



DIGITAL AND
POPULATION DATA
SERVICES AGENCY

PKI DISCLOSURE STATEMENT TEM- PORARY CERTIFICATES

Temporary certificate of the Digital and Population Data
Services Agency

15.9.2023



Jukkola Auli

15.9.2023

Document management

Owner	
Prepared by	Saaripuu Tuire, Jukkola Auli
Inspected by	
Approved by	Mikko Pitkänen

Version control

version no.	what has been done	date/person
v 1.0	Approved version 1.0.	3 May 2018
v 1.1	Approved version 1.1, Centre name change.	1 Jan 2020
v 1.2	Updated version, accessibility features	6 May 2021
v 1.3	Added information regarding log data	1.10.2021/VA
v 1.4	Updated version and CPS links	23.9.2022/SK
v 1.5	Updated version, editorial changes, driving license removed from identification documents, fax number removed from contact details.	15.9.2023/AJ





Jukkola Auli

15.9.2023

Table of contents

1	Introduction.....	3
2	PKI disclosure statement	3
2.1	Certification authority's contact details	3
2.2	Certificate type, verification procedure and intended use	4
2.3	Trusting the certificate.....	4
2.4	Certificate holder's obligations	4
2.5	Obligations of the trusting party concerning the verification of the certificate.....	5
2.6	Limitations of liability	5
2.7	Applicable agreements, certification practice statement and certificate policy	6
2.8	Privacy protection	6
2.9	Compensation policy.....	7
2.10	Applicable law and resolution of disputes.....	7
2.11	Audits of the certification authority	7





Jukkola Auli

15.9.2023

PKI DISCLOSURE STATEMENT TEMPORARY CERTIFICATES

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 temporary certificate and the restrictions on its use.

This document contains references to the following documents:

Certificate policy for temporary certificate of the Digital and Population Data Services Agency (later certification authority, CA).

OID:1.2.246.517.1.10.204

Certification practice statement for temporary certificate

OID: 1.2.246.517.1.10.204.1

and

Certification practice statement for temporary certificate for social welfare and health care personnel and actors

OID 1.2.246.517.1.10.204.2

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 kirjaamo@dvv.fi

Business ID: 0245437-2

Digital and Population Data Services Agency (DPDSA) Certificate Services

P.O. Box 123

FI-00531 Helsinki

www.dvv.fi/en





Jukkola Auli

15.9.2023

2.2 Certificate type, verification procedure and intended use

A temporary certificate is a certificate that supports the use of the organization certificate issued by the certification authority, OID: 1.2.246.517.1.10.203.

Applications for a temporary certificate are made in person by visiting the registration authority's registration point.

When an application for the certificate is submitted, the registration authority must verify the identity of the certificate applicant from a valid document issued by the police. These are: identity card issued after 1 March 1999 and passport. 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, 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.

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 organizations.

Log data relating to certificate issuing and revocation will be retained for at least seven (7) years after certificate validity.

2.3 Trusting the certificate

The intended use 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 integrity of the certificate chain and that the certificate is valid and that it does not appear on a revocation list. The party trusting the certificate must check the certificates from the revocation list or the OCSP service. The certificate status data can also be verified from the OCSP service. 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.

2.4 Certificate holder's obligations

- The intended use of the certificate is defined 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 purpose for personal authentication and encryption, or electronic signing.
- The certificate holder is responsible for ensuring that the data submitted for the application of the certificate is correct.
- Liability for the use of the temporary certificate and for the legal actions taken with it and their financial consequences rests with the certificate holder. With respect to a certificate, the provisions of the Act on Strong Electronic Identification and Trust Services (617/2009) apply. If the certificate holder is a social welfare and health care employee or a social welfare and health care actor, the certificate must also be in accordance with the provisions contained in the Act on the Electronic Processing of Client Data in Social and Health Care



Jukkola Auli

15.9.2023

(159/2007) and the Act on Electronic Prescriptions (61/2007) and the provisions and requirements issued under them.

- The certificate holder must keep his/her private key and the PIN code required for using it separately from each other and aim to prevent the loss, alteration, or unauthorized use of the private key and to ensure that it 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 temporary certificate.
- The smart card with a temporary certificate must be managed and protected with the same care as other similar cards or documents, such as credit cards, identity card or passport. 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

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.

2.6 Limitations of liability

CA is bound by the regulations conformant to the Act on Strong Electronic Identification and Trust Services (617/2009) and, where applicable, to the Tort Liability Act (412/1974).

CA is not liable for damage caused by the disclosure of a PIN code or a certificate holder's private key unless the disclosure is the direct result of CA's actions.

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

CA is not liable for indirect or consequential damage caused to the card holder. Neither is CA liable for the indirect or consequential damage incurred by a party trusting the certificate or the card holder.

CA 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.

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



Jukkola Auli

15.9.2023

CA 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.

CA 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 certificate holder's liability for the use of the certificate ends when he/she has notified the registration authority of the certificate holder's organization on the need to revoke the certificate and upon receiving a notice of the receipt of the revocation request. In order to terminate liability, the revocation request must be made without delay 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 instructions for use clearly state that the applicant for temporary certificate, with his/her signature, approves the correctness of the information provided and the creation of the certificate. At the same time, the applicant accepts the rules and terms pertaining to the use of the temporary certificate and undertakes to store the temporary certificate and its PIN code with care and to report any misuse or lost card.

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

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

CA 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 temporary certificates, irrespective of the technical instrument in which the certificate is placed.

CA 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 <https://dvv.fi/en/certificate-policy>.

2.8 Privacy protection

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



Jukkola Auli

15.9.2023

2.9 Compensation policy

CA is bound by the regulations conformant to the Act on Strong Electronic Identification and Trust Services (617/2009) and, where applicable, to the Tort Liability Act (412/1974).

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

2.10 Applicable law and resolution of disputes

Provisions on the certificates issued by the CA are contained in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (304/2019).

CA is bound by the regulations conformant to the Act on Strong Electronic Identification and Trust Services (617/2009) and, where applicable, to the Tort Liability Act (412/1974). In accordance with the Act on Electronic Services and Communication in the Public Sector, certificates can be used in all communication with public administration.

The identification service providers are supervised by the Finnish Transport and Communications Agency.

Temporary certificates have been created in accordance with 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 certificate policy, and the certification practice statement and in accordance with the data provided by the certificate applicant. If the temporary certificate has been created for social welfare and health care personnel or social welfare and health care actors, the provisions contained in the Act on the Electronic Processing of Client Data in Social and Health Care (159/2007) and the Act on Electronic Prescriptions (61/2007) and the regulations and requirements issued under them are also observed.

In addition, CA has also acted as a statutory certification authority for health care since 1 December 2010 and as a statutory certification authority for social welfare since 1 April 2015 following the amendment of 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 Population Information System and the Certificate Services of the Digital and Population Data Services Agency (304/2019). The Digital and Population Data Services Agency Certificate Service unit is responsible for the agency's certification activities.

2.11 Audits of the certification authority

Finnish Transport and Communications Agency (Traficom), which supervises the providers of identification services, may audit the operation of an identification service provider under the prerequisites set forth in the Act on Strong Electronic Identification and Trust Services. CA 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 conducted at least once a year and at the start of each new contract period.



Jukkola Auli

15.9.2023

The audit is conducted to determine the technical supplier's compliance with the agreement, considering the requirements of information security management standards. Technical suppliers are assessed on the basis of the ISO/IEC 27001 standard, CA's information security policy or technical supply agreements.

The audit is conducted by CA's Head of Information Management, or an external auditor commissioned by CA, who specializes 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.

In the audit, the policy and the application instructions are compared with the operations of the entire certificate organization and system. CA is responsible for ensuring the uniformity of the application instructions with the certificate policy.

