PKI DISCLOSURE STATEMENT

Digital and Population Data Services Agency's organisation certificate

ISO 9001

ISO/IEC 27001

01/01/2020

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

PKI disclosure statement 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 Introduction

This document provides a general description of the practices applied by the certification authority and the terms and conditions governing the use of the organisation certificate and the restrictions on its use.

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 will apply with regard to signature certificates in trust services as of 1 July 2016.

A signature certificate issued in accordance with this certificate policy meets the requirements for an approved signature certificate laid down in the Regulation. The level of the identification certificate meets the requirements of High level of assurance in accordance with the Regulation and the regulation on levels of assurance.

This document describes the procedural requirements concerning the activities and administrative practices of certification authorities that issue identification and signature certificates under the Regulation. The use of a secure signature creation device is described in the procedural requirements specified in this document.

The 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. The 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 and provided for in Articles 28 and 29 of the Regulation.

2. PKI disclosure statement

2.1 Contact details of the certification authority

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

Digital and Population Data Services Agency (DPDSA) Certificate Services

P.O. Box 123

FI-00531 Helsinki

www.fineid.fi

01/01/2020

2.2 Certificate type, verification procedure and intended use

The organisation certificate contains the signature and identification certificates, provisions on which are contained in the Act on Strong Electronic Identification and Electronic Trust Services.

This document specifies the procedural requirements that apply to certification authorities issuing signature certificates and to the Digital and Population Data Services Agency, which is the provider of a strong electronic identification means. Procedural requirements are set for the activities and administration practice of certification authorities that issue 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.

Applications for an organisation certificate are made in person by visiting the registration authority's registration point. The registration authority must verify the identity of the certificate applicant from a valid document issued by the police. These are: the identity card issued after 1 March 1999, the passport and the driving licence that has been issued after 1 October 1990. Other acceptable forms of identity are: a valid passport or identity card issued by an official government agency of an EEA member state, Switzerland or San Marino, a valid driving licence issued by an official government agency of an EEA member state after 1 October 1990, or a valid passport issued by an official government agency of another state. The method of identification is entered on the application form and confirmed by signature by the registration clerk. In accordance with the agreement made with the client organisation, certificate applications can also be made using a certificate issued by the Digital and Population Data Services Agency after 1 March 2010.

The organisation certificate can be used for personal authentication and encryption, as well as electronic signing. The signature certificates issued under the document "Varmennepolitiikka organisaatiovarmenteita varten" (Certificate policy for organisation certificates) meet the requirements for signature certificate referred to in the Regulation and the Annexes to it. The certificate can be used without limitation according to its purpose in administrative applications and services and those provided by private organisations.

In addition, as of 1 December 2010, the Digital and Population Data Services Agency is a statutory certification authority in the health care sector under the Act on the Electronic Processing of Client Data in Social and Health Care (159/2007), the Act on Electronic Prescriptions (61/2007) and the Act on the Digital and Population Data Services Agency (304/2019).

2.3 Trusting the certificate

The purpose of the certificate 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 for the intended purpose. The trusting party must check that the certificate is valid and that it does not appear on a revocation list or using OSCP. The trusting party cannot fully trust the certificate if its validity has not been verified from the revocation list. The trusting party must verify the certificates from the revocation list before approval for possible revocation.

2.4 Certificate holder's obligations

- The purpose of the certificate 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 electronic signing, authentication or encryption.

- The certificate holder is responsible for ensuring that the data submitted for the application of the certificate are correct.
- Liability for the use of the smart card and for the legal actions taken with it and their financial consequences rests with the certificate holder. With respect to a signature certificate, the provisions of the Regulation and the Act on Strong Electronic Identification and Electronic Trust Services apply.
- The certificate holder must store his/her private keys and the PIN codes required for using them separately from each other and make every effort to prevent the loss, alteration or unauthorised use of the private keys and to ensure that they cannot be accessed by third parties. Transferring the smart card or disclosing the PIN code to a third party, for example by lending, releases the certification authority and the trusting party from any liability arising from the use of the card.
- The smart card must be handled and protected with the same care as other similar cards or documents, such as credit cards, driving licence or passport. The personal card access codes must be kept physically separate from the smart card.

2.5 Obligations of the trusting party concerning the verification of the certificate

The trusting party must verify that the certificate is valid and not on a revocation list. If a party trusting the certificate copies the revocation list from a directory, it must verify the genuineness of the revocation list by checking the electronic signature of the revocation list or OCSP. The validity period of the revocation list must also be checked. The revocation list is valid for eight hours.

If the most recent revocation list cannot be retrieved from the directory because of hardware or directory service malfunction, the certificate should not be approved if the validity period of the last retrieved revocation list has expired. All certificate approvals after the validity period are at the risk of the party trusting the certificate.

2.6 Limitations of liability

The 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. The 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) also applies.

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

The maximum extent of the 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 the 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).

The Digital and Population Data Services Agency is not liable for indirect or consequential damage caused to the smart card holder. Neither is the Digital and Population Data Services Agency liable for the indirect or consequential damage incurred by other partners of the party trusting the certificate or the smart card holder.

The Digital and Population Data Services Agency is not responsible for the operation of public telecommunication connections or data networks, such as the Internet, or for the inability to execute a legal transaction because of the non-functionality of a device or card reader software used by the card holder or for the use of the card 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 develop the certificate service. A certificate holder or a party trusting a certificate must bear their own expenses thus incurred, and the certification authority is not liable to compensate the certificate holder or a party trusting the 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 end users and based on a certificate or any expenses arising from them.

The responsibility of a certificate holder ends when he/she or the representative of the certificate holder's organisation 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.

2.7 Applicable agreements, certification practice statement and certificate policy

The rights and obligations of a certificate applicant are specified in the application document and general instructions for use, which comprise an agreement concluded with the certificate applicant. The application document contains the information on the rights and obligations of both parties. The application document and the instructions for use clearly state that the applicant for an organisation certificate, with his/her signature, confirms the correctness of the information provided and approves the creation of the organisation certificate and its publication or accepts that, in accordance with the agreement with the client organisation, the party trusting the certificate is otherwise notified of the certificate. 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 the organisation certificate and its PIN codes and the reporting of any misuse or lost cards.

An agreement has been concluded between the certification authority and registration authority, card manufacturer and other vendors that produce parts of the certificate services, indisputably specifying the rights, liabilities and obligations of both parties.

By issuing the organisation certificate, the certification authority also approves the application for certificate.

The Digital and Population Data Services Agency will prepare a separate certification practice statement for each certificate type that it has issued. The certification practice statement refers to the certificate policy document, which serves as a more general set of rules and guidelines describing the certificate type and that is common to all organisation certificates, irrespective of the technical instrument in which the certificate is placed.

The Digital and Population Data Services Agency publishes a certificate policy and a certification practice statement for the certificates that it has issued. The certificate policy contains a description of the procedures, terms and conditions, allocation of responsibilities and other matters related to the use of the certificate. The certification practice statement describes in more detail how the certificate policy is applied on different technical platforms.

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

2.8 Privacy protection

The certification authority and the registration authority observe the good data handling practice and data protection provisions when handling the personal data of the certificate holders. Special attention is paid to the handling of personal data, and the Digital and Population Data Services Agency has published a specific set of procedures for the provision of certificate services in accordance with the Personal Data Act.

2.9 Compensation policy

The 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. The 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) also applies.

The maximum extent of the 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 the 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).

2.10 Applicable law and resolution of disputes

The organisation certificate meets the requirements for signature certificate laid down in the Regulation.

Provisions on electronic signatures made with a certificate are contained in the Act on Strong Electronic Identification and Electronic 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).

The Digital and Population Data Services Agency's liability for damages in connection with certificate service provision is determined in the Act on Strong Electronic Identification and Electronic Trust Services (617/2009) and in addition, the Tort Liability Act (412/1974).

Under the Act on Electronic Services and Communication in the Public Sector (13/2003), certificates can be used in all communication with public administration.

The certification authorities are supervised by the Finnish Transport and Communications Agency (Traficom).

The organisation certificates have been created with adherence to the procedures laid down in the Act on the Digital and Population Data Services Agency, the Act on Strong Electronic Identification and Electronic Trust Services and the certificate policy and according to the data provided by the certificate holder.

2.11 Audits of the certification authority

The Finnish Transport and Communications Agency may audit the operation of a certification authority under the prerequisites set forth in the Act on Strong Electronic Identification and Trust Services. The Digital and Population Data Services Agency has the right to audit its technical suppliers in accordance with the audit procedure specified in the technical supply agreement in question. The audit is carried out at least once a year and at the start of each new contract period.

The audit is carried out to determine the technical supplier's compliance with the agreement, taking into account the requirements of information security management standards. Technical suppliers are generally assessed on the basis of the ISO/IEC 27001 standard and regulations issued by the Finnish Transport and Communications Agency.

The audit is carried out by the Digital and Population Data Services Agency or an external auditor commissioned by the Digital and Population Data Services Agency, who specialises in auditing technical vendors pertaining to certificate services. In the audit, consideration is given to the implementation of the eight areas of information security. Audited information security properties include confidentiality, integrity and availability.

The audit covers Traficom regulations on the information security requirements of certification authorities.

In the audit, the policy and the application instructions are compared with the operations of the entire certificate organisation and system. The Digital and Population Data Services Agency is responsible for ensuring the uniformity of the application instructions with the certificate policy.