Belgian eID
PKI Disclosure Statement

Company:	*Certipost*
Version:	*2.6*
Status:	*FINAL*
Rel. Date:	*03/02/2021*

Document Control

Date	Version	Editor	Change
13/02/2017	1.0	Bart Eeman	Initial version
28/08/2017	2.1	Cristof Fleurus	Quality Review
29/08/2017	2.2	Don Giot	Update
29/08/2017	2.3	Cristof Fleurus	Quality Review
01/08/2019	2.4	Guillaume Nguyen	Update
15/10/2020	2.5	Bart Eeman	Update
20/01/2021	2.6	Bart Eeman	Update

Table of contents

Document Control 1
Table of contents 3
1. Summary 4
2. CA contact information 4
3. Type of certificates, validation procedures and certificate usage 4
4. Limitation of the use of the reliability of certificates (Reliance limits) 6
5. Obligations for subscribers 6
6. Obligations of the relying parties for the verification of the certificate status 7
7. Exclusion and liability limitation clauses 7
8. Applicable agreements, certification practice statement, certificate policy 9
9. Data protection 9
10. Reimbursement directives 9
11. Governing Law and settlement of disputes clauses 9
12. CA and certificate directory licenses, confidentiality trademarks and audit 10
13. Abbreviations and Terms 11

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.

The reader must read the CPS published at https://repository.eid.belgium.be/ before applying for or relying on a certificate.

The structure of this document is aligned with ETSI TS 101 456 Annex 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 / Foreigner CA
Muntcentrum / Centre Monnaie
1000 Brussels

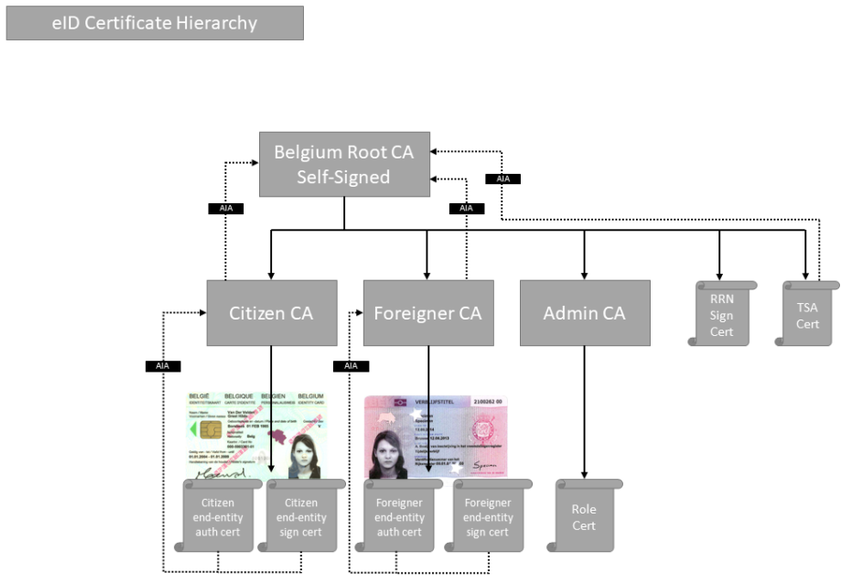
3 Type of certificates, validation procedures and certificate usage

Within the Belgian eID PKI, multiple types of issuing CAs (excl. the Belgian Root CA’s) have been defined. 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 two types of issuing CA’s with the types of certificates they can issue:

- **Citizen CA**
  - Citizen authentication certificate
  - Citizen electronic signature certificate
- **Foreigner CA**
  - Foreigner authentication certificate
  - Foreigner electronic signature certificate

3.1 The eID Hierarchy

The structure of the eID PKI hierarchy is as follows:



3.2 Initial registration for an electronic identity card

The RRN (National Register) acts as Registration Authority (RA) together with the Belgian local municipalities who are the Local Registration Authorities (LRA). When the subject (i.e. the citizen or foreigner) applies for an Electronic Identity Card (eID), the LRA will perform the identification of the subject according to the procedures and regulations applicable to the delivery of eID's. This identification process requires the subject to be physically present at the LRA.

After the identification, the LRA's request certificates for the subjects. This is an integral part of the applied enrolment process for the Electronic Identity Card. After this initial certificate request, private keys are generated on secure signature smartcards in accordance with European and Belgian Signature law. The Card manufacturer is responsible for securing the smart card on which the Qualified Signature Creation Device (QSCD) resides with a Personal Identification Number (PIN).

Following approval of the certificate application, the RA sends a certificate issuance request to the CA. If the requirements for the certificate issuance request have been fulfilled (cfr. CPS) the CA issues the certificate and delivers it to the RA.

The RA requests the Card Manufacturer to load the issued certificates on the Electronic Identity Card. The Card Manufacturer delivers the Electronic Identity Card securely with the certificates to the LRA, after which the subject can retrieve his eID card with the LRA.

3.3 Certificate purpose

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

- (Citizen/Foreigner) Authentication Certificate: The authentication certificate is used to authenticate the citizen in online applications using TLS Client Authentication.

- (Citizen/Foreigner) Electronic Signature Certificate: The electronic signature certificate is used for non-repudiation and is capable of generating a qualified electronic signature.

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 liability of the TSP towards the subscriber or a relying party is limited to paying damages amounting to 2500 € per transaction, affected by the events listed in section 7.

5 Obligations for subscribers

Unless otherwise stated in this PDS or the published Citizen / Foreigner CPS, the subject's obligations include the ones below:

- Refraining from tampering with a certificate;
- Only using certificates for legal and authorized purposes in accordance with the CPS;
- Applying for a new Electronic Identity Card (and thus Citizen or Foreigner Certificates) in case of any changes in the information published in the certificate;
- Refraining from using the subject's public key in an issued Citizen/Foreigner Certificate to have other certificates issued;
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized 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, unauthorized disclosure, or other compromise of the private key of one or both of the Citizen / Foreigner 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, unauthorized disclosure, or other compromise of the private key of one or both of the Citizen / Foreigner 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 unauthorized 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 the Citizen / Foreigner 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 is compromised, it will immediately notify the RA Helpdesk.

7 Exclusion and liability limitation clauses

The liability of the TSP 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.

7.1 Qualified certificates

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

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

- 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;
- 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;
- For assurance that the private key and the public key can be used in a complementary manner.

The TSP 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 TSP proves that he has not acted negligently.

7.2 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 TSP.

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

7.3 Excluded Liability

The TSP 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 unauthorized disclosure or unauthorized 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 Organization;
- 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 the Citizen / Foreigner 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 labor 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 (Citizen / Foreigner CPS published on https://repository.eid.belgium.be/) and refers to other operational documentation for more details concerning request and validation procedures.

9 Data protection

The TSP aims to adhere to the ISO 27001 & ISO 27002 information security standards for defining and implementing operational controls.

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 TSP operates following the terms of the EU Regulation N°910/2014 that defines the legal framework for electronic signatures in Belgium.

The TSP meets the requirements set out in ETSI policy documents and other relevant standards referring to qualified certificates, including:

- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QcStatements.
- RFC 3647 Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices;
- RFC 5280 Internet X.509 Public Key Infrastructure - Certificate and CRL Profile;
- RFC 6818 Update to the RFC 5280;
- RFC 3739 Internet X.509 Public Key Infrastructure - Qualified Certificates Profile;
- RFC 6960 X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP;
- The ISO/IEC 27001 standard on information security and infrastructure.

The TSP accepts compliance audits to ensure it meets requirements, procedures and service levels according to the contractual requirements, and relevant industry standards. The TSP accepts auditing of its own practices and procedures. It does not publicly disclose the results of the audit if it would compromise confidentiality or disclose trade secrets, etc. Such audits may be carried out directly or through an agent by:

- The supervising authority for Trust 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 TSP 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
TSPKI	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