PKI DISCLOSURE STATEMENT FOR THE DIGITAL AND POPULATION DATA SERVICES AGENCY'S SERVICE CERTIFICATES

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	Adopted 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 THE DIGITAL AND POPULATION DATA SERVICES AGENCY'S SERVICE CERTIFICATES

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

2 Certificate type, validation procedures and usage

The service certificate is a certificate issued by the Digital and Population Data Services Agency (DPDSA) that is used for the certification of a service provider's (organisation's or private individual's) server or service.

Service certificate applications are submitted using a designated form that can be printed out at www.fineid.fi.

Before issuing a certificate, the CA shall verify the applicant's details using sources such as the on line Virre –Register maintained by a governmental authority, National Board of Patents and Registration of Finland. Digital and Population Data Services Agency verifies the ownership of the Domain Name by sending an email message in order to control the ownership. Also to be submitted is a proxy if the certificate applicant (such as an IT contact person) acts on behalf of the enterprise/organisation. The same procedure will be conducted in conjunction with certificate renewal. Central and local public government and church authorities are not verified tin the Virre-register. Internet domain names ending in .fi held by the applicant and details of their management must be made available to the DPDSA during the processing of the application. Other domain names are verified in open network based registers if available or otherwise in a reliable manner. Digital and Population Data Services Agency issues certificates only to IPs or domain names dedicated for services provided by a public authority. A server certificate is issued for a maximum of 27 months.

Certificate renewal takes place following the same application procedure as for the original application. The fees charged for certificates are based on the annual fee specified in the service tariff.

Service certificates can be used for the identification of services. The service certificate enables the service user to verify the authenticity of the service provider.

3 Reliance limits

The intended use of each certificate is specified in the relevant Certificate Policy and Certification Practice Statement and well as in the certificate. Certificates may only be used in accordance with their intended use. Relying parties must check that the certificate used has not expired and that it is not included in a Certificate Revocation List (CRL). A relying party cannot rely upon a certificate in good faith if the validity of the certificate has not been verified from the CRL. Relying parties are obliged to verify whether certificates are on a CRL before accepting them to make sure they have not been revoked.

Information published by the CA is available on the CA's website. Confidential data of the certificate system is stored in the CA's own, confidential data warehouse. CA data is archived in accordance with current archiving regulations. Particular care is exercised in the processing of personal data, and the DPDSA has published a specific Code of Conduct for the provision of certification services in accordance with the Personal Data Act. The CA has also prepared for each section of the certificate system a personal data file description regarding the processing of personal data.

The provisions of the Archives Act (831/1994) apply as general legal provisions governing archiving. The right to access information is determined in accordance with the Act on the Openness of Government Activities (621/1999). Provisions laid down in legislation on electronic services also apply to the archiving of certificates. Certificate register data is retained for ten (10) years following certificate expiry.

4 Certificate holders' obligations

The intended use of each certificate is specified in the relevant Certificate Policy, Certification Practice Statement and the certificate. Certificates may only be used in accordance with their intended use.

The certificate holder (service provider) is responsible for the accuracy of the information submitted with the certificate application.

The certificate holder must store its private key in a secured environment and seek to prevent its loss, unauthorised access, modification or unauthorised use.

The certificate holder must inform the Certification Authority (CA) immediately if it is suspected that the certificate holder's private key has been illegally disclosed. In such cases the service certificate in question will be revoked by the CA.

5 Certificate status checking obligations of relying parties

Relying parties are obliged to ensure that certificates are used for their intended use.

Relying parties must comply with the Certificate Policy and the Certification Practice Statement.

Relying parties may rely upon a service certificate in good faith once it has verified that it is valid and that it is not in the Certificate Revocation List (CRL). Relying parties are obliged to verify whether a certificate is on the CRL. To ensure reliable service certificate validity, relying parties must comply with the CRL verification measures presented below.

If a relying party copies the CRL from the directory, it must verify the authenticity of the CRL by verifying the electronic signature of the CRL. The period of validity of the CRL must also be checked.

If the latest CRL cannot be accessed from the directory due to equipment or directory service malfunction, no certificate should be accepted if the period of validity of the latest obtained CRL has expired. Any certificate acceptance that takes place following this period of validity takes place at the relying party's own risk.

6 Limitations of liability

The Digital and Population Data Services Agency's (DPDSA's) liability for damages related to the provision of certificate services is determined in accordance with the provisions of the Tort Liability Act (412/1974). The DPDSA is not liable for any loss or damage arising from the disclosure of the certificate holder's private key unless such disclosure is directly attributable the DPDSA's action.

The DPDSA's liability does not exceed direct loss or damage to the certificate holder or relying party where the loss or damage is attributable to direct action by the Digital and Population Data Services Agency and never exceeds 15% of the amount of certificate invoicing in the preceding 3 months (share booked for the DPDSA).

The DPDSA is not liable for any indirect or consequential loss or damage suffered by the certificate holder. Furthermore, the DPDSA is not liable for any indirect or consequential loss or damage suffered by a relying party or other contractual partner of the certificate holder.

The DPDSA is not liable for the functioning of public telecommunications connections or information networks such as the internet.

The CA has the right to suspend the service for the duration of amendment or maintenance work. Any amendments to or maintenance work on the CRL is notified in advance.

The CA has the right to further develop the certification service. The certificate holder or relying party must cover their own costs arising due to this. The CA is not liable for compensating the certificate holder or relying party for any such costs arising from the CA's development activity.

The CA is not liable for errors in an online service or application intended for end users and based on a certificate or any costs arising from such errors during certificate usage.

The certificate holder's liability for certificate use ends as soon as the certificate holder or a representative of the certificate holder's organisation has provided the CA with the information necessary for certificate revocation. To terminate liability, the revocation notification must be made as soon as the need arises.

7 Applicable agreements, Certification Practice Statement and Certificate Policy

The certificate holder's rights and obligations are specified in the Certificate Policy and Certification Practice Statement documents. The service certificate applicant must confirm the accuracy of the information provided and the generation of the certificate and its publication with his/her signature. In doing so the applicant also accepts the rules, terms and conditions governing the use of the service certificate and undertakes to take care of the storage of the service certificate and notify of any misuse.

An agreement has been entered into between the CA and the registration authority and other providers supplying elements of certification services that specifies each party's rights, liabilities and obligations indisputably.

On issuing a service certificate the CA also approves the certificate application.

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

The CA publishes the Certificate Policy and Certification Practice Statement for certificates issued by the CA. The Certificate Policy describes the procedures, terms and conditions of use, division of responsibilities and other aspects of service certificate use. The Certification Practice Statement is a more detailed description of how the Certificate Policy is applied in certificate production.

Both the Certificate Policy and the Certification Practice Statement can be found at www.fineid.fi.

8 Privacy policy

The Certification Authority (CA) and the registration authority maintain good data processing practice and privacy protection in the processing of the details of certificate applicants. Particular care is exercised in the processing of personal data, and the Digital and Population Data Services Agency (DPDSA) has published a specific Code of Conduct for the provision of certification services in accordance with the Personal Data Act.

9 Applicable law, dispute resolution and compensation policy

The Digital and Population Data Services Agency's (DPDSA's) liability for damages related to the provision of certificate services is determined in accordance with the provisions of the Tort Liability Act (412/1974). The requirements laid down in the Act on Strong Electronic Identification and Trust Services (617/2009) and the Act on Electronic Services and Communication in the Public Sector (13/2003) also apply to the DPDSA.

10 Certification Authority audits

As a supervisor of Certification Authorities (CAs) issuing qualified certificates, the Finnish Transport and Communications Agency (Traficom) may audit the CA's operations. The Digital and Population Data Services Agency (DPDSA) may audit its technical suppliers as specified in

technical supply agreements entered into with them. Audits take place at least once a year and always at the beginning of a new contractual period.

The aim of audits is to determine whether the technical supplier operates in compliance with the agreement considering the requirements set by information security standards. As a rule, technical suppliers are assessed on the basis of the ISO 27001 standard.

Audits are conducted by the DPDSA's information security manager and an external auditor commissioned by the DPDSA who is specialised in the auditing of technical suppliers related to certificate services. Audits take place taking the implementation of the eight elements of information security into consideration. The information security aspects audited are confidentiality, integrity and availability. Audits cover the regulations issued by Traficom for the CA regarding information security.

Audits assess the policy and application instructions against the functioning of the entire certificate organisation and system. The DPDSA is responsible for the conformity of application instructions with the Certificate Policy.