PKI DISCLOSURE STATEMENT CITIZEN CERTIFICATES

Digital and Population Data Services Agency's citizen certificate

ISO 9001

ISO/IEC 27001

01/01/2020

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

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

01/01/2020

Contents

01/01/2020

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 certificate and the restrictions on its use.

This document contains references to the following documents:

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

OID:1.2.246.517.1.10.202;

Certification practice statement for citizen certificate stored on an electronic ID card

OID: 1.2.246.517.1.10.202.1;

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. 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.

1 PKI disclosure statement

1.1 Certification authority's contact details

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

1.2 Certificate type, verification procedure and intended use

Citizen certificate is a certificate for secure use of e-services and it can be stored on a broad range of different technical platforms issued by the authorities, such as an electronic ID card or a USB token.

Citizen certificate applications are made in person by visiting a police registration authority or another registration point. The applicant's identity is verified during the visit in a manner described in the certification practice statement. If the applicant does not hold any of these documents, the police will verify his/her identity by other methods. The method of identification is entered on the application form and the registration clerk signs the document, confirming that the applicant's identity has been checked. The information presented by the applicant (such as identifiers, name and official address) are compared against the data stored in the Population Information System. In citizen certificate, identification of the individual is by means of the electronic client identifier (SATU) created separately for e-services and defined in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (304/2019).

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

Citizen certificates can be used for personal authentication and encryption, as well as electronic signing. The signature certificates issued under the document "Varmennepolitiikka valtion kansalaisvarmenteita varten" (Certificate policy for Government-issued citizen certificates) meet the requirements laid down in the following piece of legislation: 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 (Regulation). The citizen certificate can be used without limitation in administrative applications and services and those provided by private organisations.

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.

The citizen certificate applicant may store the e-mail address in the citizen certificate and the population information system at his/her discretion. The e-mail address will be entered in the citizen certificate and the population information system as stated by the applicant. The e-mail address stored in the citizen certificate is stored in the public directory, as is the rest of the data content in the citizen certificate. The e-mail address cannot be changed during the validity of the citizen certificate.

1.3 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 verify the validity of the certificate. The trusting party cannot fully trust the certificate if the validity of the certificate has not been verified from the OCSP service or the revocation list. The trusting party must check the validity of the certificates before approving them.

1.4 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 for the intended purpose.

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 citizen certificate 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 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 electronic ID card and the other technical instruments containing a citizen certificate 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 citizen certificates.

The loss or suspected misuse of the smart card must be reported without delay to the certification authority by calling the free revocation service at +358 800 162 622. Deaf and hard of hearing customers can contact the textphone service at +358 100 2288.

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

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. The validity period of the revocation list must also be checked.

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.

1.6 Limitations of liability

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 Trust Services and the Act on Electronic Services and Communication in the Public Sector. 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 the Digital and Population Data Services Agency's actions.

The Digital and Population Data Services Agency is not liable for indirect or consequential damage caused to the certificate 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 ID card holder.

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 the Digital and Population Data Services Agency's direct actions.

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 Digital and Population Data Services Agency is not responsible for the functioning 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 used by the card holder or for the use of the certificates in contradiction to their intended use.

The certification authority is not liable for errors in the online service or application that occur during the use of the certificate or any expenses arising from them. 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 has reported the necessary data to the revocation service for revoking the certificate and has 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.

1.7 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 details of the rights and obligations of both parties. The application document and instructions for use clearly state that the applicant for a citizen certificate, with his/her signature, approves the correctness of the information provided and the creation of the certificate and its publication. At the same time, the applicant accepts the rules and terms pertaining to the use of the citizen certificate and undertakes to store the certificate and its PIN codes in a proper manner and to report 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 citizen certificate, the certification authority also approves the application for the 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 citizen 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 concerning 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.

1.8 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.

1.9 Compensation policy

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 Trust Services and the Act on Electronic Services and Communication in the Public Sector. 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 is for direct damage incurred, if the damage is the result of the Digital and Population Data Services Agency's direct actions.

1.10 Applicable law and resolution of disputes

The citizen certificate meets the requirements for signature certificates laid down in 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.

Provisions on electronic signatures made with a signature certificate are laid down in the Act on Strong Electronic Identification and Trust Services (617/2009). The electronic identity card is provided for in the Identity Card Act (663/2016), and certificates issued by Digital and Population Data Services Agency are provided for in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (304/2019). Electronic services are also subject to the provisions of the Act on Electronic Services and Communication in the Public Sector (13/2003).

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 Trust Services and the Act on Electronic Services and Communication in the Public Sector. Where applicable, the Tort Liability Act (412/1974) also applies.

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 services.

Citizen certificates have been created with adherence to the procedures laid down 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 in accordance with the data provided by the certificate holder.

1.11 Audits of the certification authority

The Finnish Transport and Communications Agency (Traficom), which supervises signature certification authorities and providers of strong electronic identification services and instruments, 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 27001 standard and Traficom regulations.

The audit is carried out by Digital and Population Data Services Agency's Head of Information Management 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.