PKI Disclosure Statement

Company:	*Certipost*
Version:	*1.0*
Status:	*Final*
Rel. Date:	*07/06/2017*

Table of contents

1 Summary

The purpose of this PKI Disclosure Statement (PDS) is to summarize and present the key points of the Certificate Practice Statements and specific conditions in a more readable and understandable format for the benefit of Subscribers and Relying Parties.

This PDS does not substitute or replace the Certification Practice Statements under which digital certificates are issued.
Reader must read the CPS published at repository.eid.belgium.be before applying for or relying on a certificate.

The structure of this document is aligned with ETSI TS 101 456 B.2 “The PDS Structure”.

2 CA contact information

Queries regarding this PKI Disclosure Statement shall be directed at:

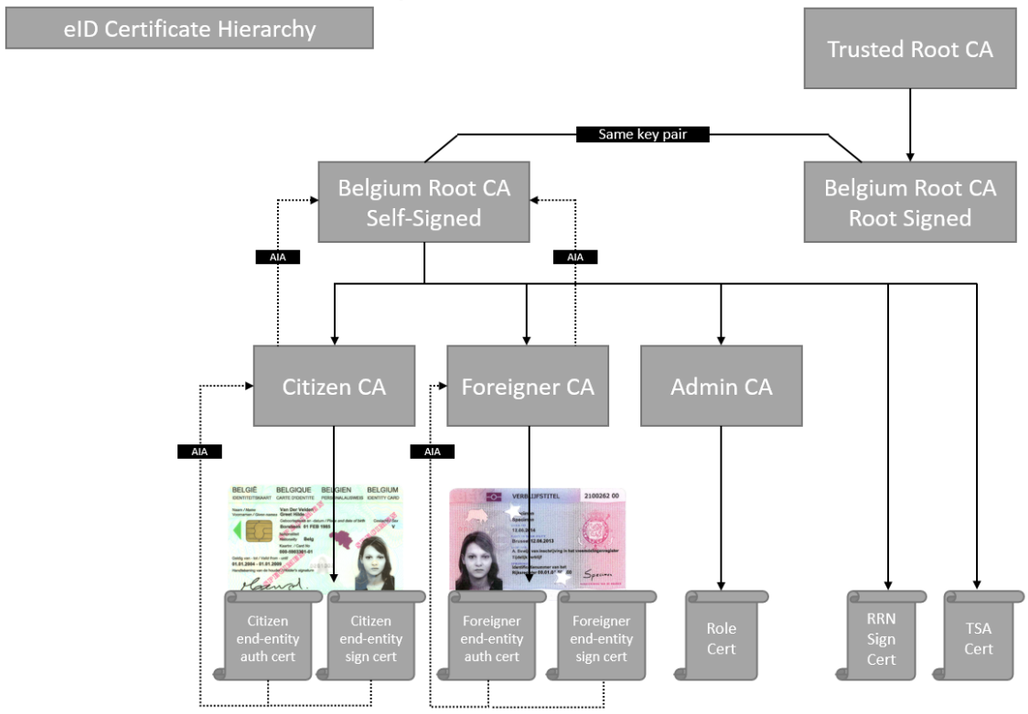
Certipost nv / sa
Policy administration - Citizen CA
Muntcentrum / Centre Monnaie
1000 Brussels

3 Type of certificates, validation procedures and certificate usage

Within the Belgian PKI there are three types of issuing CA (excl. the Belgian Root CA’s). Each type of Issuing CA can only issue Digital Certificates with approved Digital Certificate profiles (https://stage-pki.belgium.be/resources/) for that allowed type. For each type of Digital Certificate issued, a short description is provided on the registration, validation, and usage. Below is an overview of the three types of issuing CA’s with the types of certificates they can issue:

- Citizen CA
  - Citizen authentication certificate
  - Citizen digital signature certificate
- Foreigner CA
  - Foreigner authentication certificate
  - Foreigner digital signature certificate

The structure of the eID PKI hierarchy is as follows:



Initial registration:

The Registration Authorities (RA) are the Belgian local municipalities. When a citizen or foreigner applies for an eID, he needs to be physically present in the local municipality. After successful identification by the municipality, it will request two certificates (authentication & digital signature) to be issued by respectively the Citizen CA or Foreigner CA. Once the certificates have been issued by the CA, the private key and public certificate are put on the electronic chip of an eID PIN-protected smartcard. The identity information is also visibly present on the eID card.

Certificate purpose:

In this section we discuss the purpose for the existing end-entity certificates within the Belgian eID:

- (Citizen/Foreigner) Authentication Certificate:
- (Citizen/Foreigner) Digital Signature Certificate:

For a more detailed description, we refer to the CP/CPS statement for each respective Certificate Authority.

4 Limitation of the use of the reliability of certificates (Reliance limits)

The CSP does not impose reliance limits for certificates issued under this policy.

5 Obligations for subscribers

Unless otherwise stated in this CPS, citizen's obligations include the ones below:

- Refraining from tampering with a certificate;
- Only using certificates for legal and authorised purposes in accordance with the CPS;
- Applying for a new Electronic Identity Card (and thus Citizen Certificates) in case of any changes in the information published in the certificate;
- Refraining from using the citizen's public key in an issued Citizen Certificate to have other certificates issued;
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private keys;
- Notify the police, the municipality or the RA Helpdesk to request the suspension of a certificate in case of the suspicion of an occurrence that materially affects the integrity of a certificate. Such occurrences include indications of loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Citizen Certificates;
- Notify the police, the municipality or the RA Helpdesk to request the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate. Such occurrences include loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Citizen Certificates, or in case control over private keys has been lost due to compromise of activation data (e.g. PIN code);
- Obligation to exercise reasonable care to avoid unauthorised use of the subscriber's private key;
- Following compromise, the obligation to immediately and permanently discontinue the use of the subject's private key;
- The obligation to notify without any reasonable delay in case control over the private key has been lost due to compromise of activation data (e.g. PIN code).

6 Obligations of the relying parties for the verification of the certificate status

A party relying on a CA certificate will:

- Be sufficiently informed about the use of digital certificates and PKI;
- Receive notice and adhere to the conditions this CPS and associated conditions for relying parties;
- Validate a certificate by using a CRL, delta CRL, OCSP or web based certificate validation in accordance with the certificate path validation procedure;
- Trust a certificate within its validity period only if it has not been suspended or revoked;
- Rely on a certificate, as may be reasonable under the circumstances.

It is the sole responsibility of the relying parties accessing information featured in the CA Repositories and web site to assess and rely on information featured therein.

If a relying party becomes aware of or suspects that a private key has been compromised it will immediately notify the RA Helpdesk.

7 Exclusion and liability limitation clauses

.

The liability of the CSP towards the subscriber or a relying party is limited to paying damages amounting to 2500 € per transaction, affected by the events listed in this section here below.

QUALIFIED CERTIFICATES

As far as the issuance of Qualified Certificates is concerned, Article 14 of the Electronic Signatures Law governs the liability of the CSP.

Following this provision, the CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

a. as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

b. for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the private key corresponding to the public key given or identified in the certificate;

c. for assurance that the private key and the public key can be used in a complementary manner.

The CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the CSP proves that he has not acted negligently.

CERTIFICATES THAT CANNOT BE CONSIDERED AS QUALIFIED CERTIFICATES

The general rules on liability apply with regard to any damage caused to any entity or legal or natural person who reasonably relies on a certificate issued by the CSP.

The CSP explicitly declines all liability towards relying parties in all cases where the Identification Certificate is used in the context of applications allowing the use of the Identification Certificate for the generation of electronic signatures.

Excluded Liability

The CSP shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorised disclosure or unauthorised use of the Digital Certificate or any password or activation data used to control access thereto;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or Organisation;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this Citizen CA CP/CPS and/or the relevant Certificate Holder Agreement or any applicable law or regulation;

- If the Private Key associated with the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised;
- If the Digital Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation;
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that Certipost uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;
- Power failure, power interruption, or other disturbances to electrical power, provided Certipost uses commercially reasonable methods to protect against such disturbances;
- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of Certipost and/or its subcontractors or service providers;
- One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which Certipost is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of Certipost.

8 Applicable agreements, certification practice statement, certificate policy

This PKI Disclosure Statement serves as a summary for the certification practice statements (CPS's) and refers to other operational documentation for more details concerning request and validation procedures.

9 Data protection

For the Root CA, the key custodian's each have a part of the activation key, these tokens are protected by a passphrase. The protection scheme is M OF N. The tokens are stored in a vault.

The operational CA's are protect by a split operational token that (M of N) tokens are protected by passphrase. Tokens are stored in a vault.

The subscriber's key is protected by a PIN, the PIN is delivered by means of a postal service in a secured envelope directly to the subscriber. Activation Data should be memorised, not written down. Activation Data must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g. a Certificate Holder's personal information.

10 Reimbursement directives

Not applicable.

11 Governing Law and settlement of disputes clauses

All services concerning certificates are governed exclusively by Belgian law.

12 CA and certificate directory licenses, confidentiality trademarks and audit

With regard to the Qualified Certificate for electronic signature, the CSP operates following the terms of EU 910/2014 that stipulates the legal framework of electronic signatures in Belgium.

The CSP meets the requirements set out in ETSI policy documents referring to qualified certificates, including:

- EN 319 411-2 Policy requirements for certification authorities issuing qualified certificates;
- EN 319 412-5 Profiles for Trust Service Provider issuing Certificates; Qualified certificate profile. Part 5: Extension for Qualified certificate profile.

With regard to the Identification certificate, the CA meets the requirements set out in ETSI policy documents referring to public key certificates, including:

- EN 319 411-3 Policy requirements for certification authorities issuing public key certificates (Normalised level).

The CSP accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS. The CSP accepts this auditing of its own practices and procedures it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by:

- The supervising authority for Certification Service Providers in Belgium acting under the authority of the Belgian government.
- The Belgian government or a third party appointed by the Belgian government.

The CSP evaluates the results of such audits before further implementing them.

13 Abbreviations and Terms

CA	Certification Authority
CC	Common Criteria
CM	Card Manufacturer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CSPKI	Country Signing Public Key Infrastructure
CVRA	Country Verifying Registration Authority
CVCA	Country Verifying Certification Authority
EAC-PKI	Extended Access Control Public Key Infrastructure
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ICAO	International Civil Aviation Organisation
IS	Inspection System
MRTD	Machine-Readable Travel Document
OID	Object Identifier
RA	Registration Authority

14 Document Information

Version history
This PKI Disclosure statement has the following revisions:

Version	Date	Status	Description
1.0	07/06/2017	final	Bart/Don