PKI DISCLOSURE STATEMENT

for social welfare and health care professionals' certificate

01/01/2020

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

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 1.1, centre name change	1 Jan 2020 TS

Contents

01/01/2020

1 Introduction

This PKI disclosure statement is a summary of the Digital and Population Data Services Agency's certificate policy for the social welfare and health care professionals' certificate. The prerequisites, application and scope of the Public Key Infrastructure (PKI) certification activities of the Digital and Population Data Services Agency are set out in the certificate policy. At practical level, the principles contained in the certificate policy are laid out in the certification practice statement and other procedural guidelines supplementing the certificate policy.

In this PKI disclosure statement, references are made to the following documents:

Certificate policy for social welfare and health care professionals' certificate, OID: 1.2.246.517.1.10.206

Certification practice statement for social welfare and health care professionals' certificate, OID: 1.2.246.517.1.10.206.1

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. 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. 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. 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.

2 PKI disclosure statement

2.1 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

01/01/2020

Digital and Population Data Services Agency (DPDSA) Certificate Services

P.O. Box 123

FI-00531 Helsinki

www.fineid.fi

2.2 Certificate type, verification procedures and intended uses

The Digital and Population Data Services Agency issues authentication and signature certificates to health care professionals referred to in the Act on Health Care Professionals (559/1994) and to social welfare professionals meeting the qualification requirements for social welfare professionals performing professional functions that are laid down in the Act on Qualification Requirements for Social Welfare Professionals (272/2005).

The applicant's identity is verified from a valid identity document issued by the police (identity card, passport, or a 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. If the applicant does not hold any of these documents, the police will verify his/her identity by other methods. The practice rights of health care professionals are checked at the central register of Finnish health care professionals (Terhikki register) maintained by the National Supervisory Authority for Welfare and Health (Valvira), while the practice rights of social welfare professionals are checked in accordance with the instructions issued by Valvira.[1] Temporary certificates can be used for personal authentication and encryption or electronic signing. The certificate can be used without limitation according to its purpose in administrative applications and services and those provided by private organisations.

Social welfare and health care professionals' certificates are used for the electronic identification of certificate holders and electronic signing or verifying the authenticity, integrity and non-repudiation of digital documents or other data (such as patient record entries and electronic prescriptions).

[1] Under a Government proposal submitted to Parliament (HE 354/2014 vp), the Act on Social Welfare Professionals will replace the Act on Qualification Requirements for Social Welfare Professionals (272/2005) from 1 January 2016. Under the Government proposal, the practice rights of social welfare professionals would be checked at the register of social welfare professionals maintained by Valvira.

2.3 Trusting the certificate

Provisions on the main uses of the certificates are contained in the Act on the Electronic Processing of Client Data in Social and Health Care (159/2007) and in the Act on Electronic Prescriptions (61/2007). Certificates can also be used in other information systems of social welfare, health care and pharmacy services.

The intended use of the certificate is defined in the certificate policy and the certification practice statement of the certificate and the certificate may only be used in accordance with its intended use.

The party trusting the certificate must check that the certificate in question is valid (from the OCSP service or by ensuring that the certificate does not appear on the revocation list). 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. Before approving the certificates, the trusting party must verify the certificates on the OCSP service or that they do not appear on the revocation list so that they can be revocated, if necessary.

The trusting party is responsible for ensuring that in its own information systems the certificate is used only for the purpose specified in the certificate policy. The certificate policy contained in the certificate can be used to ascertain the appropriate use of the certificate.

The trusting party must ensure that its applications meet the requirements laid out in the certificate policy.

2.4 Certificate holder's obligations

Social welfare and health care professionals must undertake to act in accordance with the certificate policy when applying for and using the social welfare and health care professionals' certificate. The certificate holder is responsible for ensuring that the data provided in the application for 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.

Social welfare and health care professionals must keep and manage their certificates and key pairs and the associated codes and certificate cards with due care. The certificate holder must take measures to prevent the loss of the certificate card and protect PINs against unauthorised disclosure or misuse.

The certificate card must not be left in a reader unattended or given to another person in any circumstances.

Social welfare and health care professionals must notify the revocation service of the following:

- of the loss or suspected misuse of their certificate card.

If the certificate card is damaged, the card holder must arrange for the certificates held on the card to be revoked and apply for a new card at the registration point. The card renewal procedure is the same as the procedure for applying the card and the certificate for the first time.

PIN codes used to activate the keys must not be kept together with the certificate card. The certificate holder must change his/her PIN codes if there is reason to believe that they may have been disclosed to unauthorised parties.

If the PIN code is locked and the associated PUK unlocking code has been lost, the card holder must contact the certification authority in order to obtain the PUK unlocking code.

2.5 The trusting party's duty to verify the validity of a certificate

Before approving the certificate, the trusting party must verify that the certificate is valid and it has not been revoked.

The trusting party is responsible for verifying the validity of the certificate status data from the OCSP service or from the valid revocation list. The certificate can only be trusted if the trusting party has carried out the following certificate revocation checks:

1. The trusting party must check the revocation path and its authenticity from the certification authority's electronic signature.

2. The trusting party must check the validity period of the revocation list to ensure that the list is valid.

3. The certificates (the public key) can be stored locally in the trusting party's system, but the validity of the certificate must be verified before it is approved.

If the valid revocation list is not available due to a fault in the system or service, the certificates must not be approved. If, however, the trusting party approves the certificate, it does so at its own risk.

2.6 Non-liability clause and limitations of liability

The non-liability clauses included in the agreements concluded between the certification authority and its contractual partner or in the certification authority's specific requirements concerning certificate holders and parties using the certificate system apply to the certification authority's contractual partner, certificate holder and the party using the certificate system in the same way as non-liability clauses and limitations of liability set out in the certificate policy.

The certification authority is not liable for any damage caused by the conduct of the certificate holder or the party using the certificate system in violation of the law, the certificate policy, certification practice statement or other instructions.

The certification authority 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 certification authority's direct actions.

The maximum extent of the certification authority'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 certification authority's direct actions.

The certification authority is not liable for indirect or consequential damage caused to the certificate holder. Neither is the certification authority liable for the indirect or consequential damage incurred by a party trusting a certificate or by another contractual partner of the certificate holder.

The certification authority 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 card reader software used by the 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 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 the liability, the revocation request must be made immediately upon noticing the reason for the request.

2.7 Agreements, certification practice statement and certificate policy

The rights, responsibilities and duties of the certification authority and the certificate holder are specified in the certificate policy. By signing the certificate application, the social welfare and health care professional undertakes to observe the terms and conditions governing the use of the certificate. The social welfare and health care professional will receive the valid terms and conditions together with the certificate.

Upon signing, the social welfare and health care professional undertakes to immediately notify the revocation service if the certificate card is lost or if there is a suspicion or possibility of its misuse.

The certification authority and its authorised registration authorities conclude an agreement which states both party's rights, responsibilities and duties.

The certification authority may conclude agreements with trusting parties and other parties. Each agreement must clearly state both party's rights, responsibilities and duties. The certification authority concludes agreements with the certificate service supplier and component suppliers as necessary.

The certificate application and the general terms and conditions of use form the agreement concluded with the certificate holder. The terms and conditions of use are part of the certificate policy documents.

The application document and instructions for use clearly state that the applicant for a certificate, with his/her signature, approves the correctness of the information provided and the creation of the certificate and its publication.

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, which serves as a more general set of rules and guidelines describing the certificate type and that is common to all certificates, irrespective of the technical instrument in which the certificate is placed. 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 handling of private information in the certification authority's systems is subject to the legislation on the handling of private information and the protection of privacy. The handling of public information in the certification authority's systems is subject to the provisions of the Act on the Openness of Government Activities (621/1999). The certification authority ensures that private information handled in its systems is protected against unauthorised access. Information can be disclosed to authorities on the basis of acts, decrees and associated regulations.

The certification authority has published specific policy rules conformant to the Personal Data Act with regard to the certificate services.

2.9 Compensation for damage

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 Trust Services and the Act on Electronic Services and Communication in the Public Sector. Where applicable, the Tort Liability Act (412/1974) and Act on Electronic Services and Communication in the Public Sector (13/2003) are also applied.

2.10 Applicable law

Finnish law applies to the social welfare and health care certificate service. The parties endeavour to settle any disputes arising from the social welfare and health care certificate service by negotiations. If no settlement is reached, the disputes between the parties will be brought before the district court of the certification authority's domicile in Finland.

The Act on Strong Electronic Identification and Trust Services and the Act on Electronic Services and Communication in the Public Sector contain provisions on the identification by means of strong electronic identification and electronic signatures by means of a signature certificate. Provisions on the certificates issued by the Digital and Population Data Services Agency are contained in the Act on the Electronic Processing of Client Data in Social and Health Care, the Act on Electronic Prescriptions, and the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (304/2019).

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

2.11 Acceptance audit of the certification authority's operations

The 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 certification authority 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 the 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.