PKI DISCLOSURE STATEMENT FOR DIGITAL AND POPULATION DATA SERVICES AGENCY'S SERVICE CERTIFICATE FOR THE SOCIAL WELFARE AND HEALTHCARE SECTOR

DOCUMENT MANAGEMENT

Owner	
Prepared by	Tuire Saaripuu
Inspected by	
Approved by	Joonas Kankaanrinne

VERSION CONTROL

version no.	what has been done	date/person
v 1.0	Approved version 1.0.	3.5.2018
v 1.1	Updated version	18.6.2019
v 1.2	Updated version, Centre name change.	1.1.2020

Table of contents

1.1.2020

PKI DISCLOSURE STATEMENT FOR DIGITAL AND POPULATION DATA SERVICES AGENCY'S SERVICE CERTIFICATE FOR THE SOCIAL WELFARE AND HEALTHCARE SECTOR

1 Certification authority's contact details

Digital and Population Data Services Agency

P.O. Box 123 (Lintulahdenkuja 2)
00531 Helsinki
Business ID: 0245437-2

Tel. +358 295 535 001
Fax. +358 9 876 4369
kirjaamo@dvv.fi

Digital and Population Data Services Agency (DPDSA) Certificate Services

P.O. Box 123
FI-00531 Helsinki
www.fineid.fi

2 Certificate type, verification procedure and intended use

The service certificate is a certificate issued by the Digital and Population Data Services Agency that is used to authenticate a service provider's or an individual person's server or service.

To apply for a service certificate, a specific form should be used. You can obtain and print out this form on such sites as www.fineid.fi.

Before issuing a certificate, the Digital and Population Data Services Agency checks the information supplied by the applicant. Once the certificate has been issued, it will be delivered to the customer as agreed.

Before issuing the certificate, the certification authority will check the applicant's information in such sources as the Virre register in the online service of the Finnish Patent and Registration Office. In this connection, the Digital and Population Data Services Agency will verify the domain name by means of an e-mail message. A proxy should be submitted together with the application if the certificate holder (IT contact person or similar) is acting on behalf of a company or an organisation. The information of central or local government authorities and parishes will not be checked in the Virre register. The Digital and Population Data Services Agency must have access to any domain names ending with .fi and information on their administration when processing

the application. Other domain names will be checked using any available online services or other reliable methods. The Digital and Population Data Services Agency only issues server certificates for IP addresses or domains used for public administration purposes.

When processing certificate requests, the public key is tested for known weaknesses using a software tool.

A service certificate will be issued for no more than 27 months. The same procedure should be used for renewing a certificate as when submitting the original application. The annual fee indicated in the service price list will be charged for using the certificate.

Service certificates can be used to authenticate both public administration and private sector services. The service certificate allows the service user to verify the authenticity of the service provider.

3 Trusting a certificate

The purpose of the certificate is specified in the certificate policy and certification practice statement of each certificate type and in the certificate. The certificate may only be used for the intended purpose. The relying party must check that the certificate is valid and that it does not appear on a revocation list. The real-time certificate status can also be checked from the OCSP service. The relying party cannot trust the certificate in good faith if its status has not been checked. Before accepting certificates, the relying party must check that they are not on the revocation list.

The information published by the certification authority is available on the certification authority's website. Confidential data used in the certificate system are stored in the certification authority'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 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. The certification authority has also prepared a description of file for each component of the certificate system compliant with the Personal Data Act with respect to the processing of personal data.

The provisions of the archive act (arkistolaki, 831/1994) are applied as the general act on archiving. 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 will be kept on file for at least 5 years after certificate expiry.

4 Certificate holder's responsibilities

The purpose of the certificate is specified in the certificate policy and certification practice statement of each certificate type and in the certificate. The certificate may only be used for the intended purpose.

The certificate holder (service provider) is responsible for ensuring that the data provided in the application for the certificate are correct.

The certificate holder must keep his/her private key in a safe environment and ensure that it cannot be accessed by third parties, modified or used without authorisation. The certificate holder must notify the certification authority immediately if they suspect that the certificate holder's private key has been compromised. The certification authority will then revoke the relevant service certificate. Responsibilities of the relying party concerning certificate verification

5 Responsibilities of the relying party concerning certificate verification

It is the responsibility of the party relying on a service certificate to ensure that the certificate is used according to its intended use.

A party relying on the service certificate must adhere to the certificate policy and certification practice statement.

A party relying on a service certificate may trust the service certificate in good faith after verifying that the certificate is valid and that it is not on a revocation list. A party relying on a service certificate shall check that the certificate is not on the revocation list. In order to reliably verify the validity of a service certificate, the party relying on the service certificate must comply with the following procedure for revocation list checks.

If a party relying on the certificate copies the revocation list from a directory, it must verify the authenticity of the revocation list by checking the electronic signature of the revocation list. In addition, the validity period of the revocation list must 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 relying on the certificate.

6 Limitations of liability

The Digital and Population Data Services Agency's liability related to the provision of certificate services is determined under the valid service contracts and pursuant to the provisions in the Tort Liability Act (412/1974). The Digital and Population Data Services Agency is not liable for damage caused by the disclosure of a certificate holder's private key unless the disclosure is the direct result of the 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 relying on 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 invoiced for the certificate in the preceding 3 months (the share payable to the DPDSA).

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 indirect or consequential damages incurred by other partners of the relying party or the certificate holder.

The Digital and Population Data Services Agency is not liable for the functioning of public telecommunications or information networks, including the Internet.

The certification authority has the right to interrupt the service to carry out modifications or maintenance. Modifications 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 relying on a certificate must bear their own expenses incurred for this reason, 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 certificate holder's responsibility for certificate use ends when he or she, or a representative of the certificate holder's organisation, has provided the certification authority with the information required to revoke the certificate. In order to terminate the liability, the revocation request must be made immediately upon noticing the reason for making the request.

7 Applicable agreements, certification practice statement and certificate policy

The certificate applicant's rights and obligations are stated in the certificate policy and certification practice statement documents. By his or her signature, the applicant confirms that the information provided is correct and accepts that the certificate will be created and published. At the same time, the applicant accepts the rules and conditions pertaining to service certificate use and undertakes to protect the service certificate and report any misuse.

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

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

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 describes 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 in certificate production.

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

8 Privacy protection

The certification authority and the registration authority observe good data processing practices and data protection provisions when handling the certificate holders' data. Special attention is paid to the processing of personal data, and the Digital and Population Data Services Agency

has published a specific set of procedures for the provision of certificate services compliant with the Personal Data Act.

9 Applicable legislation, resolution of disputes and compensation policy

The Digital and Population Data Services Agency's liability related to the provision of certificate services is determined under the valid service contracts and pursuant to the provisions in the Tort Liability Act (412/1974). In addition, the requirements laid down in the Act on Strong Electronic Identification and Trust services (617/2009) apply to the Digital and Population Data Services Agency.

10 Audits of the certification authority

The Finnish Transport and Communications Agency (Traficom), which supervises certification authorities, may audit the certification authority's operation. 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. An audit is carried out at least once a year and at the start of each new contract period.

Audits are 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.

The audit is carried out by the Digital and Population Data Services Agency's Head of Information Security or an external auditor commissioned by the Digital and Population Data Services Agency, who specialises in auditing technical vendors that provide certificate services. In the audit, consideration is given to the implementation of 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 that the application instructions are consistent with the certificate policy.