PKI DISCLOSURE STATEMENT ROOT CERTIFICATE

For the root certification authority of the Digital and Population Data Services Agency

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

VERSION MANAGEMENT		
Version no	Action	Date/author
v 1.0	Approved version v 1.0., published on 14 December 2017 www.vrk.fi	14/12/2017
v.1.1	Updated version	18.6.2019
v 1.2	Updated version, Centre name change.	1.1.2020

Contents

PKI DISCLOSURE STATEMENT ROOT CERTIFICATE

1 Introduction

This document describes on a general level how the Digital and Population Data Services Agency, which acts as the root certification authority, issues (VRK Gov. Root CA - G2) CA certificates.

This document describes the practices applied by the certification authority and the terms and conditions governing the use of the CA certificate and the restrictions on its use.

This document contains references to the following documents:

Certificate policy for the Digital and Population Data Services Agency's CA certificates, OID 1.2.246.517.1.10.201.

Certification practices for the following sub-certificates:

VRK Gov. CA for Citizen Certificates - G3, OID: 1.2.246.517.1.10.201.1

VRK CA for Organisational Certificates - G3, OID: 1.2.246.517.1.10.201.2

VRK CA for Temporary Certificates - G2, OID: 1.2.246.517.1.10.201.3

VRK CA for Service Providers - G4, OID: 1.2.246.517.1.10.201.4

VRK CA for Social Welfare and Healthcare Prof. Certs, OID: 1.2.246.517.1.10.201.5

VRK CA for Social Welfare and Healthcare Prof. Temp. Certs, OID: 1.2.246.517.1.10.201.6

VRK CA for Social Welfare and Healthcare Service Providers – G2, OID: 1.2.246.517.1.10.201.7

VRK CA for Time Stamp Services, OID: 1.2.246.517.1.10.201.8

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

2 PKI disclosure statement

2.1 Certification authority's contact details

Questions regarding this Certificate Policy should be addressed to:

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

2.2 Certificate type, verification procedure and intended use

A CA certificate is a certificate issued by the Digital and Population Data Services Agency used to grant end user certificates.

CA certificates are applied from the Digital and Population Data Services Agency.

Before issuing a certificate, the Digital and Population Data Services Agency checks the information supplied by the applicant, e.g. from the trade register.

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.

Both private and public organisations may apply for the CA certificate.

2.3 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 relying party cannot trust the certificate in good faith if its validity has not been checked against the revocation list. Before accepting certificates, the relying party must check that they are not on the revocation list.

2.4 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 CA certificate.

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. 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 trusting the certificate.

2.6 Limitations of liability

The Digital and Population Data Services Agency's liability for damages in connection with certificate service provision is determined on the basis of the Tort Liability Act (412/1974). 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. 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 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 perform modifications or maintenance. Modifications and maintenance concerning 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. You should make the revocation request immediately after you have noticed the reason for making the request.

2.7 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. When applying for the certificate, the applicant accepts the rules and conditions pertaining to certificate use and undertakes to protect the 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.

When a certification authority issues a CA certificate, it also approves the application for a 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 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 in certificate production.

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

2.8 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.

2.9 Compensation policy

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. Where applicable, the provisions of the Tort Liability Act (412/1974) also apply.

2.10 Applicable law and resolution of disputes

Provisions on identification and trust services are set out in the Act on Strong Electronic Identification and Trust Services (617/2009) Provisions on the certificates issued by the Digital and Population Data Services Agency are contained in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009).

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. Where applicable, the provisions of the Tort Liability Act (412/1974) also apply.

2.11 Audits of the certification authority

Finnish Transport and Communications Agency (Traficom) 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. 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 Management or an external auditor commissioned by the Digital and Population Data Services Agency, who specialises in auditing technical vendors pertaining to certificate services. 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 organisation and system. The Digital and Population Data Services Agency is responsible for ensuring that the application instructions are consistent with the certificate policy.