the certificate creation service. However, the key used for signing the certificates will be defined as belonging to the certification authority, and the certification authority retains overall responsibility for meeting the requirements specified in this document and the responsibility for granting certificates to be granted to the public in accordance with the Act on Strong Electronic Identification and Trust Services.

It is possible that Digital and Population Data Services Agency issues a certificate for its own purposes. In that case it follows the same requirements than issuing certificates for other organisations.

The certification authority is a certificate service provider pursuant to the Act on Strong Electronic Identification and Trust Services, which grants certificates.

Digital and Population Data Services Agency (DPDSA) works in the branch of government of the Ministry of Finance. DPDSA is a public authority which administers a personal information register and is responsible for providing certified electronic services. As of 1 December 2010, Digital and Population Data Services Agency also works as the statutory certification authority for healthcare (act on the electronic processing of client data in social and health care (159/2007), act on electronic prescriptions (61/2007) and Act on the Digital and Population Data Services Agency (304/2019), GP 155/2010 vp). DPDSA's Certificate Services are responsible for the agency's certification activities. DPDSA has provided certificate-based signing and identification means since 1999 and worked as a signature certification authority as of 31 March 2003.

DPDSA’s certificate information system and certificate services are based on the public key infrastructure (PKI). DPDSA’s certificate infrastructure consists of a certificate system, supplier of certificate data contained in the cards, a revocation list, advisory service and directory service. DPDSA's activities as a certification authority include the provision of certification, directory and revocation services, registration, and the creation and identification of a card that contains the certificate. DPDSA is responsible for the functioning of the certificate system as a whole, including on behalf of any registration authorities and technical suppliers it may use. DPDSA's Certificate Services maintains certificate policy, certification practice statement and certificate description documents, which are electronically available at www.fineid.fi.

Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and

repealing Directive 1999/93/EC applies with regard to trust services as of 1 July 2016. The obligations of the Regulation have partly been implemented also in the amendment of the Act on Strong Electronic Identification and Trust Services (617/2009), which entered into force on 1 July 2016. The act provides for the provision of strong electronic identification services and electronic signature and their legal ramifications. The Certificates issued by Digital and Population Data Services Agency are provided for in the Act on the Digital and Population Data Services Agency (304/2019).

DPDSA offers highly secure digital signature and authentication certificates and associated services. Certificates are used to verify the certificate holder's identity and the accuracy, integrity and authenticity of data contained in the certificate. Digital signing based on signature certificates and identification by strong electronic identification devices enable citizens to access public services online securely and flexibly anytime, anywhere. Signature certificate and strong electronic identification service providers are supervised by the Finnish Transport and Communications Agency (Traficom).

This certificate policy describing the issuing of an organisation certificate has been registered by Digital and Population Data Services Agency.

This certificate policy describes the issuing and production of a signature certificate for digital signatures conformant to the Act on Strong Electronic Identification and Electronic Trust Services and detailed requirements pertaining to the division of responsibility.

This document also describes solutions and procedures pertaining to the granting, production and data storage of an identification certificate offered as a means referred to in the Act on Strong Electronic Identification and Trust Services, included in the organisation certificate, conforming to the requirements of the production environment of the signature certificate.

The organisation certificate consists of a certificate pair that has two different purposes. The authentication and encryption certificate meets the requirements for a strong electronic identification means. A signature certificate intended solely for implementing a signature meets the requirements of a signature certificate. The correctness of the certificate applicant's identity is guaranteed by Digital and Population Data Services Agency.

6.2 Certificate services

A certificate is an electronic certificate that links the signature authentication data to the signatory and identifies the signatory. The certificate data are signed electronically by the CA's private key. Certificates under this certificate policy are based on a public key infrastructure and public key methods. The data content of certificates conformant to this certificate policy is defined in the Act on of the Digital and Population Data Services Agency (304/2019).

An organisation certificate conformant to this certificate policy can be granted to a Finnish citizen or a foreign national habitually residing in Finland pursuant to the home municipality act (201/1994) whose personal details have been saved in the population information system.

The Digital and Population Data Services Agency, which acts as the certifier, uses an electronic client identifier to identify the certificate holder. This identifier is also a part of the data content of the certificate. The electronic client identifier is a technical means of identification, defined in

the Act on the Digital and Population Data Services Agency (304/2019), created specifically for electronic services and does not contain personally identifying data.

An organisation certificate can be granted and saved in various technical platforms, such as microchips, for example on personal identity cards. This certificate policy is a common description for the organisation certificates on these different platforms.

Both the certificate policy and the certification practice statement of DPDSA have a unique object identifier (OID).

In this document, Digital and Population Data Services Agency's granting of signature certificates is divided into the following sub-services for requirement classification reasons:

Registration service: The registration service authenticates the identity of the signer and any special attributes that may be related to the signer, and these are relayed to the certificate creation service.

The registration service as an action also includes the delivery of a key generated by the client or a party other than the certification authority. Digital and Population Data Services Agency's registration service only processes key pairs it has produced itself.

The registration of an organisation certificate is done in conformance with the procedure set forth in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency. A more detailed procedure is described in the certificate practice statement that describes the technical platform in question.

Certificate creation service: The certificate creation service creates and signs certificates based on the identity authenticated in the registration service and on other attributes.

Distribution service: With the distribution service, all certificates are distributed to the signers and made available to parties trusting the certificate, if permission is obtained for that from the signer. In addition, the service makes the certification authority's terms of use and all published data pertaining to certificate policies and certification practice statements available to the parties trusting the certificate. The directory service is a public Internet-based service which can be used to retrieve all organisation certificates granted by the certification authority and the certification authority's certificates and revocation list. The directory service is available at ldap://ldap.fineid.fi.

Revocation management service: Revocation management service revokes a certificate when the certificate holder wishes to revoke it before its stipulated expiry date.

- Revocation management service processes revocation requests and notices and specifies the necessary measures based on the processing. The results of the service are distributed via the revocation list.

Revocation status communication service:

- The service that communicates the status of revocation is used for providing certificate revocation status data to parties trusting the certificate. The service can utilise certificate revocation lists or real-time relaying of individual status data, OCSP. Digital and Population Data Services Agency communicates the data to the revocation service for use by parties trusting the certificate. The status data are updated at certain intervals, which is described in detail in the certification practice statement document.

Providing a signature creation tool to signers:

- The signature creation tool is manufactured and delivered to signers. With regard to certificates, the associated key pairs and activation data, the manufacturer of the smart card or microchip acts on behalf of the certification authority, at its responsibility and in accordance with the agreement. Smart cards and microchips are uniquely identified in accordance with data provided by the registration authority.

The sole purpose of the service division used is to clarify the procedure requirements. This description does not restrict the division of the certification authority's service implementation.

6.2.1 The trusting party

- The trusting party is a natural person or an organisation that trusts the certificate information and uses the certificate for authentication, encryption and electronic signing. The trusting party must verify that the certificate is valid and not on a revocation list. The certification authority provides an online certificate status check service that implements OCSP.

6.3 Certificate policy and certification practice statement

This section describes the relationship between the certificate policy and the certification practice statement. This section does not apply restrictions on the form of the certificate policy or the itemisations of the certification practice statement.

6.3.1 Purpose

The certificate policy whose identifier is stated in the certificates contains a general-level description of the main principles of certificate activities. The certification practice statement describes the detailed procedures and methods pertaining to certificate activities, particularly with respect to creation and maintenance, regarding how the requirements set in the certificate policy are met.

This document specifies the certificate policy that meets the requirements conformant to the Regulation regarding signature certificates. Digital and Population Data Services Agency, which serves as the certification authority, defines in its certification practice statement how these requirements are met.

Digital and Population Data Services Agency adheres to this certificate policy when issuing an organisation certificate. Certificate holders and trusting parties must comply with this certificate policy.

Organisation certificates issued under this certificate policy can be used for strong electronic identification, encryption and electronic signing. The organisation certificate can be used without limitation according to its purpose in applications and services from both the public government and private organisations.

The certificate policy and certification practice statement contain requirements concerning the obligations of the certification authority, registration authority, certificate holder and trusting party as well as matters related to legislation and dispute resolution.

Digital and Population Data Services Agency, which is the certification authority, will replace the unique identifier of the certificate policy if it changes its certificate policy with respect to applicability.

6.3.2 Level of detail

The certificate policy describes the general requirements for the certification authority's activities. The certification practice statement describes in more detail the procedures the certification authority implements in granting certificates and other administration. The certification practice statement specifies how the certification authority meets the technical and organisation and procedure requirements specified in the certificate policy.

Digital and Population Data Services Agency, which works as a certification authority, has prepared non-public documents for controlling its internal and outsourced functions.

This certificate policy has been registered by the Digital and Population Data Services Agency, Digital and Population Data Services Agency is a public authority that has public trust and administers a personal information register and is responsible for providing certified electronic services.

6.3.3 Approach

The certificate policy and certification practice statement have been prepared for different uses. The certificate policy is a general description of the certification authority's activities. The certification practice statement describes the details of the certification authority's activities in conformance with the organisation structure, procedures, facilities and information technology environment.

6.3.4 Other documents published by the certification authority

In addition to the certificate policy and certification practice statement, the certification authority may publish other documents that guide its certificate activities. Such documents include operating instructions and general presentations regarding the certificate activities for the needs of consumers, client organisations and service builders.

The rights and obligations of an applicant of organisation certificate are specified in contract documents and general instructions for use given before the signing of the organisation certificate application, the document and instructions comprising an agreement concluded with the organisation certificate applicant. An organisation applying for an organisation certificate applies for the organisation certificate for its own members that are identified in a personal way when applying for the certificate. The application document contains the details of the rights and obligations of both parties. When an applicant for an organisation certificate applies for an organisation certificate, he/she also accepts the general terms of use.

The application document and instructions for use clearly state that the applicant for organisation certificate, with his/her signature, confirms the correctness of the information provided and approves the creation and publishing of the certificate according to agreement. At the same time, the applicant accepts the rules and terms pertaining to the use of the organisation certificate and sees to the storage of organisation certificates and PIN codes and the reporting of any misuse or lost certificates/microchip.

The PKI disclosure statement is part of the certification authority's terms of use related to the functionality of the public key system. Digital and Population Data Services Agency, which acts as the certification authority, publishes the PKI disclosure statement and makes it available to certificate applicants and parties trusting the certificate.

6.4 Certificate applicant

The certificate applicant can apply for a certificate for use in their name or possibly as a member of an organisation when signing documents for the organisation. This difference is described in this document when differentiation is necessary. However, a private person is always identified in a personal way when applying for a certificate.

The applicant organisation will apply for an organisation certificate for its members that are natural persons identified in a personal way.

7 Introduction to signature certificate policies

7.1 General points

The certificate policy refers to the principles that prove the suitability of a specific certificate for a specific organisation. The certificate policy also describes the commonly applied security requirements.

In this document, the procedure requirements are defined according to the certificate policies. These certificate policies apply to signature certificates conformant to the definitions of the Regulation.

Certificates issued in conformance with this document contain the OID of the certificate policy, with which parties trusting the certificate can determine the usability and reliability of the certificate for a specific use. This document defines the signature certificate policy, which is the signature certificate policy for signature certificates issued to the public and requires the use of secure signature creation tools.

In this document, the interpretation of the concept of the public is determined according to the national legislation applicable to the case. A certification authority can be deemed as one granting certificates to the public if the use of the certificates in question is not restricted by voluntary private-law agreements between the parties.

DPDSA draws up a separate certificate policy for each type of certificate issued by it, and a separate certification practice statement for each technical platform. The certificate policy contains a general description of the practices, terms and conditions, responsibility allocation and other matters related to certificate usage for each type of certificate. The certification practice statement contains a detailed description of the applicable practices.

The title of this certificate policy is the Certificate Policy for DPDSA's Organisation Certificate, OID 1.2.246.517.1.10.203.

This certificate policy refers to the certificate authority's certificate practice statement, OID 1.2.246.517.1.10.201.2.

Digital and Population Data Services Agency adheres to a certificate policy concerning signature certificates issued to the public as per trust services under Regulation No. (EU) 910/2014. The document reference as per ETSI EN 319 411-1 [2], QSCD is: OID: 0.4.0.194112.1.2. Signature certificates issued in accordance with this certificate policy can be used to authenticate digital signatures that correspond to approved certificates and creation devices for digital signatures as referred to in the Regulation and provided for in Articles 28 and 29 of the Regulation.

The certificate policy and the certification practice statement are available at www.fineid.fi.

This certificate policy has been registered by the Digital and Population Data Services Agency, a public authority which administers a personal information register and is responsible for providing certified electronic services in addition to its other tasks. DPDSA is responsible for the administration and updating of this certificate policy.

Questions regarding this certificate policy should be addressed to:

Digital and Population Data Services Agency

P.O. Box 123 (Lintulahdenkuja 2) Tel. +358 295 535 001

00531 Helsinki Fax. +358 9 876 4369

Business ID: 0245437-2 kirjaamo@dvv.fi

Questions pertaining to the certificate policy and communication pertaining to these documents are the responsibility of Digital and Population Data Services Agency's Certificate Administration branch.

Digital and Population Data Services Agency (DPDSA) Certificate Services

P.O. Box 123

FI-00531 Helsinki

www.fineid.fi

7.2 Unique identifiers

A signature certificate granted in conformance with this certificate policy meets the requirements of the Regulation on a signature certificate. The document reference as per ETSI EN 319 411-1 [2], QSCD is: OID: 0.4.0.194112.1.2.

This certificate policy is effective as of 1 Jan 2020.

The certification authority also includes the OID codes of the signature certificate policies it adheres to in the terms of use available to certificate applicants and parties trusting the certificate and, thus, indicates it adheres to the signature certificate policy in question.

7.3 User community and applicability

7.3.1 QCP-n-qscd signature certificate policy

Digital and Population Data Services Agency adheres to a certificate policy concerning signature certificates issued to the public as per trust services under Regulation No. (EU) 910/2014. The document reference as per ETSI EN 319 411-1 [2], QSCD is: OID: 0.4.0.194112.1.2. Signature certificates issued in accordance with this certificate policy can be used to authenticate electronic

signatures that correspond to approved certificates and creation devices for electronic signatures as referred to in the Regulation. The document reference as per ETSI EN 319 411-1 [2], clause 4.3.5. 3) QSCD is: OID: 0.4.0.194112.1.2.

Signature certificates issued in accordance with this certificate policy can be used to authenticate electronic signatures that meet the requirements for digital signature certificates and creation tools as provided for in Articles 28 and 29 of the Regulation.

7.4 Compliance

7.4.1 General points

The certification authority has the right to use the signature certificate policy's OID only if the certification authority indicates it adheres to the itemised signature certificate policy and, upon request, makes proof of compliance available to the subscriber and parties trusting the certificate.

The means for proving compliance may vary depending on the legislation of the certification authority's country of establishment. The certification authority's compliance is regularly reviewed and always when the certification authority's operations are significantly changed.

7.4.2 QCP-n-qscd signature certificate policy

A compliant certification authority must prove that

a) it meets the requirements set for it

b) it has implemented management means that meet all presented requirements

8 Obligations and responsibility and limitations of liability

The requirements of this section are applied to both signature certificate policies itemised in section 5, i.e., the QCP-n-qscd signature certificate policy, unless otherwise specified.

8.1 Certification authority's obligations

The certification authority ensures that all requirements set in section 7 on the certification authority, concerning the selected signature certificate policy, are met (see items 5.4.2, 5.4.3 and 8.4).

The certification authority is responsible for adhering to the procedures specified in the signature certificate policy even if the certification authority's operations were to be implemented by commission.

The certification authority offers all areas of the certificate service as described in its certification practice statement.

8.1.1 Certification authority's obligations

Digital and Population Data Services Agency has a statutory task of working as a certification authority.

The certification authority shall act in accordance with current legislation.

The certification authority shall perform its duties duly and reliably.

The certification authority has the necessary technical ability and financial resources for appropriately arranging the certificate activities and for covering potential liability for damages.

The certification authority is responsible for all areas of the certification activity, including the reliability and functioning of services and products produced by any technical suppliers or persons who assist the certification authority, such as registration authorities and card manufacturers.

The certification authority draws up and maintains a certificate policy which describes at a general level the procedures for the issuance, maintenance and management of organisation certificates, the terms and conditions, the allocation of responsibilities, and other matters related to the use of organisation certificates.

The certification authority draws up and maintains certification practice statements which describe how the certification authority applies its certificate policy.

The certification authority complies with its certificate policy and certification practice statement.

The certification authority makes the certificate policy and the certification practice statement publicly available.

The certification authority shall employ sufficient staff with the expertise, experience and competence required for producing certificate services.

The certification authority shall use reliable systems and products protected against unauthorised use.

The certification authority shall keep information regarding the organisation certificate and certificate activities publicly available, based on which the operations and reliability of the certification authority can be assessed.

The certification authority ensures the confidentiality of signature creation data.

The certification authority will not store or copy any signature creation data provided to a signatory.

8.1.2 The registration authority’s obligations

The registration authority works at the responsibility and on behalf of the certification authority and adheres to the procedures related to registration agreed with the certification authority.

The registration authority shall comply with the certificate policy and the certification practice statement in its registration activities.

The registration authority identifies the certificate applicant personally and reliably in a way described in the certification practice statement and so that the applicant's identity and other information pertaining to the applicant's person needed in the granting of the certificate will carefully be inspected.

The registration authority shall see to the careful handling and confidentiality of personal data.

The registration authority shall provide the certificate applicant with data of the terms of use of the certificate.

8.2 Certificate applicant's obligations

The certification authority obliges the certificate applicant with an agreement to adhere to all obligations specified below.

The purpose of the organisation certificate granted by Digital and Population Data Services Agency is specified in the certificate policy and certification practice statement of each certificate type and in the certificate holder's instructions. The certificate may only be used in accordance with its intended use for digital signing, authentication or encryption.

The holder of an organisation certificate sees to it that the data stated when applying for organisation certificates are correct.

The holder of an organisation certificate is liable for the use of the organisation certificate, legal actions taken with it and their financial consequences. With respect to a signature certificate, the provisions of the Regulation and the Act on Strong Electronic Identification and Trust Services apply.

The holder of an organisation certificate shall store its private keys contained on a microchip and the PIN code required for using them separately from each other and aim to prevent the loss, access by third parties, alteration or unauthorised use of the private keys. Transferring the microchip or disclosing the PIN code to a third party, for example by lending, releases the certificate authority and the party trusting the organisation certificate from any liability arising out of the use of the organisation certificate.

The organisation certificate must be handled and protected with the same care as other corresponding microchips, cards or documents, such as credit cards, driving licence or passport. Personal PIN codes must be stored physically in a different location than the microchip containing the organisation certificate and private keys.

The loss or suspected misuse of the microchip and card must be reported without delay to the certification authority by calling the free-of-charge revoking service at +358 800 162 622.

8.3 Communication to parties trusting a certificate

Instructions made available to parties trusting the certificate must state that trusting the certificate justifiably requires that the party

Organisation electronic identification certificates are published in a generally (if not agreed otherwise) available in public directory, and revoked organisation certificates on a revocation list where a party trusting the certificate must check its validity. The electronic signature certificates are not published in the public directory. The certification authority provides an online certificate status check service that implements OCSP.

It is the obligation of the party trusting a certificate to ensure that the certificate is used according to its intended use. The intended use of a signature certificate is electronic signing. The intended use of an authentication and encryption certificate is the authentication of a person and encryption of data.

A party trusting the certificate must adhere to the certificate policy and certification practice statement.

A party trusting an organisation certificate may bona fide trust an organisation certificate after verifying that **the organisation certificate is valid and is not contained on a revocation list.** A party trusting an organisation certificate shall check the certificates on the revocation list. The certification authority provides an online certificate status check service that implements OCSP. In order to reliably verify the validity of an organisation certificate, the trusting party must comply with the following procedure for revocation list checks.

If a party trusting an organisation certificate copies the revocation list from a directory, it must verify the genuineness of the revocation list by checking the digital signature of the revocation list's certification authority. In addition, the validity period of the revocation list must be checked. The certification authority provides an online certificate status check service that implements OCSP.

If the most recent revocation list cannot be obtained from the directory because of hardware or directory service malfunction, the organisation certificate must not be accepted if the validity period of the last obtained revocation list has expired. All approvals of an organisation certificate after the validity period take place at the risk of the party trusting the organisation certificate.

8.4 Liability

Certification authorities that issue signature certificates to the public are bound by liability set forth in the Regulation and in the Act on Strong Electronic Identification and Trust Services. Service providers providing a strong electronic identification tool or service are bound by liability set forth in the Act on Strong Electronic Identification and Trust Services.

8.4.1 Certification authority's liabilities

Digital and Population Data Services Agency as a certification authority is liable for the safety of the entire certificate system. The certification authority is liable for services it has commissioned as if for its own.

Digital and Population Data Services Agency is responsible for the organisation certificate having been created with adherence to the procedures prescribed in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency, the Act on Strong Electronic Identification and Trust Services, the Act on Electronic Services and Communication in the Public Sector, the certificate policy and the certification practice

statement and according to the data provided by the applicant of the certificate. Digital and Population Data Services Agency is liable only for the data it has stored in the organisation certificate.

Digital and Population Data Services Agency is liable for the usability of the organisation certificate, when used appropriately, throughout its validity period, unless it has been placed on a revocation list. The organisation certificate has been given to a person identified in a manner required for organisation certificates. The certificate holder has been given instructions pertaining to the use of the organisation certificate prior to the signing of the agreement.

When signing an organisation certificate with its private key, the certification authority assures it has checked the personal data in the organisation certificate according to the policies described in the certificate policy and the certification practice statement.

The certification authority is responsible for including the right person's organisation certificate on the revocation list and that it appears on the revocation list in the time specified in this certificate policy.

8.4.2 Registration authority's liabilities

The registration authority of an organisation certificate is a point of registration that registers the certificate on behalf of and at the risk of Digital and Population Data Services Agency, which acts as the applicant's certification authority. With respect to the registration, the requirements of the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency and the Act on Strong Electronic Identification and Trust Services.

8.4.3 Responsibilities of an organisation certificate holder

An organisation certificate is the electronic identity of its holder and may not be given for another person to use.

The holder of an organisation certificate is liable for its use, legal actions taken with it and their financial consequences.

Leaving a card containing a microchip in a reader may enable the abuse of the organisation certificate. When terminating a terminal session or leaving a terminal device unsupervised, it is the responsibility of the organisation certificate holder to remove the microchip containing the organisation certificate from the reader device and close the applications used appropriately or otherwise closing the technical connection needed for the use of the organisation certificate.

The responsibility of an organisation certificate holder ends when they have reported the necessary data to the revocation service for revoking the certificate and when they have received a revocation notice from the official receiving the call. In order to terminate liability, the revocation request must be made immediately upon noticing the reason for the request.

8.4.4 Liabilities of a party trusting an organisation certificate

A party trusting an organisation certificate cannot bona fide trust it and the correctness of the digital signature if the validity of the organisation certificate has not been checked on the revocation list. The certification authority provides an online certificate status check service that implements OCSP. Accepting an organisation certificate in the above cases releases Digital and Population Data Services Agency of liability. A party trusting an organisation certificate shall verify that the certificate granted corresponds to its intended use in the legal action in which it is used.

8.4.5 Limitations of liability

Digital and Population Data Services Agency is not liable for damage caused by the disclosure of PIN codes, a PUK code and an organisation certificate holder's private keys unless said disclosure is the direct result of Digital and Population Data Services Agency's direct actions.

The maximum extent of Digital and Population Data Services Agency's liability to the certificate holder and a party trusting the certificate is for direct damage incurred, if the damage is the result of Digital and Population Data Services Agency's direct actions, however at most 15% of the amount of certificate invoicing for the preceding 3 months (share payable to DPDSA).

Digital and Population Data Services Agency is not liable for indirect or consequential damage caused to the organisation certificate holder. Neither is Digital and Population Data Services Agency liable for the indirect or consequential damage incurred by a party trusting an organisation certificate or by another contractual partner of the certificate holder.

Digital and Population Data Services Agency is not responsible for the operation of public telecommunication connections, such as the Internet, or for the inability to execute a legal transaction because of the non-functionality of a device or software used by the organisation certificate holder or for the use of a certificate in contradiction to its intended use.

The certification authority has the right to interrupt the service for changes or maintenance. Changes to or maintenance of the revocation list will be announced in advance.

The certification authority has the right to further develop the certificate service. An organisation certificate holder or a party trusting an organisation certificate must bear their own expenses thus incurred, and the certification authority is not liable to compensate the organisation certificate holder or a party trusting the organisation certificate for any expenses caused by the certification authority's development work.

The certification authority is not liable for errors in the online service or applications intended for citizens and organisations and based on a certificate or any resulting expenses.

8.4.6 Other parties

A party trusting an organisation certificate may trust the correctness of the digital signature of an organisation certificate if they have verified that the organisation certificate has not been included in a revocation list, the validity of the certificate has not expired and the party has no other justifiable reason to doubt the correctness of the use of the certificate.

The certification authority is responsible for the organisation certificate in accordance with the certification authority's commitments in this certificate policy and the certification practice statement on organisation certificates.

Digital and Population Data Services Agency's liability for damages related to the production of certificate services is determined according to the service agreement concluded with the certificate applicant. Digital and Population Data Services Agency is bound by the certification authority's liability for damages conformant to the Act on Strong Electronic Identification and Trust Services. Where applicable, the Tort Liability Act (412/1974) also applies.

The maximum extent of Digital and Population Data Services Agency's liability to the certificate holder and a party trusting the certificate is for direct damage incurred, if the damage is the result of Digital and Population Data Services Agency's direct actions, however at most 15% of the amount of certificate invoicing for the preceding 3 months (share payable to DPDSA).

9 Requirements on the actions of the certification authority

This section is applied to a uniquely identified signature certificate policy QCP-n-qscd signature policy unless otherwise specified.

The certification authority implements the management means, meeting the following requirements.

This document applies to Digital and Population Data Services Agency, which serves as a certification authority that issues signature certificates. The implementation of the service described in this document includes the provision of registration services, creation of certificates, distribution of certificates, certificate revocation management and communication on the revocation list. If the requirement is related to a specific area of service of the certification authority, it is described under the corresponding headings. If the area of service is not itemised below or if "certification authority in general" is mentioned, the requirement applies to the certification authority's general operations.

The purpose of these procedure requirements is not to restrict the certification authority's charging for the services.

The requirements presented apply to the security objectives and the administrative means available for attaining them, for which detailed requirements are presented, if deemed necessary for meeting the objectives.

9.1 Certification practice statement

The certification authority ensures that it proves the reliability required by the provision of certificate services as described in the Regulation.

A detailed description pertaining to the measures described in this document is contained in the certification practice statement for each certificate type and storage platform.

01/01/2020

9.2 Life cycle management of keys used in a public key system

9.2.1 Creation of certification authority's keys

Creation of certificates

The certification authority ensures that the certification authority's keys are created under secure conditions described in the Regulation.

In particular:

a) The certification authority's keys are created in a physically secure environment (section 7.4.4) and the creation is implemented by staff working in trusted roles (section 7.4.3) under supervision distributed to at least two different people. The number of staff authorised for this task is kept as small as possible and in accordance with the certification authority's policies.

b) The certification authority's keys are created with a tool that

– meets the requirements itemised in publication FIPS 140-2 at level 3 at least, or

– meets the requirements itemised in one of the following CEN workshop agreements (CWA): CEN Workshop Agreement 14167-2, CWA 14167-3 or CWA 14167-4, or

– is a reliable system whose evaluation assurance level, according to the ISO/IEC 15408 standard, is at least EAL 4 or that meets the corresponding security profile conditions. The system's own security target or protection profile must conform to the requirements of this document, be based on a risk analysis and contain both physical and non-technical security measures.

The rules of items b–e in section 7.2.2 are applied to key generation also when it is done in a separate system.

c) The generation of the certification authority's keys uses an algorithm deemed suitable for signature certificates.

d) The certification authority's signature key length and algorithm combination is set such as has been deemed suitable for signature certificates of the type the certification authority issues.

The specifications regarding the algorithms and their parameters have been published in document TS 102 176-1.

At an appropriate time prior to the expiration of the certification authority's signature key (for example, at the time stated in the certification authority's certificate), the certification authority creates a new key pair for signing the certificate and carries out all necessary measures so that the activities of organisations that may trust the key of the certification authority in question would not be disturbed. A new certification authority's key is created and its distribution is carried out according to these procedures.

These measures are taken sufficiently early so that all parties with a relationship to the certification authority (signers, certificate applicants, parties trusting the certificate, higher-level certification authorities) will receive information of the changed key pair sufficiently early so that they could implement measures necessary for undisturbed operations. This does not apply to a certification authority that discontinues its operations before the last date of validity of the certificate of its own certification authority.

9.2.2 Storage, backup and recovery of the certification authority's key

Creation of certificates

The certification authority ensures that the confidentiality and integrity of the certification authority's private keys are retained in accordance with the Regulation.

Digital and Population Data Services Agency generates its private signature keys and the public keys corresponding to the private signature keys.

The certification authority's private keys are stored in hardware security modules administered by the certification authority, meeting the requirements of the security standard.

The certification authority sees to it that the certification authority's private keys are protected against disclosure and unauthorised use. A backup is made of the certification authority's private keys in a manner conformant with critical information security.

The environment required for the generation and use of the private key requires the simultaneous presence of or activation of operation by at least two persons.

No copies are made of the private keys in Digital and Population Data Services Agency's organisation certificate.

9.2.3 Distribution of the certification authority's public key

Creation and distribution of certificates

The certification authority ensures that the integrity and authenticity of the certification authority's (public) key and the related parameters used for authenticating the signature are retained in accordance with the Regulation while distributing to the parties trusting the certificate.

In connection with the creation of the organisation certificate, a certificate generation request is created using the microchip's public keys, combining the certificate applicant's registration data with the public key in question.

The organisation certification authority's public key is part of the certification authority's certificate. The organisation certificate contains the public key of the certificate holder.

The certification authority's certificate is available in a public directory. If an organisation certificate is located on an ID card, the certification authority's certificate is also placed on the microchip of the ID card.

The certification authority's certificate contains the certification authority's public key. The certification authority's certificate is stored in a public directory. The certificate holder's certificate is

also stored in a public directory or otherwise made available in accordance with an agreement concluded with the client organisation. The certification authority's certificate is available in the certification authority's public directory and the certification authority's website.

The certification authority archives all public keys it has certified.

9.2.4 Backup key system

No copies are made of the private keys in Digital and Population Data Services Agency's organisation certificate.

9.2.5 Use of the certification authority's key

The certification authority is responsible for its private signature keys being used only according to their intended use. In particular:

Creation of certificates

a) The certification authority's signature keys conformant to section 7.3.3, used for creating certificates may also be used for signing other types of certificates and revocation state data, as long as the procedure requirements pertaining to the certification authority's operating environment conformant to sections 7.2.1–7.2.3, 7.2.5–7.2.7 and 7.4 are adhered to.

b) The certificate signature keys may only be used on physically secure premises.

CA certificate:

Purpose: Signing of certificates and revocation lists. The technical description is in the FINEID S2 specifications.

9.2.6 End of the certification authority key's life cycle

The certification authority ensures that the certification authority's private signature keys are not used after the end of their life cycle in accordance with the Regulation.

9.2.7 Life cycle management of the encryption hardware used in signing certificates

The certification authority ensures the security of the encryption hardware throughout its life cycle according to the Regulation.

9.2.8 Signer key management services provided by the certification authority

The certification authority ensures that all signature keys it creates are created securely and that the confidentiality of the signer's private key is secured in accordance with the Regulation.

The certification authority's private key, which is used to sign organisation certificates, and the corresponding public key are 4096-bit RSA keys.

The organisation certificate holder's private and public keys are 2048-bit RSA keys at minimum.

The field that determines the intended use in the certificate's content specifies the intended use of the key pertaining to the certificates. The use of the key is limited only to its stated intended use.

CA certificate:

Purpose: Signing of certificates and revocation lists. The technical description is in the FINEID S2 specifications.

Certificate holder's authentication and encryption certificate:

Purpose: Electronic identification or data encryption.

Certificate holder's signature certificate:

Purpose: Digital signature

9.2.9 Manufacturing of a secure signature creation device

If the certification authority issues qualified signature creation devices (QSCD), the certification authority must ensure its secure implementation in accordance with the Regulation.

Separateness can be attained by ensuring that the distribution of the activation data and the delivery of the qualified signature creation device take place at different times or through different routes.

The above requirements concerning the manufacture of a qualified signature creation device can be met by implementing an applicable protection profile, which is defined according to the standard ISO/IEC 15408 or in a corresponding way.

9.3 Life cycle management of certificates used in a public key system

9.3.1 Signer registration

The certification authority ensures that the signers are identified and authenticated appropriately and that the signer's certificate requests are faultless, correct and based on the appropriate authorisation in accordance with the Regulation.

The rights and obligations of a certificate applicant are specified in the contract document and general terms and conditions, which comprise an agreement concluded with the certificate applicant.

The application document and terms and conditions of use clearly state that the applicant for organisation certificate, with his/her signature, confirms the correctness of the information provided and approves the creation of the organisation certificate and its publication according to agreement with the client organisation or in a public directory. At the same time, the applicant accepts the rules and terms pertaining to the use of the organisation certificate and sees to the storage of organisation certificates and PIN codes and the reporting of any misuse or lost cards.

The organisation certificate applicant is responsible for the correctness of all material data that the applicant has given the certification authority or registration authority. The organisation certificate holder must use the organisation certificate only for its intended uses.

When a certification authority grants an organisation certificate, it also approves the application for certificate.

When granting an organisation certificate, the certification authority is responsible for its data content being correct at the time of delivery of the certificate.

The data in an organisation certificate unambiguously determine the organisation certificate holder. The certification authority will determine the official identity of the certificate applicant, if necessary.

Private keys pertaining to an organisation certificate, created on a microchip or other secure environment, are delivered to the organisation certificate applicant in connection with delivery.

It is the responsibility of the organisation certificate holder to prevent the use of private keys and the related PIN codes belonging to him/her in a way contradictory to the terms of use and to take care of them as set forth in the terms of use.

The certificate holder must immediately notify the revocation service if he/she suspects that his/her organisation certificate may have been used in breach of the terms and conditions.

The certification authority's public key is part of the certification authority's certificate. The certification authority's certificate is available in a public directory. If an organisation certificate is located on an ID card, the certification authority's certificate is also placed on the microchip of the ID card.

At the time of handing out the organisation certificate, it is emphasised to the certificate applicant that there are no copies of the private keys and no copies can be made later.

An organisation certificate can be picked up personally at a registration point.

They key pair for a Digital and Population Data Services Agency organisation certificate is created in a secure facility. The public key is used for creating the certificate, and the private key is stored on a microchip protected against reading and writing.

The card manufacturer creates activation data, i.e., PIN codes, that enables the use of the keys.

PIN codes are protected so that they cannot be read or copied from the card. It is the certificate holder's responsibility to protect the use of his/her keys by taking care of his/her microchip or card and PIN codes as described in the instructions for use.

To guarantee security, the PIN and PUK codes needed for the use of the organisation certificate are handled so that they are not in the same place at the same time before or during delivery to the certificate applicant.

A holder of an organisation certificate may download card reader software from the Digital and Population Data Services Agency website to use the organisation certificate in electronic services.

It is explained to the holder of an organisation certificate that he/she has the possibility to change the original PIN codes to new ones. The program for changing the codes is available free of charge for cardholders at www.fineid.fi.

The organisation certificate applicant may store the e-mail address in the organisation certificate and the population information system at their discretion. The e-mail address is marked in the organisation certificate and the population information system as stated by the applicant. The e-mail address stored in the organisation certificate is stored in the public directory, in the same conditions as the rest of the data content in the organisation certificate. The e-mail address cannot be changed during the validity of the organisation certificate.

For the identification of the person, the smart card may contain a visible photo and sample signature.

The holder of an organisation certificate may have the certificate revoked before the expiration of the organisation certificate's validity period.

Revocation requests are primarily made by the organisation's representative or certificate holder upon discovering that a certificate has been lost or it may have been misused. Requests can also be made by e.g. the card manufacturer or the registration authority.

The revocation request must be made immediately upon suspecting the misuse of a certificate, for example because of loss or theft. Organisation certificates can be revoked by calling the free revocation service at +358 800 162 622. All revocation requests, reasons for revocation, the method of identifying the requester, and the CA's response to the request are archived.

The revocation of a certificate is described in detail in the certification practice statement.

10 Operational requirements

10.1 Applying for a certificate

The rights and obligations of a certificate applicant are specified in contract documents and general instructions for use, which comprise an agreement concluded with the certificate applicant. The application document contains the details of the rights and obligations of both parties. When an applicant for an organisation certificate applies for an organisation certificate, he/she also accepts the general terms of use.

The application document and instructions for use clearly state that the applicant for organisation certificate, with his/her signature, approves the correctness of the information provided and the creation of the certificate and its publication according to agreement with the client organisation or in a public directory. At the same time, the applicant accepts the rules and terms pertaining to the use of the organisation certificate and sees to the storage of organisation certificates and PIN codes and the reporting of any misuse or lost certificates/microchip.

10.2 Granting of a certificate

The certification authority grants an organisation certificate upon accepting the application for certificate. When granting an organisation certificate, the certification authority is responsible for its data content being correct at the time of delivery of the certificate.

10.3 Receiving a certificate

The organisation certificate is retrieved personally from the point of registration.

At the time of handing out the certificate, it is emphasised to the certificate applicant that there are no copies of the private signature keys and no copies can be made later.

10.4 Termination and interruption of the validity of a certificate

Prerequisites for revoking a certificate

An organisation certificate must be included in a revocation list when there is reason to suspect misuse, for example because of loss or theft. Organisation certificates can be revoked by calling the free revocation service. The revocation request must be made immediately upon suspicion of potential misuse.

Requester of revocation

Certificate revocation requests are primarily made by the certificate holder or the organisation's contact person. If the caller is not the holder of the certificate being revoked, both the caller and the certificate holder must be identified.

Revocation requests can also be made by the card manufacturer or registration authority. The method of identifying the person requesting the revocation is recorded.

The reasons for revocation, the date and time, and the request handler's details are recorded.

Renewing a certificate, changing the key pair and updating a certificate

The public keys in organisation certificates and the private keys in the microchip cannot be renewed. The creation of new key pairs requires a new organisation certificate.

The renewal of the organisation certificate adheres to the same procedures as when applying for the certificate for the first time.

10.5 Creation of certificates

The certification authority ensures that it grants certificates securely in order to retain its authenticity in accordance with the Regulation.

The private keys of organisation certificate holders are created securely in a way that meets the requirements for a signature certificate. Key pairs generated by the certificate holder are not accepted. No copies are made of the private keys during creation and they cannot be transferred or copied from the microchip. The certification authority and the card manufacturer do not have access to the private keys of the certificate holders.

When the keys are generated, they have not been allocated to any person.

The certification authority's private keys and their backups are stored with strong encryption in devices that meet the requirements of critical information security.

No copies exist of the private keys of the certificate holder.

The certification authority's private keys are stored in hardware security modules administered by the certification authority.

The certification authority's private signature keys are protected with physical and logical security measures of high reliability. They are used only in a system placed in a secure environment.

10.6 Distribution of terms of use

The certification authority ensures that the terms of use and instructions are made available to the subscribers and the parties trusting certificates in accordance with the Regulation.

A signature certificate granted in conformance with this certificate policy meets the requirements of the Regulation on a signature certificate.

The data can be delivered as part of an agreement with a subscriber or a party trusting a certificate. The terms of use can be included in the certification practice statement so that the reader can easily detect and identify them.

With respect to terms of agreement pertaining to certificates granted to the public, the requirements of consumer legislation, including the directive on unreasonable terms in consumer agreements, 93/13/EEC, are taken into account.

A holder of an organisation certificate may download card reader software from the Digital and Population Data Services Agency website to use the organisation certificate in electronic services.

Organisation certificates are applied for according to the description of the certification practice statement.

The price of acquiring an electronic ID card is determined according to the then-valid Decree of the Ministry of Finance on the payment of Digital and Population Data Services Agency fees.

The prices of organisation certificates stored on other microchips are determined according to DPDSA's current list prices for commercial services.

The certification authority does not separately charge the organisation certificate holder for the use of the organisation certificates, the revocation service or a public directory. Individual online service providers may charge for the use of their services. The use of an organisation certificate does not require a specific announcement or permit from the certification authority.

Reporting an organisation certificate to a revocation list is free of charge. Retrieving revocation lists from the directory and checking the validity of organisation certificates against the revocation list are also free of charge.

The use of advisory services is subject to a separate fee according to the then-valid price list.

If the service provider wishes to arrange for information maintenance service between the unique identifier of the organisation certificates and the identifiers of its own background system or between other updated data, the service provider may apply for information disclosure permission in the information service from Digital and Population Data Services Agency. This service will be priced according to the then-valid Act on Criteria for Charges Payable to the State and the Decree of the Ministry of Finance on the payment of Digital and Population Data Services Agency fees.

Instructions and terms of use for using an organisation certificate are provided for certificate applicants to read before an agreement on the certificate is concluded or the decision to issue one is made. The information is available at both the point of registration and at Digital and Population Data Services Agency's website.

10.7 Distribution of certificates

The certification authority ensures that certificates are appropriately made available to the subscribers, signers and the parties trusting certificates in accordance with the Regulation.

The data content of the root certificate, certification authority certificate and certificate holder's certificates is described in the document FINEID S2. The document is available at the certification authority's website at www.fineid.fi.

The certification authority publishes all of the certification authority's organisation certificates and revocation lists in a non-chargeable, publicly available, public directory. The certification authority publishes the certificate policy, the certification practice statements, the PKI disclosure statement (PDS) and other public documents pertaining to the production of certificate services on its website.

Each organisation certificate is delivered as agreed or published in the public directory immediately upon its creation and remains in said directory for as long as it remains valid. The certification authority publishes a revocation list that is valid for two hours from its publication. This revocation list is updated once per hour with a new one.

Directory and revocation list data are publicly available. The FINEID specifications published by the certification authority are available on the certification authority's website. In addition, the certificate policies and certification practice statements are available on the certification authority's website.

10.8 Revoking a certificate and placing it in the suspended state

The certification authority ensures that certificates are revoked at the right time based on authorised and confirmed certificate revocation requests and in conformance with the Regulation.

The validity of an organisation certificate is at most five years. The holder of an organisation certificate may have the certificate revoked before the expiration of the organisation certificate's validity period.

Certified signatures created before the revocation or expiry of the certificate can still be authenticated after the revocation or expiry from the signature certificate.

Revocation requests are primarily made by the organisation's representative or certificate holder upon discovering that a certificate has been lost or it may have been misused. Requests can also be made by e.g. the card manufacturer or the registration authority.
The revocation request must be made immediately when suspecting use in violation of the terms of contract or the misuse of a certificate, for example because of loss or theft. Organisation certificates can be revoked by calling the free revocation service at +358 800 162 622. All revocation requests, reasons for revocation, the method of identifying the requester, and the CA's response to the request are archived.

It is the certificate holder's responsibility to protect the use of their private keys by taking care of their microchip or card and PIN codes as described in the instructions for use. The certificate holder must immediately notify the revocation service if he/she suspects that his/her certificate(s) may have been used in breach of the terms and conditions.

All revocation requests, reasons for revocation, the method of identifying the requester, and the CA's response to the request are archived. Calls concerning revocation requests are recorded.

The revocation request for an organisation certificate is primarily made by its holder. If the caller is not the holder of the certificate being revoked, both the caller and the certificate holder must be identified.

Revocation requests can also be made by the certification authority, card manufacturer or registration authority. The method of identifying the person requesting the revocation is recorded.

The reasons for revocation, the date and time, and the request handler's details are recorded.

The revocation request can be made in the following ways:

a) By calling the revocation service

b) By visiting the registration authority

10.9 Publishing frequency of the revocation list

Information of the inclusion of a certificate on a revocation list will be publicly available within an hour of the revocation request having been deemed valid and approved. The revocation list is valid for two hours.

The revocation list contains the time of publication of the next revocation list.

The new revocation list will be published by the expiration of the validity of the valid revocation list.

In case of system updates and other exceptional situations, DPDSA may publish revocation lists at a different frequency and extended validity periods.

The certification authority provides an online certificate status check service that implements OCSP. The certification authority publishes a revocation list of revoked certificates.

Closing certificates at the request of Digital and Population Data Services Agency

Digital and Population Data Services Agency will always revoke certificates when it has received information of the death of the certificate holder. Digital and Population Data Services Agency will notify the beneficiary of the deceased certificate holder of the revocation.

The Digital and Population Data Services Agency will revoke a certificate issued by it if an error is found in its data content.

Digital and Population Data Services Agency may revoke certificates signed with its private key if there is reason to believe that Digital and Population Data Services Agency's private keys have become disclosed or accessed by unauthorised parties.

All certificates that are valid and have been granted with the exposed key must be closed on one or several revocation lists whose validity period does not expire until the validity of the last revoked certificate has expired.

If the private key used by the Digital and Population Data Services Agency in certificate creation or another technical method has become exposed or otherwise unusable, the Digital and Population Data Services Agency must duly notify all cardholders and the Finnish Transport and Communications Agency of the event.

Digital and Population Data Services Agency may also revoke a certificate for other special reasons.

Certificates are revoked immediately in connection with a revocation request.

10.10 Renewing a key pair after inclusion on revocation list

The public keys in organisation certificates and the private keys in the microchip cannot be renewed. Revoked organisation certificates cannot be reinstated.

The creation of new key pairs requires applying for a new organisation certificate.

The renewal of the organisation certificate adheres to the same procedures as when applying for the certificate for the first time.

An organisation certificate cannot be temporarily suspended unless such a procedure has been specifically agreed upon between Digital and Population Data Services Agency and the client organisation.

The data content of the revocation lists published by the certification authority is described in the document FINEID S2. The document is available at the certification authority's website at www.fineid.fi.

It is the certificate holder's responsibility to protect the use of their private keys by taking care of their microchip or card and PIN codes as described in the instructions for use. The certificate holder must immediately notify the revocation service if he/she suspects that his/her certificate(s) may have been used in breach of the terms and conditions.

10.11 The certification authority's management and operating procedures

10.11.1 Security management

The certification authority ensures that it adheres to appropriate administrative and business management practice, conformant to recognised standards, in accordance with the Regulation.

The certification authority ensures that information security is retained if the certification authority obtains services from another organisation or entity.

10.11.2 Repository classification and management

The certification authority ensures that the protection level of its repositories and data is appropriate in conformance with the Regulation.

The information published by Digital and Population Data Services Agency is available on the certification authority's website. Confidential data used in the certificate system are stored in the CA's own confidential repository. The certification authority's data are archived according to the valid archiving rules. Special attention is paid to the handling of personal information, and DPDSA has published a specific set of procedures for the provision of certificate services in accordance with the Personal Data Act. The certification authority has also prepared the certificate system's register description conformant to the Personal Data Act with respect to the processing of personal data.

The data in the certificate system are confidential unless they are based on the regulations on information disclosure set forth in the Personal Data Act, the Act on the Openness of Government Activities, the Act on the Digital and Population Data Services Agency (304/2019), the Act on Strong Electronic Identification and Electronic Trust Services or for purposes set forth in the certificate policy or certification practice statement.

The data of the public directory and the revocation list are public, as are the certification practice statements and the data specified in the certificate policy and the published FINEID specifications.

The validity period of an organisation certificate is indicated in the organisation certificate. Organisation certificates revoked during their validity period are published on a publicly available revocation list.

The data disclosed to authorities are specified according to the valid legislation.

The data of the certificate system are not disclosed for purposes other than those listed above in this document.

The holder of a certificate has the right to receive information pertaining to him/her, for example personal data, in accordance with the applicable legislation.

It is material for the reliability of the certification authority that Digital and Population Data Services Agency take all measures to see to the secrecy of confidential material it obtains in connection with the certificate activities and to the good administration of data unless otherwise required by legislation pertaining to the right of authorities to obtain information on the operation of the certificate system.

Digital and Population Data Services Agency conforms to the Personal Data Act and specific legislation in the processing of personal data. Digital and Population Data Services Agency has prepared the policy rules for the processing of personal data in connection with information disclosure and with the certificate activities. Special care must be taken when processing personal data.

The certificate services produced by Digital and Population Data Services Agency are covered by a financial administration system and supervision as has separately been set forth. The implementation of the certification authority's financial administration is described in detail in the certification practice statement.

The detailed requirements are described in the ISO/IEC 17799 standard.

10.11.3 Staff and information security

The certification authority ensures that the staff and recruitment policies promote and support the reliability of the certification authority's operations in conformance with the Regulation.

Digital and Population Data Services Agency serves as the certification authority that is responsible for certificate activities. The selection of technical service providers is based on a bidding procedure related to public procurements, and the providers work at Digital and Population Data Services Agency's responsibility and on behalf of it.

Digital and Population Data Services Agency pays particular attention to the reliability of both its own staff and the technical service vendors and registration authorities and to their skills needed for the execution of the tasks.

Digital and Population Data Services Agency has a basic security clearance done for its staff and the persons of the technical vendors who work with the certificate environment.

The staff's work experience is surveyed when starting the employment. A security clearance is carried out for the person based on the information he/she has provided on a fixed-form form.

The security clearance procedure is described in detail in the certification practice statement.

The training of Digital and Population Data Services Agency's staff is planned and implemented so that duties can be carried out in the best possible way. Digital and Population Data Services Agency has a training plan whose implementation is the responsibility of Digital and Population Data Services Agency's Administration and Management Support unit.

When task rotation is planned for the certification authority's tasks, they are organised in such a way that the person can see to his/her new duties in the best possible way. The implementation of task rotation must also take into account the retention of good information administration practice and the maintenance of sufficient task-specific skill levels.

Task rotation also adheres to Digital and Population Data Services Agency's information security policy and information security plan as well as Digital and Population Data Services Agency's other general instructions.

Digital and Population Data Services Agency's staff work subject to official liability and in accordance with the internal instructions of Digital and Population Data Services Agency. The position of a public official is set forth in the State Officials Act (750/1994).

When recruiting staff, it must be seen to that the staff's skills correspond to the requirements of the task and that there is nothing detected in the person's background check that would put the person's interests at odds with the production of certificate services.

The staff always has access to Digital and Population Data Services Agency's quality and security documents.

10.11.4 Physical and environment security

The certification authority must ensure that physical address to critical services is monitored and that physical risks pertaining to the repositories are minimised in accordance with the Regulation.

An information security certificate has been granted to Digital and Population Data Services Agency, affirming that DPDSA's information security meets the requirements of the ISO/IEC 27001 standard. Digital and Population Data Services Agency uses technical service vendors for carrying out the information technology tasks of the certificate service. DPDSA is responsible, as the certification authority, for the safety and operation of certificate production in an appropriate way in all of its sub-areas.

The certification authority's systems are located in high-security data centres and meet the instructions and orders imposed on data centres regarding security.

Facility safety has been implemented in such a way that access to the facilities by unauthorised parties is prevented.

Facilities where production duties for the certificate system are carried out have controlled physical access. The access control system detects authorised and unauthorised entry. Access to data centre facilities requires the identification of the person, whereby the person is identified and the access right is verified and the transactions are registered. Data centre facilities are guarded at all times of the day.

The hardware solutions have been implemented according to good information administration practice in such a way that in the event of system failure, a backup system can be used without compromising the confidentiality, integrity or availability of the data contained in the system.

The supply and maintenance of spare parts for devices critical for operations has been ensured.

The creation, activation, backup and recovery of the certification authority's private key are carried out under supervision when two persons authorised to carry out maintenance on the system are present.

The revocation of the certification authority's private key is possible only under the supervision of two authorised persons.

At least two persons authorised to carry out maintenance on the system are present when the certification authority's private key's hardware security module is initialised.

The use of the system requires the presence of at least one person authorised to do so.

The registration of an organisation certificate and identification of the applicant requires the presence of one person.

The identification of the registration administrator for organisation certificates, certificate system administrator and certificate system user and task descriptions are described in detail in the certification practice statement.

10.11.5 Operations management

The certification authority must ensure that the certification authority's systems are safe and used appropriately, minimising risk for operational anomalies, in accordance with the Regulation.

Digital and Population Data Services Agency uses technical service vendors for the registration and information technology duties of certificate production. Digital and Population Data Services Agency serves as the certification authority that is responsible for certificate activities.

The duties of the certification authority are divided into areas of responsibility by duty, described in detail in the certification practice statement.

01/01/2020

The party responsible for the certification authority's security manages these areas of responsibility but, in practical operations, the operating staff implements the appropriate security procedure under supervision and in accordance with documents that define roles and responsibilities.

Digital and Population Data Services Agency audits the facilities, devices and operations of its technical suppliers in an appropriate fashion.

Digital and Population Data Services Agency's information security audit is carried out by Digital and Population Data Services Agency's Head of Information Management or an external auditor specialised in auditing technical vendors pertaining to certificate services.

An information security certificate has been granted to Digital and Population Data Services Agency, affirming that DPDSA's information security meets the requirements of the ISO/IEC 27001 standard.

The objects of the audit are determined by the Act on Strong Electronic Identification and Trust Services or, if Digital and Population Data Services Agency is carrying out the audit, the information security standard ISO/IEC 27001, Digital and Population Data Services Agency's information security policy or the technical terms of delivery.

The audit is carried out considering the implementation of the eight areas of information security. Audited information security properties include confidentiality, integrity and availability.

The audit compares the policy, certification practice statement and application instructions to the operation of the entire certificate organisation and system. Digital and Population Data Services Agency ensures that the application instructions are consistent with the certificate policy.

The audits will consider administrative information security and also service providers.

Observed deviations are recorded in the audit report and reacted to in accordance with legislation, the information security standard ISO/IEC 27001 and the valid terms of delivery.

The results of an audit are communicated according to the law, the information security standard ISO/IEC 27001, Digital and Population Data Services Agency's information security policy and the valid terms of delivery. A detailed, fixed-form audit result intended for internal use is confidential and will not be disclosed to the public. Fixed-form reports are prepared separately for use outside of the organisation.

The DPDSA communicates the audit results to Traficom in accordance with the Act on Strong Electronic Identification and Electronic Services and Traficom's regulations and recommendations.

Finnish Transport and Communications Agency (Traficom), which supervises signature certification authorities, may audit the operation of a certification authority under the prerequisites set forth in the Act on Strong Electronic Identification and Trust Services.

The audit covers Traficom regulations on the information security of the certification authority's operations.

10.11.6 Management of access to systems

The certification authority ensures that only appropriately authorised people have access to the certification authority's system in conformance with the Regulation.

Digital and Population Data Services Agency's information security is managed according to Digital and Population Data Services Agency's information security policy and the standard ISO/IEC 27001.

The security of telecommunication is implemented in such a way that the certificate system's telecommunication network is a consistent whole isolated from other telecommunication networks and has doubled critical components.

10.11.7 Commissioning and maintenance of systems to be trusted

The certification authority shall use reliable systems and products protected against changes in conformance with the Regulation.

10.11.8 Business continuity management and processing of anomalies

In case of an emergency, for example when the certification authority's private signature key becomes compromised, the certification authority ensures that the operations are restored as soon as possible in conformance with the Regulation.

Digital and Population Data Services Agency has a continuity and preparedness plan for states of emergency that enables the continuity of the operations of Digital and Population Data Services Agency.

Digital and Population Data Services Agency's security policy takes into account the measures necessitated by the compromising of external security. Digital and Population Data Services Agency is **ISO 27001** certified with respect to information security, setting the requirements for Digital and Population Data Services Agency's operations also after the occurrence of a catastrophe.

10.11.9 End of the certification authority's operations

The certification authority ensures that any disturbance caused to the subscribers and parties trusting a certificate by the discontinuation of services subject to the certificate policy is minimised and that data are maintained constantly with which proof concerning the certification can be presented in legal proceedings in accordance with the Regulation.

The termination of the certification authority is considered to be a situation where all services related to the granting of the certification authority's certificate are permanently terminated. The termination of the certification authority does not refer to a situation where the certificate service is transferred from one organisation to another.

The certification authority communicates the termination of the certificate services as soon as possible, however at least one month before the time of termination.

01/01/2020

10.11.10 Compliance with regulations based on legislation

The certification authority must ensure that requirements based on legislation are adhered to.

With respect to terms of agreement pertaining to certificates granted to the public, the requirements of consumer legislation, including the directive on unreasonable terms in consumer agreements, 93/13/EEC, are taken into account.

A signature certificate granted in conformance with this certificate policy meets the requirements of the Regulation on a signature certificate.

Provisions on digital signatures made with a signature certificate are set out in the Act on Strong Electronic Identification and Trust Services (617/2009) Provisions on the certificates issued by the Digital and Population Data Services Agency are contained in the Act on the Digital and Population Data Services Agency (304/2019).

Digital and Population Data Services Agency's liability for damages related to the production of certificate services is determined according to the service agreement concluded with the certificate applicant. Digital and Population Data Services Agency is bound by the certification authority's liability for damages conformant to the Act on Strong Electronic Identification and Electronic Trust Services. Where applicable, the Tort Liability Act (412/1974) and Act on Electronic Services and Communication in the Public Sector (13/2003) are also applied.

In accordance with the Act on Electronic Services and Communication in the Public Sector, signature certificates can be used in all communication with public administration offered as electronic services.

Digital and Population Data Services Agency conforms to the principles of good personal data processing set forth in the Personal Data Act (523/1999) and to the good information management practices of the Act on the Openness of Government Activities (621/1999). Digital and Population Data Services Agency also secures information security with continuous training. Digital and Population Data Services Agency has also prepared policy rules for information services and certificate services.

Digital and Population Data Services Agency procures the duties pertaining to registration and personal identification under a separate, private-law contract pertaining to registration measures. Digital and Population Data Services Agency may obtain a service, for example, by adhering to the regulations set forth in the act on the government's joint services (2007/223).

The position of Digital and Population Data Services Agency is prescribed in the act on the Digital and Population Data Services Agency (304/2019). In Finland, signature certificate authorities are supervised by the Finnish Transport and Communications Agency.

10.11.11 Retention of information pertaining to signature certificates

The certification authority ensures that all data pertaining to signature certificates are stored for an appropriate time, in particular so that it can present proof pertaining to certification in legal proceedings in conformance with the Regulation.

Records pertaining to signature certification include registration data and data regarding significant events that have taken place with the certification authority with respect to the environment, key management or certificate management.

The provisions of the Archive Act (831/1994) are applied as the general law for archiving organisation certificates. The right to obtain information is determined according to the Act on the Openness of Government Activities (621/1999). With respect to the archiving of certificates, the provisions pertaining to archiving in electronic services legislation are also applied. Certificate register data are held for at least 5 years after expiry of the certificate.

The data archived by the certification authority are described in detail in the certification practice statement.

The archive data are stored in accordance with regulations pertaining to the certification authority in question.

Archived data are stored on high-security premises with access control.

Backups are stored in a place physically separate from the original data.

The certification authority ensures the availability and readability of the archives even in the event that the certification authority's operations are interrupted or terminated.

10.12 Organisation requirements

The certification authority must ensure that its organisation is reliable in conformance with the Regulation.

Digital and Population Data Services Agency is the certificate issuer conformant to this certificate policy. The position of Digital and Population Data Services Agency is prescribed in the register administration act (166/1996) and decree (248/1996).

A signature certificate granted in conformance with this certificate policy meets the requirements of the Regulation on a signature certificate.

Digital and Population Data Services Agency conforms to the principles of good personal data processing set forth in the Personal Data Act (523/1999) and to the good information management practices of the Act on the Openness of Government Activities (621/1999). Digital and Population Data Services Agency also secures information security with continuous training. Digital and Population Data Services Agency has also prepared policy rules for information services and certificate services.

Digital and Population Data Services Agency procures the duties pertaining to registration and personal identification under a separate, private-law contract pertaining to registration measures. Digital and Population Data Services Agency may obtain a service, for example, by adhering to the regulations set forth in the act on the government's joint services (2007/223).

Digital and Population Data Services Agency is responsible for the organisation certificates having been created with adherence to the procedures prescribed in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services

Agency, the Act on Strong Electronic Identification and Trust Services, the Act on Electronic Services and Communication in the Public Sector and the certificate policy and according to the data provided by the applicant of the certificate.

With respect to the processing of personal data, Digital and Population Data Services Agency conforms to the Personal Data Act. Digital and Population Data Services Agency works in constant collaboration with the Office of the Data Protection Ombudsman with respect to the processing of personal data.

Applicable legislation is adhered to in settling appeals and disputes, in administrative supervision and implementation of law. In the provision of organisation certificates, the Act on Strong Electronic Identification and Trust Services and the supervision and appeals procedure described therein must, in particular, be taken into account.

When granting organisation certificates, Digital and Population Data Services Agency is responsible for the organisation certificate meeting the requirements set in this certificate policy for organisation certificates. Any disputes shall be settled according to Finnish law in the District Court of Helsinki.

Organisation certificates are priced according to Digital and Population Data Services Agency's price list pertaining to commercial services.

11 Specification framework for other signature policies

Digital and Population Data Services Agency’s organisation certificates are signature certificates, which means that this section is not applied with respect to the provision of this organisation certificate.

11.1 Management of the signature certificate policy

The certification authority ensures that its certificate policy is up to date.

Digital and Population Data Services Agency may change the specifications because of legislation or functional requirements. Changes to the specifications are recorded in the certificate policy and certification practice statement documents as described here.

Digital and Population Data Services Agency publishes a certificate policy and a certification practice statement, available at the website www.fineid.fi.

Digital and Population Data Services Agency’s public specifications pertaining to the production of certificates can be obtained from the same website.

Agreements concluded with information technology vendors on the delivery of certificates and production system descriptions and product-related specifications are confidential.

Digital and Population Data Services Agency approves the certificate policy and certification practice statements pertaining to organisation certificates. The documents may be amended according to Digital and Population Data Services Agency's internal change policy.

Digital and Population Data Services Agency will communicate the changes to Traficom and on its own website well in advance of their entry into force.

Digital and Population Data Services Agency maintains version management of the documents and archives all certificate policy and certification practice statement documents. Typographic corrections and changes of contact details are possible with immediate effect.

1. All items of the certificate policy and certification practice statement can be amended by communicating the main upcoming changes 30 days before their entry into force.

2. Items that Digital and Population Data Services Agency does not deem to have significant effect on certificate holders and trusting parties may be amended with communication 14 days in advance.

11.2 Exceptions to signature certificate policies that apply to signature certificates granted to parties other than the general public

Digital and Population Data Services Agency's organisation certificates include a signature certificate and a means of strong electronic identification. Thus, this section is not applied with respect to the provision of this organisation certificate.

11.3 Additional requirements

The subscribers and parties trusting a certificate must be notified of the fulfilment of the requirements

a) whether the certificate policy does not apply to public use and whether exceptions are applied
b) whether the certificate policy in question includes requirements on the use of a secure signature creation device
c) how the policy in question increases or tightens the requirements of the signature certificate policy specified in this document.

11.4 Compliance

The certification authority may state it works according to this document and the applicable signature certificate policy only

a) the certification authority indicates it adheres to the itemised signature certificate policy and, upon request, makes an account of compliance available to the subscriber and parties trusting the certificate.

Such an account may be an auditor's report that confirms that the certification authority conforms to the requirements of a specific signature certificate policy. This may be an auditor internal to the certification authority's organisation but must not have a hierarchical relationship with the certification authority's unit implementing the operations.