CIe Belge
Déclaration de divulgation PKI

Company:	*Certipost*
Version:	*1.0*
Status:	*FINAL*
Rel. Date:	*07/09/2017*

Document Control

Date	Version	Editor	Change
30/08/2017	1.0	Cristof Fleurus / Don Giot	Version Initial

Notice légale:

Cette notice légale est valable pour la "Déclaration des Pratiques de Certification" (CPS) et la "Déclaration de Divulgation PKI" (PDS). Le présent document est une traduction française du document original rédigé en anglais et publié sur le site https://repository.eid.belgium.be/. Cette version française du document constitue une source d'informations. La version anglaise du CPS est la seule version officielle du document susceptible de faire naître des obligations juridiquement contraignantes. Dans le cas où le présent document devait différer de la version anglaise du CPS, en cas de doute, ou si la version française du document est antérieure à la version anglaise du CPS tel que publiée, seule la dernière version anglaise publiée du CPS prévaudra.

Table des matières

1 Résumé

Le but de cette déclaration de divulgation PKI (PKI Disclosure Statement - PDS) est de résumer et de présenter les points clés des Déclarations de pratique de certification (Certification Practice Statement - CPS) et des conditions spécifiques dans un format plus lisible et compréhensible au profit des usagers et des parties confiantes.

Cette PDS ne remplace pas et ne se substitue pas aux Déclarations de pratique de certification en vertu desquelles les certificats numériques sont délivrés.
Le lecteur doit lire la CPS publiée sur https://repository.CIe.belgium.be avant de solliciter un certificat ou de s'y fier.

La structure de ce document est en adéquation avec ETSI TS 101 456 Annex B.2 “The PDS Structure”.

2 Informations relatives au contact CA

Les requêtes relatives à cette Déclaration de divulgation PKI doivent être adressées à :

Certipost sa
Administration de la Politique – Citizen / Foreigner CA
Centre Monnaie
1000 Bruxelles

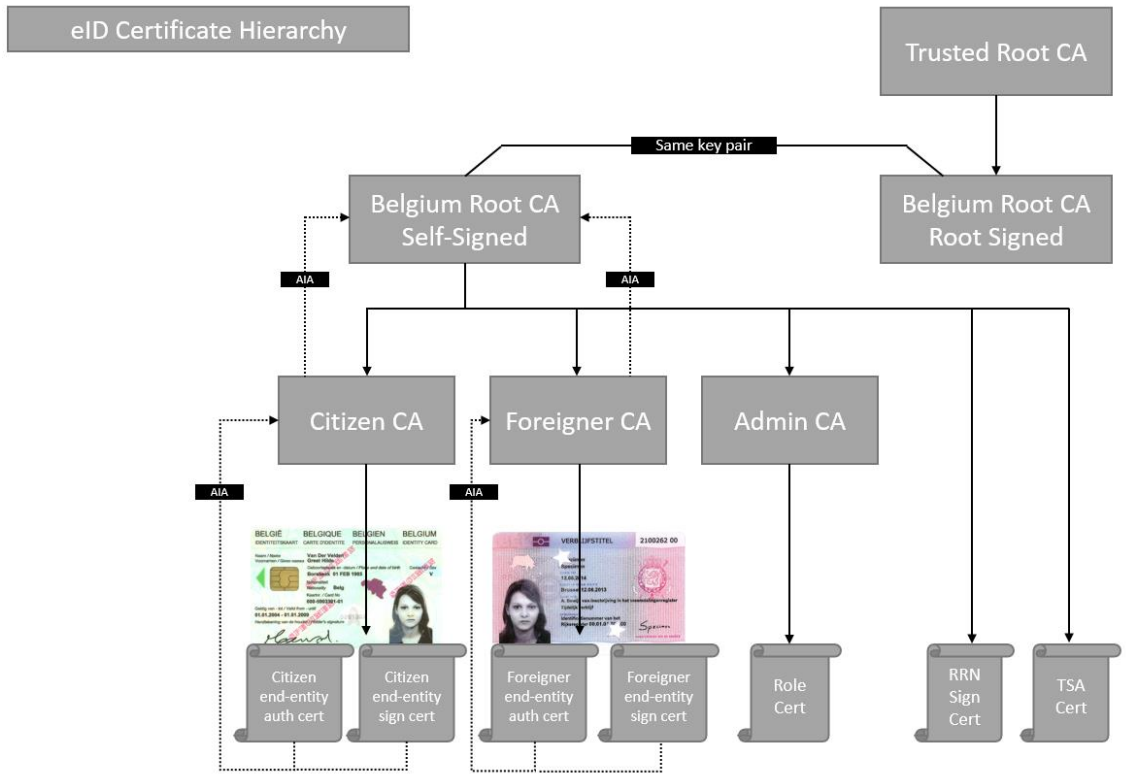
3 Type de certificats, procédures de validation et l'utilisation du certificat

Au sein du PKI belge, il existe plusieurs de types de CA émettrice (hors CA racines belges). Chaque type de CA émettrice peut uniquement émettre des certificats numériques avec des profils approuvés de certificat numérique (https://stage-pki.belgium.be/resources/) pour ce type autorisé. Pour chaque type de certificat émis, une brève description est fournie sur l'enregistrement, la validation et l'utilisation. Vous trouverez ci-dessous un aperçu des deux types de CA émettrices avec les types de certificats qu'elles peuvent émettre :

- Citizen CA
  - Certificat d'authentification citoyen
  - Certificat de signature électronique citoyen
- Foreigner CA
  - Certificat d'authentification étranger
  - Certificat de signature électronique étranger

3.1 La hiérarchie PKI CIe

La structure de la hiérarchie PKI CIe est la suivante :



3.2 Enregistrement initial: Pour une carte d'identité électronique

Le Registre National (RRN) agit en tant qu'autorité d'enregistrement (RA) avec les municipalités locales belges qui sont les autorités locales d'enregistrement (LRA). Lorsque le sujet (c'est-à-dire le citoyen ou l'étranger) demande une carte d'identité électronique (CIe), la LRA effectuera l'identification du sujet conformément aux procédures et règlements applicables à la livraison des CIE. Ce processus d'identification exige que le sujet soit physiquement présent à la LRA.

Après l'identification, la LRA demande des certificats pour les sujets. Ceci fait partie intégrante du processus d'inscription appliqué pour la carte d'identité électronique. Après cette demande de certificat initiale, les clés privées sont générées sur des cartes à puce de signature sécurisée conformément à la loi Signature européenne et belge. Le fabricant de la carte est responsable de la sécurisation de la carte à puce sur laquelle se trouve le périphérique de création de signature qualifié (QSCD) avec un numéro d'identification personnel (NIP).

Après l'approbation de la demande de certificat, la RA envoie une demande d'émission de certificat à l'autorité de certification. Si les exigences relatives à la demande d'émission de certificat ont été remplies (cfr. CPS), l'autorité de certification émet le certificat et le délivre à la RA.

La RA demande au fabricant de la carte de charger les certificats délivrés sur la carte électronique d'identité. Le fabricant de la carte fournit la carte d'identité électronique en toute sécurité avec les certificats à la LRA, après quoi le sujet peut récupérer sa carte CIe avec la LRA.

3.3 But du certificat:

Dans cette section, nous traitons de l'objectif des certificats d'entité finale existants dans l'CIe belge:

- Certificat d'authentification (Citoyen/Étranger): Le certificat d'authentification est utilisé pour authentifier le citoyen ver les applications en ligne utilisant TLS Client Authentication.
- Certificat de signature (Citoyen/Étranger): Le certificat de signature est utilisé pour la non-répudiation et est capable de générer une signature électronique qualifiée.

Pour une description plus détaillée, nous nous référons à la déclaration CP/CPS pour chaque Autorité de certification respective.

4 Limitation de l'utilisation de la fiabilité des certificats (limites de dépendance)

La responsabilité du TSP à l'égard du souscripteur ou d'une partie confiante est limitée au paiement de préjudices s'élevant à 2 500 € par transaction, affectée par les événements repris dans la section 7.

5 Obligations pour les usagers

Sauf si mentionner autrement dans la PDS ou la CPS citoyenne / étrangère publiée, les obligations du sujet impliquent ce qui suit:

- s’abstenir de falsifier un certificat ;
- utiliser uniquement des certificats à des fins légales et autorisées, conformément à la CPS ;
- demander une nouvelle carte d’identité électronique (et donc des certificats de citoyen ou de étranger) en cas de modification des informations publiées dans le certificat ;
- s’abstenir d’utiliser la clé publique de sujet dans un certificat de citoyen / étranger délivré, pour la délivrance d’autres certificats ;
- prévenir la compromission, la perte, la divulgation, la modification ou toute utilisation illicite de ses clés privées ;
- avertir la police, l'administration communale ou le Helpdesk de la RA et demander la suspension d’un certificat dans le cas où l'on suspecte ou où se produit un incident portant matériellement atteinte à l’intégrité d’un certificat. Ces incidents incluent des indications de perte, vol, modification, divulgation non autorisée ou autre compromission de la clé privée d’un des certificats de citoyen ou d’étranger, ou des deux ;

- avertir la police, l'administration communale ou le Helpdesk de la RA et demander la révocation d'un certificat dans le cas où l'on suspecte ou où se produit un incident portant matériellement atteinte à l'intégrité d'un certificat. Ces incidents incluent la perte, le vol, la modification, la divulgation non autorisée ou la compromission de la clé privée d'un des certificats de citoyen ou d'étranger, ou des deux, ou dans le cas où le contrôle de la clé privée a été perdu suite à une compromission des données d'activation (par ex. code PIN) ;
- obligation d'exercer une diligence raisonnable pour éviter une utilisation non autorisée de la clé privée de l'usager ;
- dès compromission, l'obligation d'arrêter immédiatement et définitivement l'usage de la clé privée ;
- obligation de notifier le Helpdesk RA sans délai en cas de perte de contrôle de la clé privée à la suite d'une compromission de données d'activation (par ex. code PIN).

6 Obligations des parties confiantes pour la vérification du statut du certificat

Les parties se fiant sur un certificat de la CA:

- seront suffisamment informées sur l'utilisation de certificats numériques et PKI ;
- seront informées et adhèreront aux conditions de CPS de citoyen / étranger, ainsi qu'aux conditions associées pour les parties confiante ;
- validera un certificat à l'aide d'une CRL, d'une Delta CRL, d'un OCSP ou d'une procédure de validation de certificat Internet, conformément à la procédure de validation du chemin du certificat ;
- ne se fieront à un certificat que s'il n'a pas été suspendu ou révoqué;
- se fieront à un certificat de manière raisonnable en fonction des circonstances.

Les parties accédant aux informations reprises dans les référentiels, ainsi que sur le site Web de la CA sont seules responsables de l'évaluation de ces informations et du crédit qu'elles leur accordent.

Si une partie se fiant au certificat prend connaissance de ou soupçonne la compromission d'une clé privée, elle en avertira immédiatement le Helpdesk de la RA.

7 Clause d'exclusion et de limitation de responsabilité

La responsabilité du TSP à l'égard du souscripteur ou d'une partie confiante est limitée au paiement de préjudices s'élevant à 2 500 € par transaction, affectée par les événements repris dans la section ci-dessous.

7.1 Certificats qualifiés

En ce qui concerne la délivrance de certificats qualifiés, l'article 14 de la loi sur les signatures électroniques régit la responsabilité du TSP.

Conformément à cette disposition, le TSP est responsable du préjudice causé à tout organisme ou toute personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de :

a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié ;

b) l'assurance que, au moment de la délivrance du certificat qualifié, le signataire identifié dans le certificat qualifié détenait la clé privée correspondant à la clé publique donnée ou identifiée dans le certificat ;

c) l'assurance que la clé privée et la clé publique peuvent être utilisées de façon complémentaire ;

Le TSP est responsable de tout préjudice causé à tout organisme ou personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat, sauf si le TSP prouve qu'il n'a commis aucune négligence.

7.2 Certificats qui ne peuvent pas être considérés comme des certificats qualifiés

Les règles générales en matière de responsabilité s'appliquent à tout préjudice causé à un organisme ou une personne physique ou morale qui se fie raisonnablement à un certificat délivré par le TSP.

Le TSP décline explicitement toute responsabilité à l'égard de parties confiantes dans tous les cas où le certificat d'authentification est utilisé dans le contexte d'applications permettant l'utilisation du certificat d'identification pour la génération de signatures électroniques.

7.3 Responsabilité exclue

Le TSP n'est en aucun cas responsable de quelque perte que ce soit impliquant ou résultant d'une (ou plusieurs) circonstance(s) suivantes ou cause(s):

- si le certificat numérique détenu par la partie demanderesse ou si l'objet d'une réclamation a été compromis par la divulgation non autorisée ou l'utilisation non autorisée du certificat numérique ou des données de mot de passe ou d'activation utilisées pour contrôler l'accès à celui-ci;
- si le certificat numérique détenu par la partie demanderesse ou si l'objet d'une réclamation fait suite à une fausse déclaration, erreur de fait ou omission de toute personne, entité ou organisation;
- si le certificat numérique détenu par la partie demanderesse ou si l'objet de toute réclamation a expiré ou est révoqué avant la date des circonstances donnant lieu à toute réclamation;
- si le certificat numérique détenu par la partie demanderesse ou si l'objet d'une réclamation a été modifié ou altéré de quelque façon que ce soit ou a été utilisé autrement qu'aux fins autorisées par les conditions de cette Citizen CA CP/CPS et/ou le contrat du titulaire du certificat concerné ou toute loi ou réglementation applicable;
- si la clé privée associée au certificat numérique détenu par la partie demanderesse ou si l'objet d'une réclamation est compromis;

- si le certificat numérique détenu par la partie demanderesse a été émis d'une manière qui constitue une violation de toute loi ou réglementation applicable ;
- le matériel informatique, des logiciels ou des algorithmes mathématiques développés ayant tendance à rendre la cryptographie de la clé publique ou les crypto systèmes asymétriques moins sécurisés, à condition que Certipost utilise des pratiques commercialement raisonnables pour se protéger des atteintes à la sécurité résultant d'un tel matériel informatique, de logiciels ou d'algorithmes ;
- panne de courant, coupure de courant ou d'autres perturbations à l'alimentation électrique, à condition que Certipost utilise des méthodes commercialement raisonnables pour se prémunir contre de telles perturbations ;
- défaillance d'un ou plusieurs systèmes informatiques, de l'infrastructure de communication, du traitement ou du stockage des médias ou des mécanismes, ou des sous-composantes de la précédente, et non sous le contrôle exclusif de Certipost et / ou ses sous-traitants ou fournisseurs de services ;
- un ou plusieurs des événements suivants : une catastrophe naturelle ou un cas de force majeure (y compris, sans limitation, inondation, tremblement de terre ou autre cause d'ordre naturelle ou climatique) ; une perturbation du travail ; guerre, insurrection ou hostilités miliaires manifestes ; législation défavorable ou action gouvernementale, l'interdiction, embargo ou boycott ; émeutes ou troubles à l'ordre public ; incendie ou explosion ; épidémie catastrophique ; embargo commercial ; restriction ou empêchement (y compris, sans limitation, les contrôles à l'exportation) ; un manque de disponibilité ou d'intégrité des télécommunications ; obligation légale, y compris tout jugement d'une juridiction compétente dont relève Certipost, ou peut-être, sous réserve ; toute occasion ou tout événement ou toute circonstance ou ensemble de circonstances échappant au contrôle de Certipost.

8 Accords applicables, déclaration de pratique de certification, politique de certificat

Cette déclaration de divulgation PKI sert de résumé pour les déclarations de pratique de certification (CPS) et fait référence à d'autres documents opérationnels pour plus de détails concernant les procédures de demande et de validation.

9 Protection des données

Le TSP vise à respecter les normes de sécurité d'information ISO 27001 & ISO 27002 pour définir et mettre en œuvre des contrôles opérationnels.

10 Directives de remboursement

Non applicables.

11 Droit applicable et règlement des litiges

Tous les services concernant les certificats sont régis exclusivement par le droit Belge.

12 Licences de répertoire CA et de certificat, marques de confidentialité et audit

En ce qui concerne le certificat qualifié pour la signature électronique, le TSP procède selon les termes du règlement UE 910/2014 qui établit le cadre légal des signatures électroniques en Belgique.
Le TSP répond aux exigences définies dans les documents de politique ETSI qui se réfèrent aux certificats qualifiés, y compris :

- 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
- EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

  Part 5: QcStatements

Le TSP accepte les audits de conformité afin de s'assurer qu'il respecte les exigences, normes, procédures et niveaux de service conformément aux exigences contractuelles et les normes sectorielles pertinentes. Le TSP accepte cette vérification de ses propres pratiques et procédures qu'il ne divulgue pas publiquement sous certaines conditions, comme la confidentialité, les secrets commerciaux, etc. De tels audits peuvent être réalisés directement ou via un agent par :

- L’autorité de supervision des prestataires de services de certification en Belgique qui agit sous l'autorité de l’Autorité fédérale belge.
- Le Gouvernement fédéral belge ou une tierce partie désignée par le Gouvernement fédéral belge.

Le TSP évalue les résultats de ces audits avant de les mettre en application.

13 Abréviation et termes

CA	Autorité de certification (Certification Authority)
CC	Critères communs
CIe	Carte Identité Electronique
CM	Fabricant de cartes (Card Manufacturer)
CP	Politique de certificat (Certificate Policy)
DPC / CPS	Déclaration de Pratiques de Certification (Certification Practice Statement)
CRL	Liste de révocation de certificats (Certificate Revocation List)
(L)RA	Autorité d'enregistrement (locale) ((Local) Registration Authority)
TSP	Trust Service Provider