Politique belge de Certification et Déclaration de Pratique pour l'infrastructure PKI eID Foreigner CA

OIDs: **2.16.56.1.1.1.7**
2.16.56.9.1.1.7
2.16.56.10.1.1.7
2.16.56.12.1.1.7

Entreprise: *certipost*
Version: *4.5*
Statut: *Final*
Date de publication: *28/10/2019*

Contrôle du document

Date	Version	Éditeur	Changement
13/02/2017	3.0	Bart Eeman	Version initiale 1.0
15/03/2017	3.1	Bart Eeman	Version initiale 1.1
24/03/2017	3.2	Don Giot	Mise à jour de la version 1.2
10/04/2017	3.3	Bart Eeman	Ajout Zetes
13/04/2017	3.4	Bart Eeman	Remarques RRN
04/09/2017	4.0	Don Giot/Cristof Fleurus	Mise à jour eIDAS et QA
29/05/2018	4.1	Bart Eeman/Don Giot	Mise à jour de la version 4.1 et QA
13/07/2018	4.2	Bart Eeman	Révision de la version finale 2018
08/04/2019	4.4	Bart Eeman/Bono Vanderpoorten/Guillaume Nguyen	Review 2019
28/10/2019	4.5	Bart Eeman/Jonas Deckers/Guillaume Nguyen	Remarques RRN

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 eID Repository Website. 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. Introduction

La présente Déclaration des Pratiques de Certification (ci-après abrégée en «DPC», en anglais CPS pour Certification Practice Statement) décrit les pratiques de certification applicables aux certificats numériques émis pour les étrangers résidant en Belgique par le prestataire de service de confiance (ci-après dénommé « TSP ») sous l'appellation "Foreigner CA" (ci-après dénommé « CA ») et installées sur les cartes à puce électroniques destinées aux étrangers (ci-après dénommées « cartes d'identité électroniques »).

Comme décrit ci-dessus, la présente DPC constitue une déclaration publique unilatérale portant sur les pratiques auxquelles la « Foreigner CA » doit se conformer lors de la fourniture de services de certification et décrit de manière exhaustive comment la « Foreigner CA » met ses services à dispositions.

La DPC a pour premier objectif de préciser les dispositions légales et contractuelles et d'informer l'ensemble des parties intéressées au sujet des pratiques liées à la "Foreigner CA".

certipost SA se conforme à la version actuelle des Exigences de base pour l'Émission et la Gestion de Certificats reconnus publiquement ("Exigences de base") publiée sur http://www.cabforum.org. En cas de divergence entre le présent document et ces exigences, lesdites Exigences priment le présent document.

1.1 Aperçu

Actuellement, le TSP pour « Foreigner CA » est « CERTIPOST sa » (dénommé ci-après « certipost »), dont le siège social est établi au Centre Monnaie à 1000 Bruxelles, engagée à cette fin par les Autorités fédérales belges en qualité d'autorité contractante pour le projet eID, aux conditions suivantes :

CERTIPOST assume le rôle de Prestataire de Service de Confiance (abrégé en anglais « TSP ») au sens de la loi du 21 juillet 2016, du Règlement européen N 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 relatif à l'identification électronique et aux services de confiance pour les transactions électroniques au sein du marché intérieur. Au nom et pour le compte des autorités belges, CERTIPOST assume à la fois le rôle de CA et de TSP pour les Foreigner CA et est, à ce titre, responsable des certificats d'étranger émis sous l'autorité de ces CA.

Cette DPC ne doit être utilisée que dans le domaine de la CA. La DPC vise à délimiter le domaine de prestation de services de certification aux étrangers et aux parties se fiant au certificat dans le domaine de la CA. La présente DPC met également en exergue la relation entre l'Autorité de Certification (abrégée CA en anglais) et d'autres autorités de certification dans la hiérarchie PKI (public key infrastructure, infrastructure publique à clés) du Gouvernement fédéral belge comme la Belgium Root Certification Authority (BRCA). Elle décrit également la relation entre le TSP et les autres organisations impliquées dans la fourniture des certificats pour les cartes d'identité électroniques belges (ci-après les " Certificats Étranger").

La présente DPC fournit en outre des directives opérationnelles pour l'ensemble des étrangers et des parties faisant confiance au certificat, en ce compris les personnes physiques

ou morales en Belgique et à l'étranger, et d'autres autorités de Certification, comme la BRCA, relevant de la hiérarchie PKI de l'État belge dans le cadre juridique des signatures électroniques et des cartes d'identité électroniques en Belgique. De plus, cette DPC décrit les relations entre la « Foreigner CA » et l'ensemble des autres entités jouant un rôle dans le contexte de la carte d'identité électronique belge, comme le Producteur de Cartes. L'État belge acquiert ces services par le biais d'accords appropriés conclus avec ces fournisseurs tiers.

Enfin, dans une perspective d'accréditation et de supervision, cette DPC fournit une guidance pour les autorités de supervision, les organes d'accréditation, les auditeurs, etc. pour ce qui est des pratiques du TSP.

Cette « Foreigner CA DPC » avalise et instaure les normes suivantes :

- ETSI EN 319 411-1 : Politique et exigences de sécurité pour les prestataires de service de confiance délivrant des certificats ; Partie 1 : Exigences générales ;
- ETSI EN 319 411-2 : Politique et exigences de sécurité pour les prestataires de service de confiance délivrant des certificats ; Partie 2 : Exigences pour les prestataires de service émettant des certificats qualifiés UE ;
- ETSI EN 319 412-5 : Politique et exigences de sécurité pour les prestataires de service de confiance délivrant des certificats ; Partie 5 : QCStatements ;
- RFC 3647 : Internet X.509 Infrastructure publique à clés – Politique de certificat et Pratiques de certification ;
- RFC 5280 : Internet X.509 Infrastructure publique à clés – Certificat et profil CRL
- RFC 6818 : mise à jour du RFC 5280 ;
- RFC 3739 : Internet X.509 Infrastructure publique à clés – Profil de certificats qualifiés ;
- RFC 6960 : X.509 Internet Infrastructure publique à clés – Protocole de validation de certificats en ligne - OCSP (online certificate status protocol) ;
- La norme ISO/IEC 27001 en matière de sécurité et d'infrastructure.

La DPC aborde en détail les politiques et les pratiques organisationnelles, procédurales et techniques de la CA pour ce qui est de l'ensemble des services de certification offerts et ce, durant la durée de vie complète des certificats délivrés par la « Foreigner CA ». En plus de la présente DPC, d'autres documents liés au processus de certification dans le contexte de la carte d'identité électronique belge peuvent devoir être pris en compte. Ces documents seront disponibles par le biais du référentiel CA (cf. § 2 Responsabilités en matière de publication et de référentiels).

La présente DPC est conforme aux exigences formelles de l'*Internet Engineering Task Force* (IETF) RFC 3647 sur le plan du format et du contenu. Alors que certains intitulés de sections sont inclus conformément à la structure du RFC 3647, le sujet peut ne pas s'appliquer nécessairement à la mise en œuvre des services de certification de la « Foreigner CA ». Ces sections sont indiquées en tant que « Section non applicable ». Des changements éditoriaux mineurs aux prescriptions du RFC 3647 ont été insérés dans la présente DPC afin de mieux adapter la structure du RFC 3647 aux besoins de ce domaine d'application.

La présente DPC doit également être considérée comme la Politique de Certificat (Certificate Policy, CP) pour les certificats émis par l'autorité de certification “Foreigner CA”.

Concernant les autres CA utilisées par le Gouvernement belge, nous nous référons au site Internet suivant, où un lien peut être trouvé pour chaque DPC :

- Gov CA eID Repository Website
- Citizen CA eID Repository Website
- Belgium Root CA eID Repository Website

Remarque : Chacun de ces CA (Gov & Foreigner) a son propre CP/CPS.

1.2 La hiérarchie de l'eid

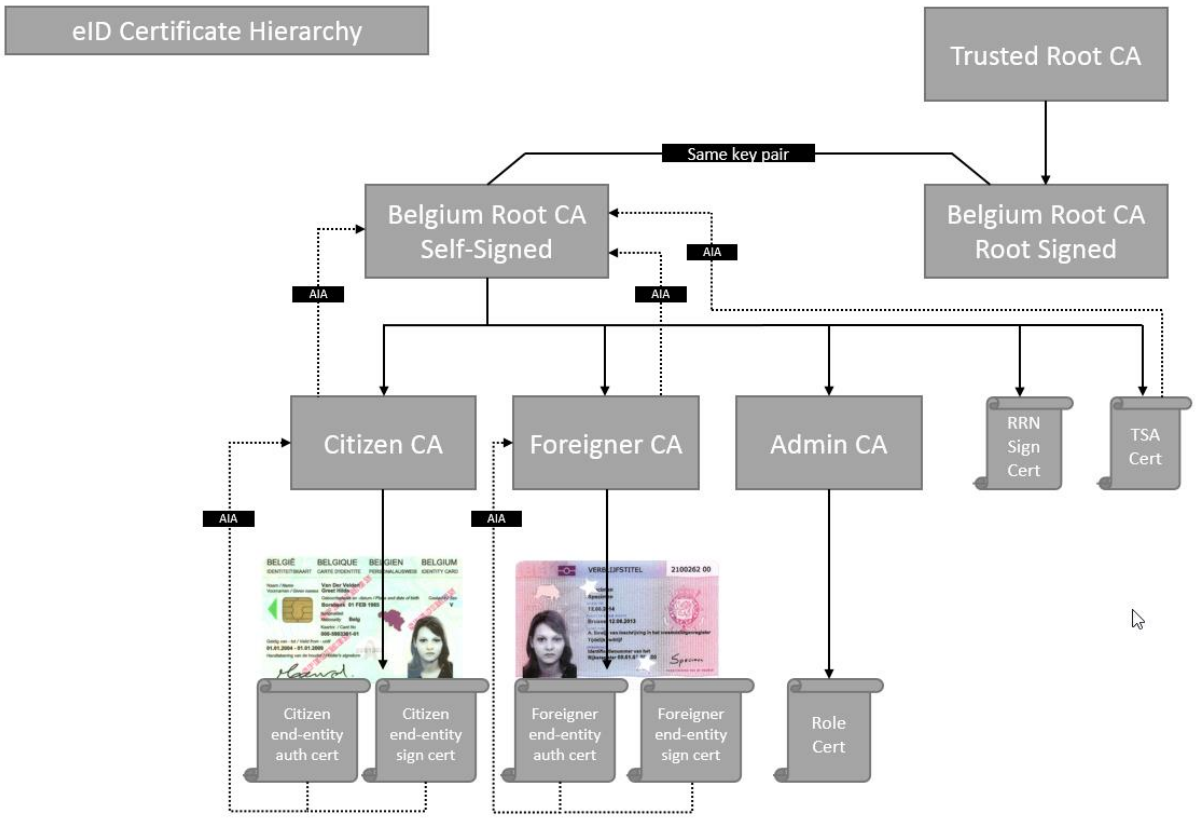

Schéma : Hiérarchie PKI eID belge

1.3 Nom et identification du document

Nom de ce document	***Politique belge de Certification et Déclaration de Pratique de certification pour l'infrastructure PKI eID Foreigner CA***
Version du document	**2.16.56.12.1.** *– v4.5* ***La présente Politique de Certification est identifiée par son nom et son numéro de version.***
	Ce document OID remplace les OID suivants ***2.16.56.1.1*** ***2.16.56.9.1*** ***2.16.56.10.1*** ***Cette Foreigner PC/DPC rend obsolètes toutes les autres versions de Foreigner PC/DPC à compter de la date de publication.***
OID renvoyant à ce document	*Les identifiants sous contrôle de certipost :* ***BRCA (1)*** *OID : 2.16.56.1.1.1.7 – Foreigner CA* *OID : 2.16.56.1.1.1.7.1 – Certificat de Signature Étranger* *OID : 2.16.56.1.1.1.7.2 – Certificat d'Authentification Étranger*
	BRCA 2 *OID : 2.16.56.9.1.1.7 – Foreigner CA* *OID : 2.16.56.9.1.1.7.1 – Certificat de Signature Étranger* *OID : 2.16.56.9.1.1.7.2 – Certificat d'Authentification Étranger*
	BRCA 3 *OID : 2.16.56.10.1.1.7 – Foreigner CA* *OID : 2.16.56.10.1.1.7.1 – Certificat de Signature Étranger* *OID : 2.16.56.10.1.1.7.2 – Certificat d'Authentification Étranger*
	BRCA 4 *OID : 2.16.56.12.1.1.7 – Foreigner CA* *OID : 2.16.56.12.1.1.7.1 – Certificat de Signature Étranger* *OID : 2.16.56.12.1.1.7.2 – Certificat d'Authentification Étranger*

1.4 Participants PKI

Plusieurs parties composent les participants de cette hiérarchie PKI. Les parties citées ci-après, y compris toutes les autorités de certification, les RA, LRA (administrations communales), les étrangers et les parties faisant confiance au certificat sont collectivement appelés les participants PKI.

1.4.1 Autorités de Certification

Une Autorité de Certification est une organisation qui émet et gère des certificats numériques correspondant à l'identité numérique.

L'autorité de certification fournit les services nécessaires pour vérifier la validité des certificats délivrés.

Au nom et pour le compte des autorités belges, CERTIPOST assume à la fois le rôle de CA et de TSP pour les Foreigner CA et est, à ce titre, responsable des certificats 'Foreigner' émis sous l'autorité de la Foreigner CA. Les autorités belges sont le TSP responsable des CA racines pour la Belgique et des certificats CA émis sous l'autorité de la CA racine pour la Belgique.

La "Foreigner CA" est une Autorité de Certification bénéficiant d'une autorisation de délivrance de certificats d'étrangers. Cette autorisation a été octroyée par la Belgium Root Certification Authority (ci-après dénommée "BRCA").

La « Foreigner CA » garantit la disponibilité de tous les services relatifs aux certificats, y compris la délivrance, la révocation, la vérification du statut et l'horodatage, dès qu'ils deviennent disponibles ou nécessaires dans des applications spécifiques.

La « Foreigner CA » est établie en Belgique. Elle peut être contactée à l'adresse publiée plus loin dans la présente DPC. En vue de la fourniture de services CA, comprenant la délivrance, la suspension, la révocation, le renouvellement, la vérification du statut de certificats, la « Foreigner CA » exploite un système sécurisé et prévoit un centre de secours en Belgique pour assurer la continuité des services CA.

Le domaine de responsabilité de la « Foreigner CA » couvre la gestion globale du cycle de vie d'un certificat, en ce compris :

- Délivrance ;
- Suspension/réhabilitation après suspension ;
- Révocation ;
- Vérification d'état (service d'état du certificat) ;
- Service de répertoire.

1.4.2 Autorités d'enregistrement

Le RRN (Registre National) et les administrations communales sont la RA au sein du domaine « Foreigner CA », à l'exclusion de tout autre organisme. Le RRN est constitué et agit en vertu des dispositions de la loi sur le Registre national et de la Loi sur les Cartes d'identité.

L'Autorité d'Enregistrement ("RA") qui, au nom et pour le compte du TSP, certifie qu'une clé publique donnée appartient à une entité déterminée (par exemple, une personne) en délivrant un certificat numérique et en le signant avec sa clé privée. Pour la carte d'identité électronique belge, le "Registre National", une administration publique relevant du Service Public Fédéral Intérieur, assume le rôle de "RA". La plupart des opérations d'enregistrement sont exécutées par les services administratifs locaux dans les administrations communales, appelées Autorités d'Enregistrement Locales (ci-après abrégé en « LRA »). Sur la base de ce processus, la RA prie la CA d'émettre un certificat.

En particulier, les RA et LRA sont responsables de :

- La validation d'identité des étrangers ;
- L'enregistrement des données à certifier ;
- L'autorisation d'émettre un certificat pour un étranger donné ;
- Veiller à ce que les certificats d'étrangers soient stockés sur la carte d'identité correcte ;
- Veiller à ce qu'un étranger reçoive la carte qu'il s'attend à recevoir et active la carte en question uniquement si celle-ci a été attribuée en bonne et due forme à l'étranger approprié ;
- La SRA (Autorité de Suspension et de Révocation) : entité qui suspend et/ou révoque les certificats conformément aux normes ETSI référencées.

1.4.3 Usager et sujet

certipost, en assumant le rôle de TSP pour le Foreigner CA, a conclu un accord contractuel avec les autorités belges. Ainsi, nous pouvons considérer le gouvernement comme « l'usager » des services CA dans le domaine « Foreigner CA ».

Les sujets des services CA au sein du domaine "Foreigner CA" sont des étrangers résidant en Belgique qui sont titulaires d'une Carte d'identité électronique avec certificats activés conformément à la loi sur les Cartes d'identité (i.e. lois du 19 juillet 1991, - modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques). Dans la suite du présent document, le terme « sujet » peut être remplacé par le terme « étranger ». Ces étrangers :

- Sont identifiés dans les deux certificats d'étranger ;
- Détiennent les clés privées correspondant aux clés publiques consignées dans leurs certificats d'étranger respectifs ;
- Sont des étrangers résidants en Belgique.

Les étrangers ont le droit de signaler au début du processus de demande de carte d'identité électronique s'ils souhaitent des certificats. La Carte d'identité électronique est délivrée aux étrangers dont les certificats d'étranger sont chargés. Pour les étrangers ne souhaitant pas

obtenir de Certificats d'Étranger, un ou aucun certificat peut être présent sur la carte eID. Se référer au document EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C) pour plus de détails à ce sujet.

Le certificat d'authentification ne sera pas installé sur la carte eID des étrangers n'ayant pas atteint l'âge de 6 ans. Le certificat de signature électronique ne sera pas installé sur la carte eID pour les étrangers n'ayant pas atteint l'âge de 18 ans.

	Certificat d'authentification	Certificat de signature
0 – 6 ans	0	0
6 – 18 ans	X	0
+18 ans	X	X

Le tableau ci-dessus décrit pour chaque catégorie d'âge le certificat qui y est associé.

1.4.4 Parties faisant confiance au certificat

Les parties se fiant au certificat sont des entités, parmi lesquelles figurent les personnes physiques et morales, qui s'appuient sur un certificat et/ou une signature numérique vérifiable par référence à une clé publique énoncée dans un certificat d'étranger.

1.4.5 Autres participants

1.4.5.1 Producteurs de cartes

Le fabricant de cartes pour le « Foreigner CA » est "Zetes SA", dont le siège social est établi rue de Strasbourg 3, 1130 Bruxelles, engagée à cette fin par les Autorités fédérales belges en qualité d'autorité contractante pour le projet eID.

Le producteur de cartes transforme des cartes intelligentes non personnalisées en cartes d'identité électroniques personnalisées, en imprimant les données d'identité et la photographie de l'étranger sur la carte.

Le producteur de cartes fournit aussi les services suivants :

- Génération des paires de clés requises pour la carte ;
- Stockage des deux certificats d'étranger eID sur la carte ;
- Génération des codes d'activation personnels du demandeur et de l'administration communale et du code PIN initial du demandeur ;
- Chargement des certificats racine (« root ») gouvernementaux actifs sur la carte ;
- Fourniture de la carte d'identité électronique à l'administration communale ;
- Fourniture du code d'activation personnel et du code PIN au demandeur ;
- Enregistrement des données dans le registre des cartes d'identité.

1.4.5.2 Fournisseur de Signature racine

Le fournisseur de signature racine (« root sign ») garantit la confiance en la BRCA dans des navigateurs et des applications très répandus. Le fournisseur de signature racine veille à ce que la root certification authority maintienne sa confiance dans de tels navigateurs et applications et notifie à la RA tous les événements affectant la confiance dans sa propre racine. Le fournisseur de signature racine de tous les BRCA actives est Digicert. La politique et les profils de certification de Digicert sont disponibles sur : https://www.digicert.com/legal-repository/

1.4.5.3 Sous-traitant

certipost emploie un sous-traitant pour soutenir le TSP avec des tâches et des responsabilités opérationnelles. Le sous-traitant fournit le support technique pour les services suivants :

- Délivrance du certificat ;
- Révocation/suspension du certificat ;
- Validation du certificat :
  - OCSP ;
  - CRL et delta CRL.

Un accord de niveau de service existe entre le sous-traitant, certipost et le gouvernement. Il détermine la qualité de ces services fournis en termes de performance et de disponibilité. Le sous-traitant rapporte mensuellement ses indicateurs de performance mesurés pour prouver la conformité avec l'accord de niveau de service. Le sous-traitant fournit également un soutien organisationnel pendant les cérémonies clés.

1.5 Utilisation du certificat

L'utilisation des certificats sur la carte d'identité électronique fait l'objet de certaines restrictions.

Deux types de certificats électroniques sont émis par la “Foreigner CA”, qui ont chacun leur usage spécifique :

- Certificat d'authentification : ce certificat est employé pour des transactions d'authentification électroniques supportant un accès à des sites Web et à d'autres contenus en ligne ;
- Certificat de signature électronique qualifiée : ce certificat est utilisé pour créer des signatures électroniques qualifiées.

Chaque eID fourni à un étranger résidant en Belgique peut contenir à la fois un certificat d'authentification et un certificat de signature électronique qualifié étant donné que les exigences élevées de sécurité recommandent de ne pas utiliser de certificats d'authentification à des fins de signature électronique. Le « Foreigner CA » décline donc toute responsabilité envers les parties prenantes dans tous les cas où le certificat d'authentification a été utilisé pour la génération de signatures électroniques

1.6 Administration de la politique

1.6.1 Organisation gérant le document

La gestion administrative est réservée à CERTIPOST, dont voici les coordonnées de contact :

- Par courrier postal :

  certipost sa
  Administration de la Politique - Foreigner CA
  Centre Monnaie
  1000 Bruxelles

- e-mail :

  To: eid.cps@bpost.be
  Concerne : Administration de la Politique - Foreigner CA

1.6.2 Personne de contact

Le contact principal en cas de questions ou de suggestions concernant la Foreigner CA PC/DPC se trouve sous § 1.6.1 ORGANISATION GÉRANT LE DOCUMENT.

Tout feed-back, positif ou négatif, est le bienvenu et doit être transmis à l'adresse e-mail ci-dessus pour qu'il soit traité de manière appropriée et en temps voulu.

1.6.3 Personne déterminant l'adéquation de la DPC à la politique

Conformément à la norme ETSI EN 319 411-2 appuyant la Directive européenne (Règlement 910/2014) CERTIPOST assume la gestion de ses tâches de TSP via un Conseil de gestion PKI (CEPRAC) intégrant toute l'expertise requise.

À travers sa participation officielle aux réunions régulières sur l'état d'avancement du service eID, auxquelles l'ensemble de parties susmentionnées sera dûment représenté, CERTIPOST rassemble l'ensemble des informations nécessaires et pose toutes les questions pertinentes à ces parties pour assumer sa responsabilité de TSP. Les problèmes et questions sont analysés au sein du Conseil de Gestion PKI (PKI Management Board) et si nécessaire, des propositions/corrections sont formulées lors de la réunion sur l'état d'avancement.

Le Conseil de Gestion PKI relaiera en amont vers le Comité de Pilotage eID (eID Steering Committee) dirigé par les Autorités fédérales belges, tout problème ne pouvant être résolu par ce processus. Ce Comité de Pilotage peut faire appel à des experts externes pour obtenir un avis supplémentaire et assume la responsabilité en matière de règlement des litiges.

1.7 Définitions et acronymes

1.7.1 Définitions

Des listes des définitions figurent à la fin de la présente DPC.

1.7.2 Acronymes

Des listes d'acronymes figurent à la fin de la présente DPC.

2. Responsabilités en matière de publication et de référentiels

2.1 Référentiels

La « Foreigner CA » conserve un répertoire en ligne des documents dans lequel elle révèle certaines de ses pratiques et procédures ainsi que le contenu de certaines de ses politiques, y compris sa DPC, accessibles via eID Repository Website. La CA se réserve le droit de mettre à disposition et de publier des informations sur ses politiques par tous les moyens qu'elle juge appropriés.

Le référentiel est disponible sur le site web eID Repository Website.

2.2 Publication des informations de certification

La CA publie un référentiel qui répertorie tous les certificats numériques émis et tous les certificats numériques qui ont été révoqués. L'emplacement du référentiel et des répondants du protocole de validation de certificats en ligne (ci-après abrégé « OCSP » est mentionné dans les profils individuels de certificat, détaillé dans EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C). La CA crée et tient à jour un répertoire de tous les certificats qu'elle a délivrés. Ce répertoire renseigne aussi l'état d'un certificat délivré.

Vu leur caractère sensible, la CA ne publie pas certains sous-composants et éléments de ces documents, notamment certains contrôles de sécurité, des procédures liées entre autres au fonctionnement d'organismes d'enregistrement, des stratégies de sécurité internes, etc. L'accès conditionnel à ces documents et pratiques documentées est néanmoins accordé, pour vérification, à des parties désignées envers lesquelles le TSP a des obligations.

La « Foreigner CA » publie les informations relatives aux certificats dans un ou des référentiels en ligne accessibles au public dans le domaine Internet eid.belgium.be. La CA se réserve le droit de publier des informations concernant le statut du certificat dans des référentiels tiers.

2.3 Moment ou fréquence de publication

Les participants PKI sont avertis que la CA peut publier des informations qu'ils soumettent directement ou indirectement à la CA sur des répertoires publics, à des fins associées à la fourniture d'informations sur l'état des certificats électroniques. Aux intervalles de temps dont la fréquence est indiquée dans la présente DPC, la CA publie des informations sur le statut des certificats.

Des versions approuvées des documents à publier sur le référentiel sont téléchargées conformément au processus de gestion du changement.

2.4 **Contrôles d'accès aux référentiels**

Bien que la « Foreigner CA » mette tout en œuvre pour maintenir la gratuité de l'accès à son référentiel public, elle pourrait faire payer, dans le cadre de son contrat avec le gouvernement belge, des services tels que la publication d'informations d'état dans des bases de données tierces, des répertoires privés, etc.

Le service OCSP, le service de vérification du statut des certificats par interface Web, le référentiel de certificats et les listes de révocation de certificats (les CRL et Delta CRL) sont mis à la disposition du public sur le site Internet de la CA et sont accessibles via les réseaux de l'Autorité fédérale belge.

Dans le cadre du contrat conclu avec l'Autorité fédérale belge, les restrictions d'accès à des services fournis par la « Foreigner CA » incluent :

- Par l'entremise de l'interface publique au référentiel de certificats, un seul certificat peut être délivré pour chaque demande formulée par toute partie à l'exception de la RA ;
- La CA peut prendre des mesures raisonnables en vue d'assurer une protection contre les abus du service OCSP, du service de vérification du statut par interface web et du service de téléchargement des CRL et Delta CRL ;
- La CA ne doit pas restreindre le traitement de demandes OCSP pour toute partie qui, de par la nature de ses activités, requiert une vérification fréquente du statut OCSP.

3. Identification et authentification

3.1 Dénomination

Les règles de dénomination et d'identification des étrangers résidant en Belgique pour les besoins des certificats d'étranger sont les mêmes que les règles légales appliquées à la dénomination et à l'identification des étrangers pour les cartes d'identité.

3.1.1 Types de noms

Certificat utilisateur final Objet attributs de champs sont décrits dans le document **EID-DEL-004 eID hiérarchie PKI profil certificat** (cfr. Annexe C).

3.1.2 Les noms doivent être significatifs

Cf. section 3.1.1

3.1.3 Anonymat ou pseudonymat des usagers

Section non applicable.

3.1.4 Règles pour l'interprétation des différentes formes de noms

Cf. section 3.1.1

3.1.5 Unicité des noms

Le DN du certificat d'un utilisateur final doit être unique.

3.1.6 Reconnaissance, authentification et rôle des marques déposées

Section non applicable.

3.2 Validation de l'identité initiale

L'identification de l'étranger qui demande une carte d'identité électronique repose sur les procédures et règles applicables à la délivrance de cartes d'identité électroniques. La RA définit les procédures à mettre en œuvre par les LRA.

Les procédures applicables sont disponibles sur :

Néerlandais : http://www.ibz.rrn.fgov.be/fr/identiteitsdocumenten/eid/reglementering/

Français : www.ibz.rrn.fgov.be/fr/documents-didentite/eid/reglementation/

Allemand : www.ibz.rrn.fgov.be/de/identitaetsdokumente/eid/vorschriften/

3.2.1 Méthode pour prouver la possession de la clé privée

Conformément à la législation européenne et belge sur les signatures, les clés privées sont générées sur des cartes à puce à signature sécurisée. Le producteur de cartes est responsable de la sécurisation de la carte à puce sur laquelle se trouve l'appareil de création de signature qualifiée (QSCD) avec un numéro d'identification personnel (PIN). Le titulaire de la certification, l'étranger résidant en Belgique, est responsable de la confidentialité du PIN de sa carte à puce. certipost vérifie bi-annuellement que la carte eID Belge figure bien sur la liste des QSCD de l'UE.

3.2.2 Authentification de l'identité organisationnelle

Section non applicable.

3.2.3 Authentification de l'identité individuelle

Cf. section 3.2

3.2.4 Informations d'usager non vérifiées

Section non applicable.

3.2.5 Validation de l'autorité

Cf. section 3.2

3.2.6 Critères pour l'interfonctionnement

Section non applicable.

3.3 Identification et authentification pour des demandes de recomposition (re-key)

L'identification et l'authentification de l'étranger qui demande la recomposition sont soumises à l'application des procédures spécifiées par la RA et mises en œuvre par la LRA.

Les procédures applicables sont disponibles sur :

Néerlandais : http://www.ibz.rrn.fgov.be/fr/identiteitsdocumenten/eid/reglementering/

Français : www.ibz.rrn.fgov.be/fr/documents-didentite/eid/reglementation/

Allemand : www.ibz.rrn.fgov.be/de/identitaetsdokumente/eid/vorschriften/

3.3.1 Identification et authentification pour le renouvellement de recomposition

Cf. section 3.3

3.3.2 Identification et authentification pour recomposition après révocation

Cf. section 3.3

3.4 Identification pour la demande de révocation

L'identification de l'étranger qui demande une révocation de son Certificat d'Étranger reposera sur les procédures et règles applicables à la délivrance de cartes d'identité électroniques.

L'identification et l'authentification de titulaires demandant la révocation de leurs certificats d'étranger seront exécutées par l'entité qui en reçoit la demande. Il peut s'agir :

- De l'administration communale ;
- Des services de police ;
- DOCSTOP 00800 2123 2123 ou +32 2 518 2123

Par la suite, cette entité transmet aussitôt toutes les demandes de révocation à la CA par l'entremise de la RA. La RA représente le seul point de contact de la CA pour l'obtention d'une demande de révocation.

La RA envoie à la CA la demande de révocation signée numériquement, au moyen d'un réseau sécurisé. La CA confirme la révocation à la RA.

4. Exigences opérationnelles posées au cycle de vie d'un certificat

Toutes les entités du domaine du TSP, y compris les LRA, les étrangers résidant en Belgique, les parties se fiant au certificat et/ou d'autres participants, sont constamment tenus d'informer directement ou indirectement la RA de toutes les modifications touchant aux informations contenues dans un certificat durant la période opérationnelle dudit certificat ou de tout autre fait affectant concrètement la validité d'un certificat. La RA prendra alors les mesures qui s'imposent afin de rectifier la situation (p. ex. demander à la CA de révoquer les certificats existants et de générer de nouveaux certificats avec les données correctes).

La CA ne délivre, révoque ou suspend des certificats qu'à la demande de la RA ou du TSP, à l'exclusion de toute autre autorité, sauf sur instruction explicite de la RA.

Dans l'exécution de ses tâches, le TSP fait appel aux services d'agents tiers. Le TSP assume, à l'égard des étrangers et des parties se fiant au certificat, la pleine responsabilité des actes ou omissions de tout agent tiers auquel il fait appel pour la fourniture de services de certification.

4.1 Demande de certificat

4.1.1 Qui peut soumettre une demande de certificat ?

Le processus d'inscription de l'étranger demandeur des certificats fait partie intégrante du processus de traitement de la carte d'identité électronique par son administration communale, c'est-à-dire la LRA. La LRA met en œuvre une procédure d'inscription pour l'étranger telle que prévue par la RA.

4.1.2 Procédure d'inscription et responsabilités

Une fois la demande de certificat approuvée, la RA envoie une demande de délivrance de certificat à la CA. La CA ne vérifie pas l'exhaustivité, l'intégrité et l'unicité des données soumises par la RA, mais se fie totalement à la RA pour ce qui est de l'exactitude de toutes les données. La CA se borne à contrôler que le numéro de série de certificat affecté à la demande de certificat par la RA est bien un numéro de série unique qui n'a pas encore été attribué à un autre certificat d'étranger, auquel cas il le notifie à la RA.

Toutes les demandes émanant de la RA sont approuvées dans la mesure où :

- Elles présentent un format valable ;
- Elles transitent par le canal de communication sécurisé adéquat ;
- Elles ont subi toutes les vérifications qui s'imposent conformément au contrat de la CA.

La CA vérifie l'identité de la RA en se fondant sur les données d'identification présentées.

La CA s'assure que le certificat délivré contient toutes les données qui lui ont été présentées dans la demande de la RA et, en particulier, un numéro de série affecté au certificat par la RA.

Après la délivrance d'un certificat, la CA publie un certificat délivré sur un référentiel et suspend le certificat. Le certificat est ensuite délivré à la RA.

La RA prie le producteur de cartes de charger les certificats d'étranger sur la carte d'identité électronique. Le producteur de cartes transmet par un moyen sécurisé la carte d'identité électronique avec les certificats d'étranger à la LRA.

4.2 Traitement de la demande de certificat

La LRA donne suite à une demande de certificat pour valider l'identité du demandeur conformément à la procédure relative à la demande de carte d'identité électronique. Les procédures de validation de l'identité d'un demandeur font l'objet d'un document spécifique.

A la suite d'une demande de certificat, la LRA approuve ou rejette la demande de carte d'identité électronique comprenant aussi la demande de certificat. Si la demande est approuvée, la LRA transmet les données d'enregistrement à la RA. À son tour, la RA approuve ou rejette la demande.

Les procédures applicables sont disponibles sur :

Néerlandais : http://www.ibz.rrn.fgov.be/fr/identiteitsdocumenten/eid/reglementering/

Français : www.ibz.rrn.fgov.be/fr/documents-didentite/eid/reglementation/

Allemand : www.ibz.rrn.fgov.be/de/identitaetsdokumente/eid/vorschriften/

4.2.1 Appliquer les fonctions d'identification et d'authentification

Section non applicable.

4.2.2 Approbation ou rejet des demandes de certificat

Section non applicable.

4.2.3 Durée de traitement des demandes de certificat

Section non applicable.

4.3 Délivrance du certificat

Une fois la demande de certificat approuvée, la RA envoie une demande de délivrance de certificat à la CA. La CA ne vérifie pas l'exhaustivité, l'intégrité et l'unicité des données soumises par la RA, mais se fie totalement à la RA pour ce qui est de l'exactitude de toutes les données. La CA se borne à contrôler que le numéro de série de certificat affecté à la demande de certificat par la RA est bien un numéro de série unique qui n'a pas encore été attribué à un autre certificat d'étranger, auquel cas il le notifie à la RA.

Toutes les demandes émanant de la RA sont approuvées dans la mesure où :

- Elles présentent un format valable ;
- Elles transitent par le canal de communication sécurisé adéquat ;
- Elles ont subi toutes les vérifications qui s'imposent conformément au contrat de la CA.

La CA vérifie l'identité de la RA en se fondant sur les données d'identification présentées.

La CA s'assure que le certificat délivré contient toutes les données qui lui ont été présentées dans la demande de la RA et, en particulier, un numéro de série affecté au certificat par la RA.

À la suite de l'émission, la CA suspend le certificat et est délivrée à la RA.

La RA prie le producteur de cartes de charger les certificats d'étranger sur la carte d'identité électronique. Le producteur de cartes transmet par un moyen sécurisé la carte d'identité électronique avec les certificats d'étranger à la LRA.

4.3.1 Actions de la CA lors de la délivrance du certificat

Sans objet.

4.3.2 Notification à l'usager par la CA de la délivrance du certificat

Sans objet.

4.4 Acceptation du certificat

Une fois produite, la carte d'identité électronique possède un statut « non activé ». La LRA active la carte d'identité électronique en présence de l'étranger. L'étranger et la RA ont tous deux besoin des données d'activation de la carte qui doit être fournie par le producteur de cartes par un moyen sécurisé. La carte ne peut être activée qu'au moyen des données d'activation combinées de la RA et de l'étranger.

4.4.1 Démarche d'acceptation du certificat

Des objections à l'acceptation d'un certificat délivré sont notifiées à la RA via la LRA en vue de prier la CA de révoquer les certificats.

4.4.2 Publication des certificats par la CA

Sans objet.

4.4.3 Notification par la CA de la délivrance de certificat à d'autres entités

Section non applicable.

4.5 Paire de clés et emploi du certificat

L'emploi des clés et des certificats implique les responsabilités exposées ci-après.

4.5.1 Utilisation de la clé privée et du certificat par le sujet

Sauf indication contraire dans la présente DPC, les droits et obligations de l'étranger sont les suivants :

- S'abstenir de falsifier un certificat ;
- Prévenir la compromission, la perte, la divulgation, la modification ou toute utilisation illicite de ses clés privées ;
- Utiliser uniquement des certificats à des fins légales et autorisées, conformément à la présente DPC.

4.5.2 Utilisation de la clé privée et du certificat par la partie utilisatrice

Une partie se fiant à un certificat :

- 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 ;
- Fera confiance à un certificat uniquement s'il n'a pas été suspendu ou révoqué ;
- Se fiera à un certificat de manière raisonnable en fonction des circonstances ;
- Pour vérifier la validité d'un certificat numérique, les parties confiantes doivent toujours opérer une vérification en se basant sur la période de validité du certificat et sur la déclaration de validité du certificat auprès du service de vérification de la CA (p. ex. OCSP, CRL, Delta CRL ou interface Web) avant de s'appuyer sur des informations fournies dans un certificat.

4.6 Renouvellement du certificat

Selon la RFC 3647, un renouvellement du certificat signifie : « *The issuance of a new Certificate without changing the Public Key or any other information in the Certificate* ». Pour les certificats d'entité finale (certificats d'authentification et de signature), cette aptitude n'est pas supportée.

4.6.1 Circonstance de renouvellement d'un certificat

Le renouvellement de certificat n'est pas supporté.

4.6.2 Le renouvellement de certificat n'est pas supporté.

Cf. section 4.6.1.

4.6.3 Qui peut demander un renouvellement ?

Cf. section 4.6.1.

4.6.4 Traitement des demandes de renouvellement de certificat

Cf. section 4.6.1.

4.6.5 Notification à l'usager de la délivrance du nouveau certificat

Cf. section 4.6.1.

4.6.6 Démarche d'acceptation d'un certificat renouvelé

Cf. section 4.6.1.

4.6.7 Publication du certificat renouvelé par la CA.

Cf. section 4.6.1.

4.6.8 Notification par la CA de la délivrance de certificat aux autres entités

Cf. section 4.6.1.

4.7 Recomposition d'un certificat

Selon RFC 3647, la recomposition d'un certificat est définie comme : *«… a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key».* Dans le contexte de la carte d'identité électronique, cela signifie que le sujet (le citoyen) fera une demande d'émission d'un nouveau certificat avec les mêmes informations d'identification mais avec une clé publique et une période de validité différentes. La diligence raisonnable, la génération de la paire de clés, l'émission et la gestion sont effectuées conformément à la présente PC/DPC.

4.7.1 Circonstance de recomposition d'un certificat

La recomposition d'un certificat est supportée.

4.7.2 Qui peut demander la certification d'une nouvelle clé publique ?

Cf. section 4.1

4.7.3 Traitement des demandes de recomposition de certificat

Les demandes de nouvelle clé de certificat sont traitées de la même manière que les demandes de nouvelle authentification ou de signature de certificats et conformément aux dispositions du présent PC / DPC.

4.7.4 Notification à l'usager de la délivrance du nouveau certificat

Section non applicable.

4.7.5 Démarche d'acceptation d'un certificat recomposé

Section non applicable.

4.7.6 Publication du certificat recomposé par la CA

Section non applicable.

4.7.7 Notification par la CA de la délivrance de certificat à d'autres entités

Section non applicable.

4.8 Modification du certificat

Section non applicable.

4.9 Suspension et révocation du certificat

Jusqu'à leur acceptation par l'étranger, les certificats d'étranger demeurent suspendus dans la carte d'identité électronique. Les RA et LRA font diligence pour se conformer à cette exigence.

Pour demander la révocation d'un certificat, un étranger doit contacter une LRA, les services de police ou le DOCSTOP. Alors que les heures d'ouverture d'une LRA sont limitées, le DOCSTOP est accessible 24 heures sur 24, 7 jours sur 7.

Les cartes d'identité contenants des certificats suspendus sont directement transmises aux étrangers habitants hors du territoire. Après quoi, ils peuvent se rendre à l'ambassade afin

d'activer la puce et les certificats présents sur cette carte. Cependant, cette activation n'est pas limitée dans le temps.

Les services de police, la LRA ou le DOCSTOP font diligence pour demander la révocation des certificats d'étranger via la RA :

- Après avoir reçu notification de l'existence de soupçons concernant une perte, un vol, une modification, une divulgation non autorisée ou toute autre compromission de la clé privée d'un ou de ses deux certificats d'étranger ;
- Si l'exécution d'une obligation de la LRA au sens de la présente DPC est retardée ou empêchée par une catastrophe naturelle, une panne informatique, une interruption des télécommunications ou toute autre cause indépendante de la volonté raisonnable de la personne et crée en conséquence un doute quant à la menace ou à la compromission matérielle des informations d'une tierce personne ;
- Après une notification, par l'étranger, de l'existence d'une perte, d'un vol, d'une modification, d'une divulgation non autorisée ou de toute autre compromission de la clé privée d'un ou de ses deux certificats d'étranger ;
- Si les informations contenues dans un certificat d'étranger ont été modifiées ;
- Si l'exécution d'une obligation de la RA au sens de la présente DPC est retardée ou empêchée par une catastrophe naturelle, une panne informatique, une interruption des télécommunications ou toute autre cause indépendante de la volonté raisonnable de la personne et crée en conséquence une menace ou une compromission matérielle pour les informations d'une tierce personne ;
- Une obligation légale imposée par la RA.

À la demande de la RA ou du TSP, la CA révoque les certificats d'étranger.

Dans le cas où le sujet a demandé la suspension ou la révocation d'un certificat par le biais de DOCSTOP, le sujet est informé de la modification du statut du certificat par une lettre envoyée à son adresse officielle.

Dans des circonstances spécifiques (p. ex. une catastrophe a été évitée, une clé CA se caractérise par une violation de sécurité, etc.), le TSP peut demander la suspension et/ou la révocation de certificats.

Le TSP demandera au eID TSP steering l'autorisation de procéder à ces révocations. Selon le degré d'urgence, il peut toutefois arriver que le eID CSP Steering ne soit averti qu'une fois le processus terminé. La RA veille à prévenir les étrangers concernés de cette suspension/révocation.

Les parties confiantes doivent utiliser les ressources en ligne que la CA met à leur disposition via son référentiel afin de vérifier l'état des certificats avant de s'y fier. La CA met à jour en conséquence l'OCSP, le service de vérification d'état de la certification par interface Web, les CRL et les Delta CRL. Les CRL sont actualisées fréquemment, au minimum toutes les trois heures.

La CA donne accès aux ressources OCSP et à un site Web sur lequel les requêtes d'état peuvent être soumises. De plus, pour tout certificat émis sous la Foreigner CA, les informations liées au statut de la révocation seront disponibles au-delà de la période de validité du certificat par l'intermédiaire de la CRL.

4.9.1 Circonstances pour révocation

La CA publie des avis concernant les certificats suspendus ou révoqués dans le référentiel.

4.9.2 Qui peut demander une révocation ?

Cf. section 4.9

4.9.3 Procédure de demande de révocation

Cf. section 4.9

4.9.4 Période de grâce demande de révocation

La période de grâce de la demande de révocation est la période à partir de laquelle le sujet (c'est-à-dire le citoyen) a demandé une révocation de certificat en contactant le LRA, la police ou DOCSTOP jusqu'à ce que la révocation du certificat soit reflétée dans les services de validation des certificats.

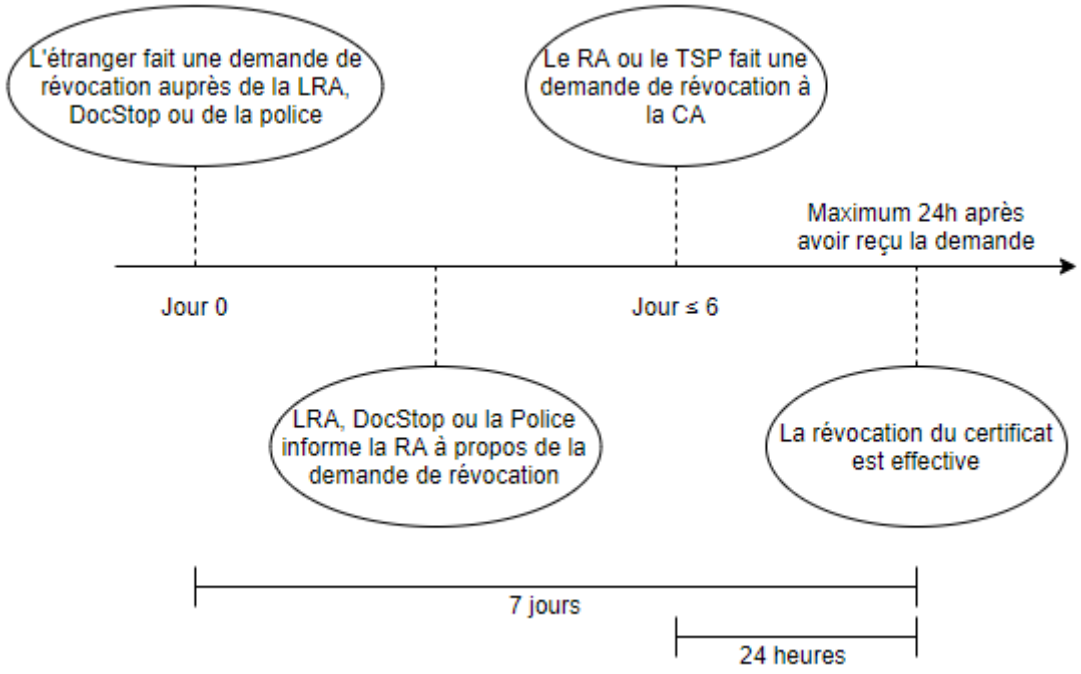

Figure 1: Ligne du temps d'une révocation

La Figure 1: Ligne du temps d'une révocation représente la ligne du temps de la révocation et montre que, dans le contexte de la carte d'identité électronique, un maximum de 6 jours peut s'écouler avant que la CA ne reçoive la demande de révocation après quoi, un maximum de 24 heures peut s'écouler avant que la révocation ne soit effective.

La période de grâce pour le traitement de la demande de révocation est de 7 jours. Cependant, la mise à jour du statut est reflétée dans le service de validation endéans les 3h suivant la réception de la demande de révocation par la CA.

4.9.5 Délai au cours duquel la CA doit traiter la demande de révocation

La CA révoquera un Certificat citoyen après avoir reçu la demande de révocation de la RA aussi rapidement que possible après validation de la demande de révocation. Le délai maximal entre la réception d'une demande ou d'un rapport de révocation et la décision de modifier ses informations de statut à la disposition de toutes les parties confiantes est au maximum de 24 heures.

Généralement, on utilise les délais suivants :

- Les demandes de révocation reçues trois heures ou plus avant que les émissions de CRL ne soient traitées, avant que la prochaine CRL ne soit publiée ;
- Les demandes de révocation reçues dans les trois heures suivant l'émission de CRL sont traitées avant que la CRL suivante ne soit publiée ;
- Les demandes de révocation sont reprises dans le service de validation du certificat OCSP dans les trois heures suivant la réception de la demande.

4.9.6 Exigence de vérification de révocation pour les parties qui se fient au certificat

Voir **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C)**.

4.9.7 Fréquence de publication de la CRL (si d'application)

Voir **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C)**.

4.9.8 Temps de latence maximum pour les CRL (si d'application)

Voir **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C)**.

4.9.9 Disponibilité de la vérification en ligne de la révocation et du statut

Voir **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C)**.

4.9.10 Exigences relatives à la vérification en ligne de la révocation

Voir **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C)**.

4.9.11 Autres formulaires d'annonce de révocation disponibles

Section non applicable.

4.9.12 Exigences particulières en cas de compromission de recomposition

Section non applicable.

4.9.13 Circonstances de suspension

Cf. section 4.9

4.9.14 Qui peut demander une suspension ?

Cf. section 4.9

4.9.15 Procédure de demande de suspension

Cf. section 4.9

4.9.16 Limites de la période de suspension

Cf. section 4.9.1

4.10 Services d'état du certificat

La CA met à disposition des services de vérification du statut des certificats, parmi lesquels des CRL, des Delta CRL, des OCSP et des interfaces web adéquates.

4.10.1 CRL et delta CRL

Une Delta CRL reprend tous les ajouts depuis la publication de la dernière CRL de base.

Les CRL et les Delta CRL sont signées et datées par la CA.

Une CRL est publiée dans des intervalles minimum de 3 heures, à une heure convenue. Une Delta CRL est publiée toutes les 3 heures, selon un horaire convenu. Les CRL et les Delta CRL sont signées et datées par la CA. Les CRL et Delta CRL se trouvent sur :

https://crl.eid.belgium.be/

4.10.2 OCSP

La CA met les réponses OCSP à la disposition de l'Administration belge qui les exploite via ses propres réseaux de l'administration publique.

Une interface Web simple donne accès aux services de vérification d'état et permet à un utilisateur d'obtenir des informations sur l'état d'un certificat. La CA met ces interfaces web d'accès aux services de vérification du statut à la disposition de l'administration belge qui les exploite via ses propres réseaux de l'administration publique et dans le cadre de ceux-ci.

service de vérification d'état par interface Web : https://status.eid.belgium.be/

Il est possible de consulter les répondants OCSP à l'adresse suivante :

https://ocsp.eid.belgium.be ou https://ocsp.eid.belgium.be/2

4.10.3 Caractéristiques opérationnelles

*Voir **EID-DEL-004 eID hiérarchie PKI profil certificat** (CFR. ANNEXE C).*

4.10.4 Disponibilité du service

Les services d'état du certificat sont disponibles 24 heures sur 24 et 7 jours sur 7.

En dehors des périodes de maintenance, pour chaque mois civil, le temps total d'indisponibilité de chacun des services CA suivants, mesuré en minutes cumulées sur le mois complet, ne doit pas excéder 0,5 % du nombre total de minutes du mois civil concerné :

- Vérification OCSP d'état du certificat à la suite d'une demande introduite par le RRN, un sujet ou une partie faisant confiance au certificat ;

- Téléchargement de CRL ou de delta CRL via Internet ou les réseaux des pouvoirs publics ;
- Service de vérification du statut de certificats par interface Web.

L'indisponibilité du service OCSP, du service de téléchargement de CRL et de delta CRL et du service de vérification du statut par interface web comprend l'indisponibilité de l'infrastructure locale de la CA, notamment les serveurs, réseaux et pare-feu locaux, mais n'inclut pas l'indisponibilité (de parties) du réseau Internet et l'indisponibilité de l'infrastructure locale du demandeur du service.

Au niveau interne, la CA archive les éléments, données et documents suivants relatifs à son service :

- CRL et delta CRL. Les CRL et delta CRL sont archivées pendant une période d'au moins 25 ans suivant leur publication.

4.10.5 Caractéristiques optionnelles

La CA ne doit pas restreindre le traitement de demandes OCSP pour une partie qui, de par la nature de ses activités, requiert une vérification fréquente du statut OCSP.

4.11 Fin de la souscription

Section non applicable.

4.12 Séquestre et récupération de clés

Il n'y a pas d'autorisation de séquestrer ni de récupérer les clés.

5. Contrôles des installations, de la gestion et des activités

Ce chapitre décrit les contrôles de sécurité non techniques utilisés par la "Foreigner CA" et les autres partenaires PKI, dans le cadre des opérations de génération de clé, d'authentification de la personne concernée, de délivrance du certificat, de révocation de certificat, d'audit et d'archivage.

5.1 Contrôles physiques

Le TSP met en œuvre des contrôles physiques sur son propre site. Les contrôles physiques de l'opérateur du TSP comprennent les aspects suivants :

Les sites du TSP hébergent l'infrastructure nécessaire pour fournir les services TSP. Les sites TSP mettent en œuvre les contrôles de sécurité adéquats, y compris le contrôle d'accès, la détection des intrusions et la surveillance. L'accès aux sites est limité au personnel autorisé mentionné sur la liste de contrôle d'accès, qui fait l'objet d'un audit.

Un contrôle d'accès strict est mis en œuvre partout où il y a du matériel et des infrastructures hautement sensibles, y compris le matériel et les infrastructures destinés à la signature des certificats, aux CRL et delta CRL, aux OCSP et aux archives.

5.1.1 Situation et construction du site

Les locaux sécurisés des opérateurs TSP sont situés à un endroit approprié pour les opérations hautement sécurisées. Ces locaux comprennent des zones numérotées et des pièces, cages, coffres-forts et armoires verrouillables.

5.1.2 Accès physique

L'accès physique est restreint par la mise en œuvre de mécanismes qui contrôlent le passage d'une zone à une autre, ou l'accès aux zones hautement sécurisées, comme la localisation des opérations TSP dans une salle informatique sécurisée, surveillée physiquement et protégée par des alarmes de sécurité et un système impliquant que tout mouvement d'une zone à une autre s'effectue avec un jeton et des listes de contrôle d'accès.

5.1.3 Alimentation électrique et climatisation

Fonctionnement largement redondant de l'alimentation électrique et de la climatisation.

5.1.4 Expositions à l'eau

Les locaux sont protégés contre toute exposition à l'eau.

5.1.5 Prévention et protection contre l'incendie

Le TSP met en œuvre des mesures de prévention, de protection et de lutte contre l'incendie.

5.1.6 Stockage des équipements

Les équipements sont entreposés en toute sécurité. Les équipements de back-up en outre sont stockés à un autre endroit, protégé physiquement contre le feu et les dégâts des eaux.

5.1.7 Élimination des déchets

Pour prévenir toute diffusion indésirable des données sensibles, les déchets sont évacués de manière sécurisée.

5.1.8 Back-up hors site

Le TSP réalise le back-up partiellement hors site.

5.2 Contrôles des procédures

Le TSP applique des procédures, en matière de personnel et de management, qui offrent une garantie raisonnable quant à la fiabilité et la compétence des membres de l'équipe et à la réalisation satisfaisante de leurs tâches dans le domaine des technologies de signature électronique.

Le TSP fait signer à chaque membre de l'équipe une déclaration d'absence de conflit d'intérêts avec le TSP, de respect de la confidentialité et de protection des données personnelles.

Tous les membres de l'équipe qui assument des fonctions de gestion des clés, les administrateurs, le personnel de sécurité et les auditeurs de système ou de toute autre opération pouvant affecter matériellement ces opérations sont considérés comme occupant des postes de confiance.

Le TSP mène une enquête initiale pour tous les membres de l'équipe qui sont candidats à un poste de confiance en vue de déterminer leur degré de fiabilité et de compétence.

Lorsqu'un double contrôle est requis, au moins deux personnes occupant une position de confiance doivent apporter leurs connaissances respectives et distinctes pour procéder aux opérations courantes.

Le TSP veille à ce que toutes les actions concernant le TSP puissent être attribuées au système du TSP et au membre de l'équipe TSP qui a réalisé l'action.

5.2.1 Rôles de confiance

Le TSP distingue les groupes de travail suivants :

- Personnel d'exploitation TSP qui gère les opérations pour les certificats ;
- Personnel administratif qui s'occupe de la plate-forme de support du TSP ;
- Personnel de sécurité qui met en œuvre les mesures de sécurité.

5.3 Contrôles du personnel

Le TSP met en œuvre des contrôles de sécurité pour les tâches et les performances des membres de son équipe. Ces contrôles de sécurité sont documentés dans une politique et recouvrent les domaines ci-après.

5.3.1 Exigences en matière de compétences, d'expérience et d'habilitation

Le TSP effectue des contrôles pour définir les antécédents, les qualifications et l'expérience nécessaires pour fonctionner dans le domaine de compétence du job spécifique. Ces vérifications d'antécédents comprennent :

- Les condamnations pour délits graves ;

- Les fausses déclarations du candidat ;
- L'exactitude des références ;
- Toute autorisation, le cas échéant.

5.3.2 Procédures de vérification des antécédents

Le TSP effectue les contrôles nécessaires pour les employés potentiels au moyen de rapports de situation fournis par une autorité compétente, des déclarations de parties tierces ou des déclarations personnelles signées.

5.3.3 Exigences en matière de formation

Le TSP offre au personnel des formations pour que celui-ci puisse assumer ses fonctions TSP.

5.3.4 Fréquence et exigences de recyclage

Des recyclages périodiques sont également prévus pour assurer la continuité et l'actualisation des connaissances du personnel et des procédures.

5.3.5 Fréquence et séquence de rotation des emplois

Section non applicable.

5.3.6 Sanctions pour actions non autorisées

Le TSP sanctionne le personnel pour toute action non autorisée, abus d'autorité et usage non autorisé des systèmes dans le but d'imposer une responsabilité au personnel participant, le cas échéant.

5.3.7 Exigences pour les contractants indépendants

Les sous-contractants indépendants du TSP et leur personnel font l'objet des mêmes contrôles d'antécédents que le personnel TSP. VOIR 5.3.1 EXIGENCES EN MATIÈRE DE COMPÉTENCES, D'EXPÉRIENCE ET D'HABILITATION.

5.3.8 Documentation fournie au personnel

Le TSP met à la disposition du personnel la documentation nécessaire durant la formation initiale, le recyclage ou autre.

5.4 Procédures de journalisation d'audit

Les procédures pour la journalisation d'audit comprennent la journalisation d'événements et l'audit des systèmes, dans le but de maintenir un environnement sécurisé. La CA met en œuvre les contrôles suivants :

Le système de journalisation d'événements de la CA consigne les événements tels que, entre autres :

- Émission d'un certificat ;
- Révocation d'un certificat ;
- Suspension d'un certificat ;

- (Ré)activation d'un certificat ;
- Révocation automatique ;
- Publication d'une CRL ou delta CRL.

Le TSP audite tous les enregistrements du journal d'événement. Les enregistrements du rapport d'audit comportent :

- L'identification de l'opération ;
- La date et l'heure de l'opération ;
- L'identification du certificat, impliqué dans l'opération ;
- L'identité du demandeur de la transaction.

En outre, le TSP conserve les journaux internes et les rapports d'audit des événements opérationnels importants dans l'infrastructure. Il s'agit notamment :

- Du démarrage et de l'arrêt des serveurs ;
- Des pannes et des problèmes majeurs ;
- De l'accès physique du personnel et d'autres personnes aux parties sensibles du site TSP ;
- Du back-up et des récupérations ;
- Du rapport des tests de remise en service après catastrophe ;
- Des inspections d'audit ;
- Des extensions et changements des systèmes, logiciels et infrastructure ;
- Des intrusions et tentatives d'intrusion dans les zones sécurisées.

Autres documents nécessaires pour les audits, notamment :

- Plans et descriptions de l'infrastructure ;
- Plans et descriptions des sites physiques ;
- Configuration du matériel informatique et des logiciels ;
- Listes de contrôle d'accès du personnel.

Le TSP veille à ce que le personnel désigné à cet effet vérifie les fichiers journaux à intervalles réguliers et rapporte les événements anormaux.

Les fichiers journaux et les rapports d'audit sont archivés pour inspection par le personnel autorisé de la CA, les RA et les auditeurs désignés. Les fichiers journaux doivent être protégés de façon adéquate par un mécanisme de contrôle d'accès. Les fichiers journaux et les rapports d'audit font l'objet d'un back-up.

Les événements d'audit ne donnent pas lieu à une consignation dans le journal.

5.4.1 Types d'événements journalisés

Le TSP conserve d'une manière fiable les dossiers des certificats numériques, données d'audit, informations et documentation sur les systèmes TSP.

5.4.2 Fréquence du traitement du journal

La CA passe régulièrement en revue les journaux d'audit à la recherche d'anomalies ou d'alertes.

5.4.3 Période de rétention pour le journal d'audit

Le TSP conserve d'une manière fiable les dossiers des certificats numériques pendant la durée mentionnée à l'article 5.5 de cette DPC.

5.4.4 Protection du journal d'audit

Seul le gestionnaire des dossiers (membre de l'équipe chargée de la conservation des dossiers) peut accéder aux archives TSP. Des mesures doivent être prises pour assurer :

- La protection contre la modification des archives, comme l'entreposage des données sur un support non réinscriptible ;
- La protection contre toute suppression des archives ;
- La protection contre la détérioration des médias sur lesquels les archives sont stockées, comme le transfert régulier des données sur des médias non utilisés.

Le TSP agira conformément à l'application potentielle par l'Autorité Fédérale belge de la procédure de l'article 14 de la Loi du 8 août 1983 *organisant un registre national des personnes physiques* et l'article 7 de la loi du 12 mai 1927 *sur les réquisitions militaires*. Dans pareil cas, la CA agit conformément aux instructions fournies par la personne désignée par l'Arrêté Royal pour ce qui concerne les données faisant partie des cartes d'identité électroniques et des certificats d'étranger.

5.4.5 Procédures de back-up du journal d'audit

Un back-up différentiel des archives du TSP est effectué quotidiennement les jours ouvrables.

5.4.6 Système de collecte d'audit

Le système de collecte des archives du TSP est interne.

5.4.7 Notification du sujet ayant causé un événement

Section non applicable.

5.4.8 Évaluations de vulnérabilité

Section non applicable.

5.5 Archivage des dossiers

Le TSP conserve en interne les dossiers des éléments suivants :

- Tous les certificats pendant une période d'au moins 25 ans après expiration du certificat ;
- Journaux d'audit de l'émission des certificats pour une période d'au moins 25 ans après émission du certificat ;

- Journal d'audit de la révocation d'un certificat d'au moins 25 ans après révocation du certificat ;
- CRL et Delta CRL d'au moins 25 ans après leur publication ;
- Le TSP doit conserver le dernier back-up des archives de la CA au moins 25 ans après émission du dernier certificat.

Le TSP conserve les archives dans un format consultable.

Le TSP veille à l'intégrité des dispositifs de stockage physique et met en œuvre des mécanismes de copie adéquats pour éviter toute perte de données.

Les archives sont accessibles au personnel autorisé de la CA et de la RA.

5.5.1 Types de documents archivés

Le TSP conserve d'une manière fiable les dossiers des certificats numériques, données d'audit, informations et documentation des systèmes TSP.

5.5.2 Période de rétention pour l'archivage

Le TSP conserve d'une manière fiable les dossiers des certificats numériques pendant la durée mentionnée à l'article 5.5 de cette DPC. Cette exigence fait l'objet d'une vérification périodique.

5.5.3 Protection des archives

Seul le gestionnaire des dossiers (membre de l'équipe chargée de la conservation des dossiers) peut accéder aux archives TSP. Des mesures doivent être prises pour assurer :

- La protection contre la modification des archives, comme l'entreposage des données sur un support non réinscriptible ;
- La protection contre toute suppression des archives ;
- La protection contre la détérioration des médias sur lesquels les archives sont stockées, comme le transfert régulier des données sur des médias non utilisés.

Le TSP agira conformément à l'application potentielle par l'Autorité Fédérale belge de la procédure de l'article 14 de la Loi du 8 août 1983 *organisant un registre national des personnes physiques* et l'article 7 de la loi du 12 mai 1927 *sur les réquisitions militaires*. Dans pareil cas, la CA agit conformément aux instructions fournies par la personne désignée par l'Arrêté Royal pour ce qui concerne les données faisant partie des cartes d'identité électroniques et des certificats d'étranger.

5.5.4 Procédures de back-up des archives

Un back-up différentiel des archives du TSP est effectué quotidiennement les jours ouvrables.

5.5.5 Condition d'horodatage sur les dossiers

Section non applicable.

5.5.6 Système de collecte des archives (internes ou externes)

Le système de collecte des archives du TSP est interne.

5.5.7 Procédures d'obtention et de vérification des informations d'archivage

Seuls les membres de l'équipe TSP ayant un contrôle hiérarchique clair et une description de job définie peuvent obtenir et vérifier les informations d'archivage.

Le TSP conserve les dossiers en format électronique ou sur papier.

5.6 Changement de clé

La Foreigner CA dispose d'un calendrier pour le changement clé des CA émettrices subordonnées et des certificats CA émis (les certificats CA Foreigner peuvent être téléchargés sur eID Repository Website):

À la fin de chaque année, une quantité de certificats CA Foreigner est générée lors d'une cérémonie clé. Cette quantité est déterminée par le TSP et le gouvernement et est basée sur la demande attendue des certificats d'entité finale au cours de l'année prochaine. Dans la cérémonie clé, les certificats Foreigner CA sont émis par les BRCA, qui sont des certificats approuvés de longue date de l'eID PKI.

Une fois que le nouveau lot de certificats Foreigner CA est mis dans l'environnement de production, ces certificats d'émission seront utilisés pour émettre les certificats d'entité finale de l'année en cours et le lot précédent de certificats Foreigner CA ne sera plus utilisé pour l'émission de nouveaux certificats. En d'autres termes, un certificat Foreigner CA ne sera utilisé que pendant un an pour émettre de nouveaux certificats. Un certificat Foreigner CA doit être valide plus longtemps que tout certificat d'entité finale délivré.

Une fois qu'un certificat Foreigner CA a expiré ou a été révoqué, le matériel clé sera détruit lors de la prochaine cérémonie clé.

5.7 Récupération de compromission et de catastrophe

Un plan de continuité des opérations a été élaboré pour assurer la continuité des opérations suite à une catastrophe naturelle ou autre.

Toutes ces mesures sont implémentées conformément à ISO 27001.

Le TSP établit :

- Les ressources de récupération en cas de catastrophe dans deux endroits, suffisamment distants l'un de l'autre ;
- Une communication rapide entre les deux sites pour assurer l'intégrité des données ;
- Une infrastructure de communication des deux sites vers la RA supportant les protocoles de communication sur Internet, ainsi que les protocoles de communication utilisés par l'administration publique belge ;
- Les infrastructures et procédures de récupération après catastrophe sont testées au moins chaque année.

5.7.1 Procédures de traitement des incidents et des compromissions

Dans un document interne distinct, la « Foreigner CA » spécifie les procédures de rapport et de traitement des incidents et des compromissions. Le TSP spécifie les procédures de récupération utilisées si les ressources informatiques, les logiciels et/ou les données sont corrompus ou suspectés de corruption.

Le TSP définit les mesures nécessaires pour assurer une récupération complète et automatique en cas de catastrophe, de corruption des serveurs, des logiciels ou des données.

5.7.2 Corruption des ressources informatiques, logiciels, et/ou données.

Le TSP a des procédures spécifiques de récupération dans l'éventualité où les ressources informatiques, les logiciels et/ou les données sont corrompus ou suspectés de corruption.

5.7.3 Procédures en cas de compromission de la clé privée d'une entité

En cas de compromission réelle ou présumée de la clé privée Foreigner CA, les procédures de gestion de crise TSP sont adoptées selon le processus de gestion des incidents et avec l'approbation du senior management de certipost et des représentants du gouvernement belge. Les parties concernées sont informées par le biais d'un plan de communication et si la révocation du certificat CA est requise, le statut révoqué est communiqué aux parties se fiant au certificat sur le site web eID répertoire ou sur le site web eID CRL.

5.7.4 Possibilités de poursuivre les activités après un désastre

Le TSP a développé la capacité de récupérer ses opérations CA dans les quatre (4) heures ouvrables après une catastrophe avec le soutien de toutes les fonctions clés, à savoir la délivrance de certificat, la révocation du certificat et la publication d'informations CRL.

5.8 Résiliation CA ou RA

Dès l'instant où le TSP reçoit la notification par le Gouvernement fédéral belge que son contrat va s'achever et/ou dès le moment où son contrat est annulé prématurément, le TSP consulte l'État belge pour déterminer les étapes requises pour (1) garantir une transition aisée pour la prestation des services au nouveau TSP, et pour (2) assurer la destruction, la suppression, la restitution et/ou la sécurité de l'information, des données à caractère personnel et des fichiers reçus par le TSP dans le cadre de sa mission de TSP conformément au règlement de l'UE 910/2014 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

6. Contrôles de sécurité techniques

Ce chapitre définit les mesures de sécurité que la CA prend pour protéger ses clés cryptographiques et les données d'activation (ex. PIN, mots de passe ou parts de clés détenues manuellement).

6.1 Génération et installation de la paire de clés

La CA protège sa (ses) clé(s) privée(s) conformément à la présente DPC. La CA utilise des clés de signature privées uniquement pour signer les certificats, les CRL, les Delta CRL et réponses OCSP en conformité avec l'usage prévu pour chacune de ces clés.

La CA s'abstiendra d'utiliser ses clés privées utilisées dans le cadre de la CA autrement que dans la portée du domaine de « Foreigner CA ».

6.1.1 Génération de paires de clés

La CA et la RA utilisent une procédure fiable pour la génération de sa clé privée CA selon une procédure documentée. La CA distribue les parts de secret de sa (ses) clé(s) privée(s). Le TSP est habilité à transférer ces parts de secret aux détenteurs de parts de secret selon une procédure documentée.

Les paires de clés pour les CA émetteurs subordonnés du Foreigner CA (clés CA émettrices) ont été générées dans un HSM hors ligne répondant au minimum aux exigences FIPS 140-2 niveau 3. Par conséquent, les clés CA émettrices ont été clonées dans un HSM en ligne répondant au minimum aux exigences FIPS 140-2 niveau 3.

6.1.2 Transmission de la clé privée au sujet

La clé privée du sujet est générée par le producteur de cartes et par le QSCD. La clé privée n'est pas extraite à partir du QSCD.

6.1.3 Délivrance de clés publiques à un émetteur de certificats

La clé publique du sujet est transférée du producteur de cartes après la génération de paire de clés sur le QSCD vers la RA au moyen d'un message crypté en passant par une connexion sécurisée. La RA incorpore la clé publique dans une demande et l'envoie à la CA par le biais d'un lien privé sécurisé.

La même méthode est utilisée pour retourner le certificat au producteur de cartes.

6.1.4 Délivrance de la clé publique de la CA aux parties se fiant au certificat

La clé publique de la CA est disponible sur le site web du répertoire eID.

6.1.5 Taille des clés

Pour plus de détails, se référer à **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C)**.

6.1.6 Génération et contrôle de la qualité des paramètres des clés publiques

Voir section 6.1.1 GÉNÉRATION DE PAIRES DE CLÉS.

6.1.7 Usages visés des clés (conformément au champ d'usage de clé X.509 v3)

Pour plus de détails, se référer au document EID-DEL-004 eID HIÉRARCHIE PKI PROFIL CERTIFICAT (CFR. ANNEXE C) .

6.2 Protection de la clé privée et contrôles du module cryptographique

6.2.1 Module cryptographique sécurisé

Le matériel informatique du dispositif cryptographique sécurisé est la puce NXP P5CC081, certifiée EAL5+.

L'applet "Belpic" V1.7 qui fonctionne sur la plateforme MultiAppID v2.1 80K CC avec la puce est certifiée EAL4+.

6.2.2 Génération de clé privée

La paire de clés (clé privée-publique) est générée sur la puce.

Seule la clé publique peut être exportée de la puce. La clé privée reste sécurisée dans la puce.

6.2.3 Contrôle multi-personnes de clé privée

Non applicable. Le dispositif cryptographique sécurisé ne doit être utilisé que par le Sujet désigné.

6.2.4 Entiercement de clé privée

Les clés privées ne peuvent pas et ne sont jamais extraites du dispositif cryptographique sécurisé sur lequel elles ont été générées. Les clés privées ne sont jamais mises en main tierce.

6.2.5 Back-up de clé privée

Les clés privées figurant sur un dispositif cryptographique sécurisé sont générées de façon intégrée dans le dispositif et ne peuvent pas faire l'objet d'un back-up.

6.2.6 Archivage de clé privée

Les clés privées figurant sur un dispositif cryptographique sécurisé sont générées de façon intégrée dans le dispositif et ne peuvent pas être extraites pour un back-up, un blocage ou l'archivage.

6.2.7 Transfert de clés privées vers ou à partir d'un module cryptographique

Les clés privées figurant sur un dispositif cryptographique sécurisé ne peuvent pas être transférées.

6.2.8 Stockage de clé privée dans un module cryptographique

Les clés privées figurant sur un dispositif cryptographique sécurisé sont stockées dans une mémoire sécurisée. La micropuce intégrée protège les clés privées et les autres informations liées à la sécurité contre le piratage.

6.2.9 Méthode d'activation des clés privées

Les données d'activation pour le dispositif cryptographique sécurisé sont constituées de codes PIN et PUK. Les codes PIN et PUK sont fournis au Sujet dans un emballage de protection inviolable tel qu'une lettre et/ou une enveloppe PIN scellées.

6.2.10 Méthode de destruction de la clé privée

La clé privée peut être bloquée ou même désactivée (bloquée de façon irréversible) si l'on tente à plusieurs reprises d'introduire un code PIN ou PUK incorrect.

6.2.11 Évaluation du module cryptographique

Des normes minimales pour les modules cryptographiques ont été spécifiées dans **ANNEXE B : EXIGENCES POUR LES AUTORITÉS DE CERTIFICATION.**

6.3 Autres aspects de la gestion de la paire de clés

Le TSP utilise des dispositifs cryptographiques appropriés pour réaliser les tâches de gestion de clé de la CA. Ces dispositifs cryptographiques s'appellent les Hardware Security Modules (HSM).

De tels dispositifs répondent aux conditions formelles (au minimum du FIPS 140-2 Niveau 3), qui garantit, entre autres choses, que toute tentative de violation du dispositif est immédiatement détectée et que les clés privées ne peuvent pas laisser les dispositifs non cryptés.

Les mécanismes informatiques matériels et logiciels qui protègent les clés privées de la CA sont documentés. Le document démontre que les mécanismes qui protègent les clés de CA sont de force au moins équivalente aux clés de CA qu'elles protègent.

6.3.1 Archivage des clés publiques

6.3.2 Périodes opérationnelles des certificats et périodes d'utilisation des paires de clés

Pour plus de détails, se référer au document : **EID-DEL-004 EID HIÉRARCHIE PKI PROFIL CERTIFICAT (CFR. ANNEXE C)**.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

L'activation de la racine CA est établie à l'aide des dépositaires de clés.

Les CA opérationnelles sont activées à l'aide d'un token opérationnel.

La clé du sujet est activée :

- Tout d'abord, à la réception de l'eID (QSCD) à l'administration communale :

- La carte et la clé peuvent seulement être activées à l'administration communale ;
- Avec la coopération de l'agent public.

- Pour l'activation opérationnelle, le code d'identification personnel du sujet est utilisé.

6.4.2 Activation de la protection des données

Pour la CA racine, les gardiens des clés ont chacun un rôle dans l'activation des clés, ces tokens sont protégés par un mot de passe. Le schéma de protection est M de N. Les tokens sont stockés dans une chambre forte.

Les CA opérationnelles sont protégées par un token opérationnel scindé et les (M de N) tokens sont protégés par un mot de passe. Les tokens sont stockés dans un coffre-fort.

La clé du sujet est protégée par un code PIN, le code PIN est transmis directement par courrier postal au sujet dans une enveloppe sécurisée. Les données d'activation doivent être mémorisées et pas notées sur un papier. Les données d'activation ne doivent jamais être partagées. Les données d'activation ne peuvent pas seulement contenir des informations qui pourraient être devinées facilement, par ex. les informations personnelles du détenteur du certificat.

6.4.3 Autres aspects des données d'activation

La CA stocke et archive en toute sécurité les données d'activation associées à sa propre clé privée et ses opérations.

6.5 Contrôles de la sécurité informatique

La CA met en œuvre des contrôles de sécurité informatique appropriés, y compris des contrôles d'accès physiques et logiques, la séparation des rôles, des contrôles à plusieurs niveaux, la détection d'intrusion et les processus d'authentification multi-facteurs pour l'ensemble du personnel pouvant entraîner l'émission d'un certificat ou permettre à une personne d'être capable de délivrer un certificat.

6.5.1 Mesures de sécurité technique spécifiques aux systèmes informatiques

La Foreigner CA fournit la fonctionnalité suivante par le biais du système d'exploitation et une combinaison du système d'exploitation, du logiciel PKI et des contrôles physiques :

- Contrôles d'accès aux services CA et rôles PKI ;
- Séparation forcée des tâches pour les rôles PKI ;
- Identification et authentification des rôles PKI et des identités connexes ;
- Utilisation de moyens cryptographiques pour les communications de la session et la sécurité de la base de données ;
- Archivage de l'historique et des données d'audit de la CA et des entités finales ;
- Audit des événements relevant de la sécurité ;
- Mécanismes de récupération des clés et du système de la CA.

Des informations concernant ces fonctions sont fournies dans les sections correspondantes de la présente DPC.

6.5.2 Indice de sécurité informatique

Section non applicable.

6.6 Contrôles de sécurité au cours du cycle de vie

Tout le matériel et les logiciels achetés pour faire fonctionner une CA émettrice dans la Foreigner CA doivent être achetés d'une manière qui permettra d'atténuer le risque que tout composant particulier puisse être altéré, comme la sélection aléatoire des composants spécifiques. Équipement développé pour une utilisation au sein de l'eID PKI doit être développé dans un environnement contrôlé en vertu des procédures strictes des contrôles de changement.

Une chaîne continue de la responsabilité, de l'endroit où tout le matériel et les logiciels identifiés comme soutenant une CA émettrice dans l'eID PKI, doit être maintenue en faisant en sorte qu'ils soient expédiés ou livrés par des méthodes contrôlées. L'équipement de la CA émettrice ne doit pas avoir installé une application ou un composant de logiciel ne faisant pas partie de la configuration de la CA émettrice. Toutes les mises à jour ultérieures des équipements de la CA émettrice doivent être achetées ou développées de la même manière que l'équipement d'origine et être installées par un personnel de confiance, formé d'une manière définie.

L'usine qui produit la CA a mis en place une politique de sécurité du système approuvé qui intègre des contrôles de sécurité informatique spécifiques à l'eID PKI et répond à ce qui suit :

6.6.1 Contrôles des développements du système

Les procédures formelles sont suivies pour le développement et l'implémentation de nouveaux systèmes. Une analyse des exigences de sécurité est menée à la phase de conception et du cahier des charges. Les projets de développement de logiciels externalisés sont étroitement surveillés et contrôlés.

6.6.2 Contrôles de la gestion de la sécurité

L'autorité du certificat étranger suit la Famille de Composantes d'émission et de gestion de certificat des profils de protection (CIMC) qui définit les exigences pour les composants qui émettent, révoquent et gèrent des certificats de clés publiques, tels que les certificats X.509. Le CIMC est basé sur les critères communs / normes ISO IS15408.

6.6.3 Contrôles de sécurité du cycle de vie

La CA utilise une méthodologie de gestion de configuration pour l'installation et la maintenance continue des systèmes d'autorité de certification. Le logiciel "Certificate Authority" fournira lors du premier chargement une méthode à la CA pour vérifier que le logiciel installé sur le système :

- Provient du développeur de logiciel ;
- N’a pas été modifié avant l'installation ;
- Est la version destinée à être utilisée.

Le chef de la sécurité CA vérifie périodiquement l'intégrité du logiciel Certificate Authority et surveille la configuration des systèmes du Certificate Authority.

6.7 Contrôles de sécurité du réseau

La CA assure la sécurité des systèmes, y compris des pare-feu. Les intrusions sur le réseau sont surveillées et détectées.

En particulier:

- Toutes les communications entre la CA et l'opérateur RA concernant l'une des phases du cycle de vie de certificats d'étranger sont sécurisées par des techniques de chiffrement et de signature fondées sur un système cryptographique à clé publique en vue de garantir la confidentialité et l'authentification mutuelle. Cela implique des échanges d'informations concernant la demande, la délivrance, la suspension, la réhabilitation après suspension et la révocation de certificats ;
- Le site web de la CA fournit des connexions encryptées par le biais du protocole Secure Socket Layer (SSL) et une protection anti-virus ;
- Le réseau de la CA est protégé par un pare-feu et un système de détection des intrusions ;
- Il est interdit d'accéder aux ressources sensibles de la CA, y compris les bases de données CA externes au réseau de l'opérateur CA ;
- Les sessions Internet pour la demande et la fourniture d'informations sont encryptées.

6.8 Horodatage

Section non applicable.

7. Certificat, CRL, et profils OCSP

7.1 Profil du certificat

Les profils et attributs du certificat sont décrits dans le document : **EID-DEL-004 eID HIÉRARCHIE PKI PROFIL CERTIFICAT (CFR. ANNEXE C) ET ANNEXE A EID PROFIL CERTIFICAT**.

7.1.1 .Numéro(s) de version

Cf. section 7.1

7.1.2 Extensions de certificat

Cf. section 7.1

7.1.3 Identificateurs des objets algorithmes

Cf. section 7.1

7.1.4 Formes des noms

Cf. section 7.1

7.1.5 Contraintes relatives aux noms

Cf. section 7.1

7.1.6 Identificateur d'objet de la politique de certification

Cf. section 7.1

7.1.7 Usage d'une extension de contraintes de politique

Cf. section 7.1

7.1.8 Syntaxe et sémantique des qualificatifs de politique

Cf. section 7.1

7.1.9 Sémantique de traitement pour l'extension critique de la politique de certification

Sans objet.

7.1.10 Validité du certificat

La validité d'un certificat Foreigner d'entité finale comporte deux contraintes :

- La période de validité ne doit pas dépasser 10 ans et 8 mois (*voir la section 7.1*) ;
- La période de validité du certificat ne peut pas dépasser la période de validité de la carte eID sur laquelle se trouve la puce dans laquelle réside le certificat.

La RA choisira toujours la période de validité la plus courte de ces deux contraintes lors de la génération de la demande d'émission de certificat.

7.2 Profil des CRL

Les profils et attributs des CRL sont décrits dans le document : **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C) et Annexe A eID profil certificat**.

7.2.1 Numéro(s) de version

Cf. section 7.2

7.2.2 Extensions des CRL et des entrées de CRL

Cf. section 7.2

7.3 Profil OCSP

Les profils et attributs des OCSP sont décrits dans le document : **EID-DEL-004 eID hiérarchie PKI profil certificat (cfr. Annexe C) et Annexe A eID profil certificat**.

7.3.1 Numéro(s) de version

Cf. section 7.3

7.3.2 Extensions OCSP

Cf. section 7.3

8. Audit de conformité et autres évaluations

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: Exigences pour les prestataires de service émettant des certificats qualifiés UE ;
- Profils EN 319 412-5 pour les prestataires de service de confiance délivrant des certificats ; profil de certificat qualifié. 5e partie : Extension pour profil de certificat qualifié.

Le TSP accepte les audits de conformité afin de s'assurer qu'il respecte les exigences, normes, procédures et niveaux de service conformément à la présente DPC. 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 confiance 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.

8.1 Fréquence ou circonstances des évaluations

L'entreprise PKI est auditée chaque année.

8.2 Identité/qualifications de l'évaluateur

Les services d'audit doivent être effectués par des cabinets d'audit ou des entreprises de conseil en technologie de l'information indépendants, reconnus, crédibles et établis ; à condition qu'ils soient qualifiés pour exécuter et qu'ils soient expérimentés dans la réalisation d'audits de la sécurité de l'information, ayant spécifiquement une expérience significative avec les technologies PKI et cryptographiques.

8.3 Relations de l'évaluateur avec l'entité évaluée

L'auditeur et la CA émettrice faisant l'objet d'un audit ne doivent pas avoir une relation qui porterait atteinte à l'indépendance et à l'objectivité de l'auditeur en vertu des normes d'audit généralement acceptées. Ces relations comprennent les relations financières, juridiques, sociales ou autres qui pourraient résulter en un conflit d'intérêts.

8.4 Sujets couverts par l'évaluation

L'audit aborde les aspects suivants :

- Conformité des principes et des procédures du TSP avec les procédures et les niveaux de service définis dans la DPC ;
- Gestion des infrastructures qui mettent en œuvre les services TSP ;
- Gestion des infrastructures physiques sur site ;
- Adhésion à la DPC ;
- Respect des lois belges afférentes ;
- Respect des niveaux de service convenus ;
- Inspection des rapports d'audit, des registres, des documents pertinents, etc. ;
- Cause de toute non-conformité aux conditions reprises ci-dessus.

8.5 Mesures prises à la suite du constat de lacunes

Si des irrégularités sont détectées, le TSP soumettra un rapport à l'auditeur, mentionnant les mesures qui seront prises pour rectifier la situation et garantir la conformité. Si les mesures proposées sont jugées insuffisantes, un second audit sera réalisé pour garantir la conformité.

8.6 Communication des résultats

L'avis d'audit basé sur les résultats des audits sera généralement disponible sur demande.

9. Autres points et considérations juridiques

Certaines conditions légales sont applicables à la délivrance de certificats de citoyen au sens de la présente DPC comme décrit dans cette section.

9.1 Honoraires

9.1.1 Délivrance de certificat ou renouvellement des honoraires

L'article 6 de la loi du 19 juillet 1991 visée sous le point §1.3 du chapitre 1, règle d'une part la question de la rétribution liée à l'insertion de certificat (art. 6,§ 5) et d'autre part la récupération des frais de fabrication des cartes d'identité à l'intervention du Ministre de l'Intérieur (art. 6, § 8).

La CA ne facture aucun honoraire pour la publication et le retrait de la présente DPC.

La CA fournira gratuitement les services suivants au citoyen :

- Publication des CRL et Delta CRL ;
- Accès aux pages web du référentiel ;
- Service web de vérification du statut via les pages du référentiel.

L'Autorité fédérale belge peut si besoin est accéder gratuitement aux ressources suivantes :

- Services de vérification du statut OCSP ;
- Téléchargement des CRL et delta CRL ;
- Service de vérification du statut du certificat ;
- Service de répertoire de certificat ;
- Publication de certificats ;
- Révocation de certificats ;
- Suspension de certificats.

La CA met en œuvre des mécanismes qui visent à protéger ces services de tout abus.

9.1.2 Honoraires d'accès certificat

Cf. section 9.1.1

9.1.3 Honoraires pour l'accès aux informations sur le statut ou la révocation

Cf. section 9.1.1

9.1.4 Honoraires pour les autres services

Cf. section 9.1.1

9.1.5 Politique de remboursement

Section non applicable.

9.2 Responsabilité financière

Le TSP est responsable de la tenue de ses livres comptables et registres conformément aux normes belges GAAP et recourra aux services d'un cabinet international d'experts-comptables pour fournir des services financiers, y compris des audits périodiques.

9.2.1 Couverture assurance

Le TSP fournit chaque année à l'organisme de surveillance du gouvernement une preuve des couvertures d'assurance.

9.2.2 Autres actifs

L'entreprise PKI et les autorités d'enregistrement maintiendront suffisamment d'actifs et de ressources financières pour effectuer leurs tâches dans l'eID PKI et seront raisonnablement capables de faire porter la responsabilité aux détenteurs de certificats et aux parties faisant confiance aux certificats.

9.2.3 Couverture de l'assurance ou de la garantie pour les entités finales

Section non applicable.

9.3 Confidentialité des informations d'entreprise

Dans le cadre des services prestés, la CA et l'opérateur RA (RRN) agissent en tant que « processeurs » de données à caractère personnel conformément à l'article 16 de la loi du 8 décembre 1992, alors que les administrations communales agissent en tant que « processeurs » pour le traitement des données à caractère personnel.

9.3.1 Portée des informations confidentielles

Le TSP respecte les réglementations relatives aux données à caractère personnel comme décrit dans cette DPC. Les informations confidentielles englobent :

- Toute information personnelle identifiable sur des citoyens, autres que celles reprises dans un certificat ;
- Le motif exact pour la révocation ou la suspension d'un certificat ;
- Les rapports d'audit ;
- Les informations consignées à des fins de reporting, tels que des enregistrements de requêtes par la RA ;
- La correspondance relative aux services CA ;
- La(les) clé(s) privée(s) CA.

9.3.2 Informations ne relevant pas des informations confidentielles

Les éléments suivants ne sont pas des informations confidentielles :

- Les certificats et leur contenu ;
- Le statut d'un certificat.

9.3.3 Responsabilité quant à la protection des informations confidentielles

Les parties qui demandent et reçoivent des informations confidentielles en reçoivent la permission à condition qu'elles les utilisent aux fins requises, qu'elles les sécurisent contre toute compromission, et s'abstiennent de les utiliser ou de les divulguer à des tiers.

Ces parties sont également tenues d'observer les règles régissant la protection des données à caractère personnel en conformité avec la loi.

9.4 Protection des informations personnelles

9.4.1 Protection de la vie privée

Le TSP ne divulgue pas, ni n'est tenu de divulguer, des informations confidentielles sans une demande authentifiée et justifiée spécifiant :

- La partie envers laquelle la CA est tenue au devoir de garder l'information confidentielle. La CA est tenue à une telle obligation envers la RA et répond promptement à toute demande de ce type ;
- Un ordre du tribunal.

Dans le cadre du Contrat Cadre entre le TSP et l'Autorité fédérale belge, le TSP peut facturer des frais administratifs pour procéder à de telles divulgations d'informations.

9.4.2 Informations traitées comme privées

Toutes les informations, c'est-à-dire concernant les détenteurs de certificat, ne seront pas divulguées par la CA aux citoyens, ni aux parties se fiant au certificat, à l'exception des informations :

- Sur eux-mêmes ;
- Sur des personnes dont ils ont la garde.

Seule la RA est autorisée à accéder aux informations confidentielles.

9.4.3 Informations non considérées comme privées

Des informations non confidentielles peuvent être divulguées à tout citoyen et partie se fiant au certificat aux conditions ci-après :

- Le statut d'un certificat unique est fourni sur demande d'un citoyen ou d'une partie se fiant au certificat ;
- Les citoyens peuvent consulter des informations non confidentielles que le TSP détient à leur sujet ;
- Le contenu des certificats numériques émis est considéré comme des informations publiques et ne sont donc pas privées.

9.4.4 Responsabilité à l'égard de la protection des informations privées

La CA gère en bonne et due forme la divulgation d'informations au personnel CA.

La CA s'authentifie à l'égard de toute partie qui demande la divulgation d'informations par :

- La signature des réponses aux demandes OCSP, aux CRL et delta CRL.

Le TSP crypte toutes les communications d'informations confidentielles, y compris :

- Le lien de communication entre la CA et la RA ;
- Les sessions visant à fournir les certificats.

Outre les informations conservées par le TSP, la RA conserve également des informations relatives aux certificats de citoyen, plus spécifiquement dans le registre des cartes d'identité. La loi belge du 19 juillet 1991 réglemente l'accès au registre des cartes d'identité et à d'autres données sur les citoyens qui sont détenus par le registre national.

9.4.5 Avis et consentement d'utilisation des informations privées

Le TSP agit dans les limites de la loi belge du 8 décembre 1992 sur la *protection de la vie privée à l'égard du traitement des données à caractère personnel* telle que modifiée par la loi du 11 décembre 1998 *transposant la directive européenne 1995/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. Ceci est conforme à loi de 13 juin 2005 *relative aux communications électroniques concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*. Et dans les limites du *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).*

Le TSP ne conserve pas d'autres données sur les certificats ou les citoyens autres que les données qui lui ont été transmises et autorisées par la RA. Sans le consentement de la personne concernée ou l'autorisation explicite par la loi, les données à caractère personnel traitées par le TSP ne seront pas utilisées à d'autres fins.

9.4.6 Divulgation dans le cadre d'un processus judiciaire ou administratif

Voir section 9.4.5

9.4.7 Autres circonstances de la divulgation des informations

certipost n'est soumise à aucune obligation de divulguer des informations autres que celles fournies par une ordonnance judiciaire légitime et légale et en conformité avec les exigences de la présente PC/DPC.

9.5 Droits de propriété intellectuelle

L'État belge détient et se réserve tous les droits de propriété intellectuelle associés à ses propres bases de données, ses sites web, les certificats numériques CA et toute autre publication, quelle qu'elle soit , provenant de la CA, y compris la présente DPC.

Le TSP détient et se réserve tous les droits de propriété intellectuelle qu'il détient sur ses propres infrastructures, bases de données, site web, etc.

Les logiciels et la documentation développés par le TSP dans le cadre du projet de carte d'identité électronique belge sont la propriété exclusive de l'État belge.

9.6 Représentations et garanties

Toutes les parties dans le domaine du TSP, en ce compris le CA lui-même, le CM, la RA, les LRA et les citoyens, garantissent l'intégrité de leur(s) clé(s) privée(s) respective(s). Si une desdites parties soupçonne qu'une clé privée a été compromise, elle informera immédiatement son LRA (administration communale), la police ou l'Helpdesk RA.

9.6.1 Représentations et garanties de la CA

Dans les limites de ce qui est spécifié dans les sections pertinentes de la DPC, le TSP :

- Se conformera à la présente DPC et à ses amendements tels que publiés sous eID Repository Website ;
- Fournira des services d'infrastructure et de certification, notamment l'établissement et le fonctionnement du centre de demande et du site web de la CA pour le fonctionnement de services de certification publique ;
- Fournira des mécanismes de confiance, et notamment un mécanisme de génération de clés, une protection de clé ainsi que des procédures de partage de secret concernant sa propre infrastructure ;
- Avertira rapidement la RA en cas de compromission de sa (ses) propre(s) clé(s) privée(s) ;
- Délivrera des certificats électroniques conformément à cette DPC et répondra à ses obligations telles que présentées dans la DPC ;
- Avertira la RA si la CA est incapable de valider l'application conformément à cette DPC;
- Agira rapidement pour délivrer un certificat conformément à cette DPC, après avoir reçu une demande authentifiée de la RA ;
- Révoquera rapidement un certificat conformément à la DPC, après avoir reçu une demande authentifiée de révocation de la part de la RA ;
- Suspendra rapidement un certificat conformément à la DPC, après avoir reçu une demande authentifiée de suspension de la part de la RA ;
- Lèvera rapidement la suspension d'un certificat conformément à la DPC, après avoir reçu une demande authentifiée de levée de la suspension de la part de la RA ;

- Publiera des certificats conformément à cette DPC ;
- Publiera les réponses CRL, delta CRL et OCSP de tous les certificats suspendus et révoqués, sur une base régulière, et conformément à cette DPC ;
- Fournira des niveaux de service appropriés selon un accord de niveau de service défini dans le cadre du contrat entre la CA et l'Autorité fédérale belge ;
- Fera une copie de cette DPC et des politiques en vigueur disponibles via son site web;
- Agira conformément aux lois belges. Concrètement, le TSP répondra à toutes les exigences légales associées à un profil de certificat qualifié émanant du Règlement UE 910/2014 sur les signatures électroniques.

Si le TSP prend connaissance ou soupçonne la compromission d'une clé privée, y compris la sienne, il avertira immédiatement la RA.

En cas de recours à des agents tiers, le TSP fera de son mieux pour garantir la responsabilité financière et civile adéquate dudit contractant.

Le TSP est, vis-à-vis des citoyens et des parties confiantes, responsable des actes ou omissions suivantes :

- La délivrance de certificats numériques ne reprenant pas les données telles que soumises par la RA ;
- La compromission d'une clé de signature privée de la CA ;
- Le fait de ne pas répertorier un certificat révoqué ou suspendu dans une CRL ou delta CRL ;
- La non-déclaration, par le répondeur OCSP, d'un certificat révoqué ou suspendu ;
- La non-déclaration, par une interface web, d'informations sur le statut du certificat ;
- La divulgation non autorisée d'informations confidentielles ou de données privées conformément aux sections 9.3 et 9.4 ;
- Responsable comme défini sous 9.8.1.

Le TSP reconnaît qu'il n'a pas d'autres obligations dans le cadre de cette DPC.

9.6.1.1 Confiance à ses propres risques et périls

Les parties accédant aux informations reprises au centre de demande, ainsi que sur le site web sont seules responsables de l'évaluation de ces informations et du crédit qu'elles leur accordent.

9.6.1.2 Précision des informations

Le TSP met tout en œuvre pour veiller à ce que les parties accédant au centre de demande reçoivent des informations précises, mises à jour et exactes. Le TSP, néanmoins, ne peut accepter une responsabilité au-delà des limites définies dans l'article 9.8.1 de la DPC.

9.6.2 Représentations et garanties de la RA

La RA agissant dans le domaine de la CA :

- Fournira des informations correctes et précises dans ses communications avec la CA ;
- Garantira que la clé publique soumise à la CA correspond à la clé privée utilisée ;
- Créera des demandes de certificats conformément à cette DPC ;
- Procédera à toutes les vérifications et authentifications prescrites par les procédures de la CA et de cette DPC ;
- Soumettra la demande du requérant à la CA, dans un message signé ;
- Recevra, vérifiera et transmettra à la CA toutes les demandes de révocation, suspension et réhabilitation après suspension d'un certificat conformément aux procédures de la CA et de la DPC ;
- Vérifiera l'exactitude et l'authenticité des informations fournies par le citoyen au moment du renouvellement d'un certificat conformément à cette DPC.

Si la RA prend connaissance de ou soupçonne la compromission d'une clé privée, elle informera immédiatement la CA.

Le RRN agit à titre de RA unique dans le domaine CA et a la responsabilité exclusive des répertoires qu'il tient à jour, y compris les répertoires de certificats. La RA est responsable de tous les audits qu'elle effectue, ainsi que des résultats et recommandations de ces audits.

La RA, par l'intermédiaire de la LRA, est seule responsable de l'exactitude des données du citoyen ainsi que de toute autre donnée cédée qu'elle fournit à la CA. La RA ne tiendra pas la CA pour responsable de tous les dommages encourus à la suite de données non vérifiées qui ont été reprises dans un certificat.

La RA se conforme aux lois et règlements belges relatifs au fonctionnement du RRN et est responsable de ses actes ou omissions en vertu de la législation belge.

9.6.3 Représentations et garanties du sujet

Sauf mention contraire dans la DPC, les obligations du citoyen impliquent ce qui suit :

- S'abstenir de falsifier un certificat ;
- Utiliser uniquement des certificats à des fins légales et autorisées, conformément à la DPC ;
- Demander une nouvelle carte d'identité électronique (et donc des certificats de citoyen) en cas de modification des informations publiées dans le certificat ;
- S'abstenir d'utiliser la clé publique de citoyen dans un certificat de citoyen 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 docstop pour 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 des indications de perte, vol, modification, divulgation non autorisée ou autre compromission de la clé privée d'un des certificats de citoyen, ou des deux ;
- Avertir la police, l'administration communale ou docstop pour 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 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 du sujet ;
- Dès compromission, l'obligation d'arrêter immédiatement et définitivement l'usage de la clé privée ;
- Obligation de notification 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).

9.6.4 Représentations et garanties de la partie se fiant au certificat

Les parties se fiant à un certificat de la CA :

- Seront suffisamment informées sur l'utilisation de certificats numériques et PKI ;
- Seront informées et adhèreront aux conditions de cette DPC, ainsi qu'aux conditions associées pour les parties confiantes ;
- Valideront 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 l'Helpdesk de la RA.

9.6.5 Représentations et garanties des autres parties

Obligations du producteur de cartes (CM) : le producteur des cartes d'identité électroniques (CM) est responsable de l'initialisation, de la personnalisation et de la distribution des cartes d'identité contenant 0, 1 ou 2 certificat(s) de citoyen.

L'initialisation comprend les opérations suivantes dans la carte à puce :

- La génération des paires de clés pour le certificat d'identification et de signature ;
- Le stockage des données d'identification, des certificats d'identification et de signature dans la carte à puce ;
- L'authentification des données, ainsi que l'initialisation des différents fichiers stockés sur la carte d'identité électronique.

Le CM collectera en toute sécurité les documents de base et distribuera les lettres de convocation, les nouvelles cartes d'identité personnalisées et initialisées, ainsi que les lettres sécurisées destinées aux citoyens et qui contiennent les codes PIN et PUK.

Le CM mettra en œuvre un processus sécurisé pour récupérer les cartes d'identité non valides ou annulées auprès des administrations communales et les détruire.

9.7 Dégagements de garantie

Dans la limite fixée par la loi belge, la CA ne sera en aucun cas (sauf en cas de fraude ou d'inconduite délibérée) responsable pour :

- La perte de profits ;
- La perte de données ;
- Tous préjudices indirects, consécutifs ou punitifs découlant de ou en rapport avec l'utilisation, la livraison, la licence et l'exécution ou la non-exécution de certificats ou signatures numériques ;
- Tout autre préjudice.

9.8 Limitations de responsabilité

9.8.1 Les responsabilités du TSP

La responsabilité du TSP à l'égard du sujet 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.

9.8.2 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 personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de :

- 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 ;
- 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 ;

- L'assurance que la clé privée et la clé publique puissent 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.

9.8.3 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 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'identité est utilisé dans le contexte d'applications permettant l'utilisation du certificat d'identité pour la génération de signatures électroniques.

9.8.4 Responsabilité exclue

Le TSP n'est en aucun cas responsable de toute 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 PC/DPC 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 cryptosystèmes 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.

9.9 Indemnités

Cf. section 9.8

9.10 Durée et Résiliation de la PC/DPC

9.10.1 Durée

La présente PC/DPC devient effective dès la publication dans le référentiel eID. Les amendements à cette PC/DPC entrent en vigueur dès leur publication dans le référentiel eID.

9.10.2 Résiliation

La présente DPC reste d'application jusqu'à communication contraire par la CA dans son référentiel, sur le site eID Repository Website.

9.10.3 Effet de la cessation des activités et survie

Les dispositions de la présente Citizen CA PC/DCP survivront à la cessation des activités ou au retrait d'un détenteur de certificat ou une partie se fiant au certificat de l'eID PKI en ce qui concerne toutes les actions basées sur l'utilisation ou se fondant sur un certificat numérique ou une autre participation au sein de l'eID PKI. Une telle cessation ou un tel retrait ne doit pas porter atteinte ou affecter un droit d'action ou un recours pouvant être accordé à toute personne, jusqu'à et y compris la date du retrait ou de la cessation.

9.11 Remarques individuelles et communications avec les participants

Les remarques relatives à cette DPC peuvent être adressées à : *Cf. section 1.6.1.*

9.12 Amendements

9.12.1 Procédure d'amendement

Les changements apportés à cette DPC sont gérés par l'Administration de la politique responsable du TSP**.** Tous les changements proposés par rapport à la DPC doivent être approuvés par le Conseil de gestion PKI.

9.12.2 Notification du mécanisme et de la période

Après approbation, une nouvelle version de la DPC est générée et publiée en plus de la version antérieure sur le site web (eID Repository Website).

9.12.3 Circonstances dans lesquelles l'OID doit être changé

Les changements mineurs apportés à la présente DPC qui n'affectent pas matériellement le niveau de garantie de cette DPC sont identifiés par un changement du nombre décimal (par exemple version 1.1 au lieu de 1.0), alors que les changements majeurs sont identifiés par un changement du numéro de version au niveau du nombre entier (par exemple version 2.0 au lieu de 1.0).

Les changements mineurs apportés à cette DPC ne requièrent aucun changement dans la DPC OID ou au niveau du pointeur vers la DPC (URL) qui pourrait être communiqué par la CA. Les changements majeurs susceptibles de modifier matériellement l'acceptabilité de certificats destinés à des fins spécifiques peuvent requérir des changements adaptés au niveau de la DPC OID ou du pointeur vers la DPC (URL).

9.13 Dispositions de règlement de différends

Tous les litiges associés à la présente DPC seront réglés conformément à la législation belge.

Les plaintes relatives à la présente DPC et aux certificats doivent être adressées à : *Cf. section 1.6.1.*

Un accusé de réception sera envoyé dans les 2 jours ouvrables suivant la réception de la plainte. Une réponse sera fournie dans les 10 jours ouvrables suivant la réception de la plainte.

Conformément à la loi belge sur la signature numérique tout arbitrage, sauf convention contraire entre les parties, a lieu en Belgique.

9.14 Droit applicable

Le TSP fournit ses services conformément aux dispositions de la loi belge et du Règlement UE 910/2014.

9.15 Respect de la loi applicable

La présente PC/DPC est soumise au droit applicable.

9.16 Dispositions diverses

Le TSP incorpore par référence les informations suivantes dans tous les certificats numériques qu'il délivre :

- Les termes et conditions décrits dans la présente DPC ;
- Toute autre politique de certificat applicable, telle qu'elle peut être précisée sur un certificat de citoyen délivré ;
- Les éléments obligatoires des normes applicables ;
- Les éléments non obligatoires mais personnalisés des normes applicables ;
- Le contenu d'extensions et la dénomination améliorée non abordée ailleurs ;
- Toute autre information indiquée comme telle dans un champ d'un certificat.

Pour incorporer par référence des informations, la CA utilise des pointeurs basés sur un ordinateur ou sur du texte et incluant des URL, OID, etc.

9.16.1 Intégralité de la Convention

Section non applicable.

9.16.2 Cession

Section non applicable.

9.16.3 Divisibilité

Toute disposition de cette Citizen CA PC/DPC qui est déterminée invalide ou inapplicable sera sans effet dans la mesure de cette détermination, sans invalider les autres dispositions de cette Citizen CA PC/DPC ou sans affecter la validité ou l'applicabilité de ces autres dispositions.

9.16.4 Application (honoraires d'avocats et renonciation de droits)

L'échec ou le retard du TSP à exercer ou à appliquer un droit, pouvoir, privilège ou n'importe quel recours que ce soit ou conféré autrement par le présent Citizen CA PC/DPC ; ne doit pas être considéré comme une renonciation à un tel droit ou opérer de manière à interdire l'exercice ou l'exécution de celui-ci à tout moment par la suite, aucun exercice unique ou partiel d'un tel droit, pouvoir, privilège ou recours n'empêchera l'exercice ultérieur de ce droit ou l'exercice de n'importe quel autre droit ou recours. Aucune renonciation n'est effective à moins qu'elle ne soit effectuée par écrit. Aucun droit ou recours conféré par l'une des dispositions de la présente Citizen PC/DPC n'est destiné à être exclusif de tout autre droit ou recours, sauf stipulation expresse dans la présente Citizen PC/DPC, et tous les droits ou recours sont cumulatifs et s'ajoutent à tout autre droit ou recours mentionné ci-dessous ou qui existent ou existeront en droit ou en justice ou du fait d'une loi ou autre.

9.16.5 Force majeure

Le TSP décline toute responsabilité en cas de violation de la garantie, de retard ou de défaut d'exécution résultant d'événements échappant à son contrôle, tels que les cas de force majeure, les actes de guerre, les actes de terrorisme, les épidémies, panne de courant ou des

services de télécommunications, incendie et autres catastrophes naturelles. Voir aussi section 9.8.2 (Responsabilité exclue) ci-dessus.

9.17 **Autres dispositions**

Section non applicable.

Annexes

This page is intentionally left blank

Annexe A

Définitions et acronymes

CA	Autorité de certification
CC	Critères communs
CM	Producteurs de cartes
CP	Politique de certificat
DPC / CPS	Déclaration de Pratiques de Certification
CRL	Liste de révocation de certificats
EAL	Niveau d'évaluation sécuritaire
eIDAS	Règlement UE 910/2014 également connu sous le nom de règlement d'eIdentification et de signature
OID	Identificateur d'objet
(L)RA	Autorité d'enregistrement (Locale)

Annexe B

EXIGENCES POUR LES AUTORITÉS DE CERTIFICATION

Les modules cryptographiques utilisés par les autorités de certification DOIVENT être évalués et certifiés au regard de l'une des normes suivantes :

- FIPS PUB 140-2 niveau 3 ou supérieur
- PP-SSCD 4,5,6
- Modules cryptographiques BSI, Niveau de sécurité «accru»

Annexe C

ISSUING CAs eID HIÉRARCHIE PKI PROFIL CERTIFICAT EXTRAIT DE EID-DEL-004

Starting from next page

Table of contents

1. Certificate profiles

The different CAs are profiled according to PKIX certificate profile, and made up to three parts according to RFC5280: tbsCertificate, Signature algorithm and Signature value.

Note: All the URI's specified in the certificate profiles are resolved by BOSA[1].

Hereunder the most significant certificate profile fields will be described. Changes that were made to these fields during the course of the eID project are reflected by specifying a release date, which is the date the change was put in operations.

1.1 Version

The version field indicates the X.509 version of the certificate format. In eID project, only certificates complying with version 3 of the X.509 recommendation, allowing for extensions, are used.

Version	
All certificates	Version 3 – Value = "2"

1.2 Certificates Serial Number

The field certificate serial number specifies the unique, numerical identifier of the certificate within all certificates issued by the same Certification Authority (CA).

The RRN[2] can assign a serial number to the eID hierarchy certificates.

The CA operator checks the uniqueness of the end-user certificate serial numbers before processing the certification requests.

All serial numbers are maximal 16 bytes long, except for the Self-signed Belgium Root CA2 were the serial number is 8 bytes.

Serial Number	
eID hierarchy certificates	Generated by the CA at the time of Key Generation Process

Remark: if no serial number is received in the requests issued by the RRN, the CA provider will generate this number using its own allocation scheme.

[1] BOSA is the acronym for FOD beleid en ondersteuning / Stratégie et appui

[2] RRN is an acronym for Rijksregister – Registre National

1.3 Signature

The signature field determines the cryptographic algorithm used by a CA to sign a certificate. The algorithm identifier, which is a number registered with an internationally recognised standards organisation, specifies both the public-key algorithm and the hashing algorithm used by the CA to sign certificates. The Object Identifier for SHA1withRSA is 1.2.840.113549.1.1.5. The Object Identifier for SHA256withRSA is 1.2.840.113549.1.1.11.

Signature	
Certificates under BRCA1, BRCA2 and BRCA3	SHA1withRSA
Certificates under BRCA4	SHA256withRSA

1.4 Issuer

The Issuer field identifies the certification authority that has signed and issued the certificate. Issuer is structured as a "Distinguished Name", that is a hierarchically structured name, composed of attributes, most of which are standardised in the X.500 attributes. The ones used are: country, organisation, serial number, common name, locality. The subject serial number mentioned in the issuer field is the serial number attributed by the RRN to identify the CA.

Issuer		
Certificate	Releases	Field attributes
eID hierarchy Operational CA certificates Citizen CA, Foreigner CA	<2008 >=2008 >=06/2013	C: BE, CN: Belgium Root CA C: BE, CN: Belgium Root CA2 C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4
End user certificates Citizen	<2005 >=2005	C: BE, CN: Citizen CA C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[3]
Foreigner		C: BE, CN: Foreigner CA, Serial Number: <yyyy><ss>
End user certificates Citizen		C: BE, CN: Citizen CA,

[3] See paragraph 4.1 Serial number to reference a CA

Foreigner	>=2017	Serial Number: <yyyy><ss>[4] O: certipost N.V. / S.A. L: Brussels C: BE, CN: Foreigner CA, Serial Number: <yyyy><ss> O: certipost N.V. / S.A. L: Brussels

1.5 **Validity**

The validity field indicates the time interval during which the certificate can be used and on which the issuing CA maintains certificate status information.

The certificates can be used, unless a certificate is suspended or revoked during its period of validity. Validity should be interpreted as the period when the (non-revoked) certificate can be trusted to perform a certain transaction. All transactions executed after this period based on the certificate should be handled as not trusted.

Validity				
	Release	Not before	Not after	Validity period[5]
eID hierarchy Operational CA certificates Citizen CA Foreigner CA	2003/1 2003/2 >2004 - <2014 >=2014 >=2006 >=2015			6y 5m 6y 2m 6y 8m 11 yr, 8m 6y 8m 11y 8m
	Release	Standard validity period[6]		
eID hierarchy End user certificates Citizen	2003/1 2003/2 2004 2005 2006 2007 2008 >=2014			5 years 5 years 5 years 5y 3m 5y 3m 5y 3m 5y 3m 10y 3m

[4] See paragraph 4.1 Serial number to reference a CA

[5] Certificate validity periods defined during key ceremony.

[6] for end user certificates variable validity periods are applied from April 1st 2006.

Foreigner	>=2006 >=2015	5y 3m 10y 3m

1.6 **Subject**

The Subject field identifies the entity holding the private key corresponding to the public key published in the certificate. Subject is structured as a set of attributes, defined in the X.500 attributes.

Subject		
Certificate	Release	Field attributes
eID hierarchy		
Root certificate		
Belgium Root CA Self-signed crt	<2008 >=2008-2013 >=2013	C: BE, CN: Belgium Root CA C: BE, CN: Belgium Root CA2 C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4
Operational CA certificates		
Citizen CA	<2005 >=2005 >=2017	C: BE, CN: Citizen CA C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[7] C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[8] O: certipost N.V. / S.A. L: Brussels
Foreigner CA	<2017 >=2017	C: BE, CN: Foreigner CA, Serial Number: <yyyy><ss> C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[9] O: certipost N.V. / S.A. L: Brussels
End user certificates		

[7] See paragraph 4.1 Serial number to reference a CA

[8] See paragraph 4.1 Serial number to reference a CA

[9] See paragraph 4.1 Serial number to reference a CA

Citizen, Foreigner RRN signing	>=2005	See Table "End use certificate Subject field (eID Hierarchy)" C:BE, CN:RRN, O:RRN

End user certificate Subject fields definition (eID hierarchy)			
Field	**Length**	**Description**	**Example**
C (countryName)	2	countryName is a dynamic element corresponding to the two letter country code ISO3166 standard. The country code is provided with the certificate creation request by the RRN. It is not checked by the CA.	C=BE
CN (commonName)	Max 255 Min 1	Concatenation of • <given name>: first given name of the card holder • <surname>: surname of the eID card owner • (<purpose>): (Authentication) or (Signature)	CN=John Smith (Authentication) CN=John Smith (Signature)
surname	Max 255 Min 1	Surname of the eID card owner	S=Smith
givenName	Max 255 Min 1	1 or 2 given names of the eID card owner (This field may not appear in case the owner has no given name)	G=John William
subjectSerialNumber	Max 255 Min 1	This is a unique number provided by the RRN ("Rijksregisternummer" – 11 digits long).	SN=12345678901

The CA operator does not perform a check on the content provided by the RRN, except that the subject distinguished name has to be unique.

1.7 Subject Public Key Info

The Subject Public Key Info field is used to carry the public key being certified and identify the algorithms with which the key has been generated.

Subject Public Key Info	
eID hierarchy	
Root certificate	
Self-signed Belgium Root CA1 & 2	RSA 2048 bits key
Self-signed Belgium Root CA3 & 4	RSA 4096 bits key
Operational CA certificates	
Citizen CA, Foreigner CA <2014	RSA 2048 bits key
Citizen CA, Foreigner CA >=2014	RSA 4096 bits key
End user certificates	
Citizen, Foreigner <2014	RSA 1024 bits key
Citizen, Foreigner CA >=2014	RSA 2048 bits key

1.8 Key usage

The Key usage field specifies the purpose of the key contained in the certificate.

Key usage									
Key usage	Digital Signature	Non Repudiation	Key Encipherment	Data Encipherment	Key Agreement	Key Certificate Signing	Crl Signing	Encipher Only	Decipher Only
eID hierarchy									
Root certificate									
Self-signed Belgium Root CA	NA	NA	NA	NA	NA	A	A	NA	NA
Operational CA certificates									
Citizen CA, Foreigner CA	NA	NA	NA	NA	NA	A	A	NA	NA
End user certificates									
Citizen, Foreigner Authentication crt	A	NA	NA	NA	NA	NA	NA	NA	NA
Citizen, Foreigner Signature crt	NA	A	NA	NA	NA	NA	NA	NA	NA

The digital signature bit is not asserted in the Citizen & Foreigner Signature Certificates for strict application of the standards, and to prevent possible mistakes with applications.

1.9 Extended Key usage

The Extended Key usage field specifies the purpose of the key contained in the certificate.

Extended Key usage							
Extended Key usage	Any Key Usage	Server Authentication	Client Authentication	Code Signing	Email Protection	Time Stamping	OCSP Signing
eID hierarchy							
Root certificate							
Self-signed Belgium Root CA	NA	NA	NA	NA	NA	NA	NA
Operational CA certificates							
Citizen CA, Foreigner CA	NA	NA	A	NA	A	NA	NA
End user certificates							
Citizen, Foreigner Authentication crt	NA	NA	A	NA	NA	NA	NA
Citizen, Foreigner Signature crt	NA	NA	NA	NA	A	NA	NA

The client authentication & email protection bit is asserted in the Citizen & Foreigner CA Certificates to comply with the CA/B Forum's Baseline requirements regarding technical constraints for the eID PKI.

1.10 Authority and Subject Key Identifiers

To facilitate certification path construction, the authority and subject key identifier appears in all conforming CA certificates, that is, all certificates including the basic constraints extension where the value of CA is TRUE. The value of the subject key identifier is the value placed in the key identifier field of the Authority Key Identifier extension of certificates issued by the subject of this certificate.

The Authority Key Identifier extension is present in the Root signing and end user certificates of the eID hierarchy.

The Subject Key Identifier will be present in the Citizen CA and the Foreigner CA certificate(s). It will not be present in end-user certificates.

1.11 NetscapeCertType

This extension was removed as from 05/2017. This extension can be used to limit the applications for a certificate. If the extension exists in a certificate, it will limit the uses of the certificate to those specified. If the extension is not present, the certificate can be used for all applications except Object Signing.

- bit-0 SSL client - this cert is certified for SSL client authentication use
- bit-1 SSL server - this cert is certified for SSL server authentication use

- bit-2 S/MIME - this cert is certified for use by clients
- bit-3 Object Signing - this cert is certified for signing objects such as Java applets and plugins
- bit-4 Reserved - this bit is reserved for future use
- bit-5 SSL CA - this cert is certified for issuing certs for SSL use
- bit-6 S/MIME CA - this cert is certified for issuing certs for S/MIME use
- bit-7 Object Signing CA - this cert is certified for issuing certs for Object Signing

NetscapeCertType Key usage extension								
Netscape Key usage	bit-0 - SSL client	bit-1 - SSL server	bit-2 - S/MIME	bit-3 - Object Signing	bit-4 - Reserved	bit-5 - SSL CA	bit-6 - S/MIME CA	bit-7 - Object Signing CA
eID hierarchy								
Root certificate								
Self-signed Belgium Root CA	NA	NA	NA	NA	NA	A	A	A
Operational CA certificate								
Citizen CA, Foreigner CA	NA	NA	NA	NA	NA	A	A	A
End user certificates								
Citizen, Foreigner Authentication crt	A	NA	A	NA	NA	NA	NA	NA
Citizen, Foreigner Signature crt	NA	NA	A	NA	NA	NA	NA	NA

1.12 **Policy mapping**

This extension is only useful in case of cross-certification between CAs. It makes indeed little sense to have a policy mapping between a commercial CA and a Governmental CA. Also this extension is not handled by Netscape or by Microsoft products. As such the Policy Mapping has not been implemented.

1.13 **Policy constraint**

This extension can be used in CA certificates only. It can be used to constrain path validation in two ways: to prohibit policy mapping, or to require that each certificate in a path contain an acceptable policy identifier. If present, this extension should be marked critical [X509].

For the same reasons as mentioned in chapter 1.12, the Policy Constraint has not been implemented.

1.14 **Certificate policies**

Certificate policies are identified in the eID certificates using a CPS Pointer qualifier containing a pointer to the Certification Practice Statement (CPS) published by the CA.

The same sequence will be used for all eID certificates as it has been decided this qualifier will point to a web page that may reference multiple applicable documents.

With the implementation of the Belgium Root CA2 new OID's are being used to address the different policy in the certificate profiles. The new OID tree that is used is 2.16.56.9.1.*

With the implementation of the Belgium Root CA3 new OID's are being used to address the different policy in the certificate profiles. The new OID tree that is used is 2.16.56.10.1.*

With the implementation of the Belgium Root CA new OID's are being used to address the different policy in the certificate profiles. The new OID tree that is used is 2.16.56.12.1.*

Certificate Policies				
	Policy Identifier	Policy Qualifiers	Policy Qualifier Id	Qualifier
eID hierarchy				
Operational CA certificates				
Citizen CA	2.16.56.1.1.1.2 2.16.56.9.1.1.2 2.16.56.10.1.1.2 2.16.56.12.1.1.2	NA	CPS	eID Repository Website
Foreigner CA	2.16.56.1.1.1.7 2.16.56.9.1.1.7 2.16.56.10.1.1.7 2.16.56.12.1.1.7	NA	CPS	eID Repository Website
End user certificates				
Citizen Authentication certificate	2.16.56.1.1.1.2.2 2.16.56.9.1.1.2.2 2.16.56.10.1.1.2.2 2.16.56.12.1.1.2.2	NA	CPS	eID Repository Website
Citizen Signature certificate	2.16.56.1.1.1.2.1 2.16.56.9.1.1.2.1 2.16.56.10.1.1.2.1 2.16.56.12.1.1.2.1	NA	CPS	eID Repository Website

Foreigner Authentication certificate	2.16.56.1.1.1.7.2 2.16.56.9.1.1.7.2 2.16.56.10.1.1.7.2 2.16.56.12.1.1.7.2	NA	CPS	eID Repository Website
Foreigner Signature certificate	2.16.56.1.1.1.7.1 2.16.56.9.1.1.7.1 2.16.56.10.1.1.7.1 2.16.56.12.1.1.7.1	NA	CPS	eID Repository Website

1.15 Basic constraint

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-user. If the subject may act as a CA, then the certificate is a cross-certificate, and it may also specify the maximum acceptable length of a certificate beyond the cross-certificate. This extension should always be marked as critical; otherwise some implementations will ignore it and allow a non-CA certificate to be used as a CA certificate.

Basic constraint extension		
	CA	Path Lenght Constraint
eID hierarchy		
Root certificate		
Self-signed Belgium Root CA	TRUE	None
Operational CA certificate		
Citizen CA, Foreigner CA	TRUE	0
End user certificates		
Citizen, Foreigner Authentication	FALSE	-
Citizen, Foreigner Signature	FALSE	-

1.16 CRL Distribution Point

The CRL Distribution Points extension identifies the CRL distribution point or points to which a certificate user should refer to ascertain if the certificate has been revoked. A certificate user can obtain a CRL from an applicable distribution point or it may be able to obtain a current complete CRL from the authority directory entry.

CRL Distribution Point extension (CDP)		
	Releases	Distribution Point
eID hierarchy		
Operational CA certificates		
Citizen CA	<2008	http://crl.eid.belgium.be/belgium.crl
	>=2008	http://crl.eid.belgium.be/belgium2.crl
Foreigner CA	<2014	
	>=2014	http://crl.eid.belgium.be/belgium3.crl
		http://crl.eid.belgium.be/belgium4.crl
End user certificates		
Citizen certificates	2003/1	http://crl.eid.belgium.be/eidc0001.crl
	2003/2	http://crl.eid.belgium.be/eidc0002.crl
	2004	http://crl.eid.belgium.be/eidc2004-1.crl
	>=2005	http://crl.eid.belgium.be/eidc<yyyy><ss>[10].crl
Foreigner certificates		http://crl.eid.belgium.be/eidf<yyyy><ss>.crl

1.17 Freshest CRL - Delta CRL Distribution Point

This field is implemented for CRL certificates issued by operational CA certificates.

The freshest CRL extension identifies how delta CRL information is obtained.

The same syntax is used for this extension and the CRL Distribution point extension, and is described in Section 5.15.

1.18 Authority Information Access

The Authority Information Access extension indicates how to access the information and services provided by the issuer of a certificate, such as on-line validation services or LDAP server location.

An HTTP reference to the issuing CA has been added as a caIssuers element in order to allow the certificate chain to be reconstructed up to a trusted root.

[10] See paragraph 4.2 CRL and delta CRL names

Authority Information Access extension		
	Access Method	Access Location
eID hierarchy		
Root certificate		
Self-signed Belgium Root CA	None	None
Operational CA certificate		
Citizen CA, Foreigner CA	None	None
>2017	id-ad-ocsp (OCSP)	http://ocsp.eid.belgium.be/2
	id-ad-caIssuers (HTTP)	http://certs.eid.belgium.be/belgiumrs4.crt
End user certificates		
Citizen, Foreigner certificates		
<2008	id-ad-ocsp (OCSP)	http://ocsp.eid.belgium.be
>=2008 <2014		
>=2014		http://ocsp.eid.belgium.be/2
		http://certs.eid.belgium.be/belgiumrs.crt
<2008	id-ad-caIssuers (HTTP)	http://certs.eid.belgium.be/belgiumrs2.crt
>=2008 <2014		http://certs.eid.belgium.be/belgiumrs3.crt
>=2014		http://certs.eid.belgium.be/belgiumrs4.crt
>2017		http://certs.eid.belgium.be/<issuingca>

RFC5280 specifies: “The id-ad-caIssuers OID is used when the additional information lists CAs that have issued certificates superior to the CA that issued the certificate containing this extension. The referenced CA issuers’ description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.” It has no practical use to put accessMethod caIssuers in the Admin hierarchy and the eID Operational CA certificates. The LDAP access method will not be used in any of the eID certificate profiles described in this document.

1.19 Subject Directory attributes

The Subject Directory Attributes are applicable to Citizen or Foreigner certificates only, and convey any desired Directory attribute values for the subject of the certificate that are complement to the information contained in the subject field. This extension is always non-critical.

No subject directory attributes will be present in the eID certificates

1.20 Qualified Certificate Statement

The Qualified Certificate Statement, identified by the OID { id-etsi-qcs 1 } is present in end-user signature certificates as per ETSI TS 101 862 V1.3.2.

As from 05/2017 the Qualified Certificate Statements, identified by the OIDs { id-etsi-qcs 4 } { id-etsi-qcs 5 } { id-etsi-qcs 6 } are present in end-user signature certificates.

2. CRL profiles

The CRLs and Δ CRLs will be created according to the profiles as described in the chapters 2.1 and 2.2. All CRLs and Δ CRLs are signed by the issuing CA.

2.1 CRL Profile

Version	v2
Signature	Sha256RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time> + 7 days
RevokedCertificates	
UserCertificate	<certificate serial number>
RevocationDate	<revocation time>
CrlEntryExtensions	
CRL Reason Code	certificateHold(6) (for suspended certificates) Note: otherwise not included
CrlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
Freshest CRL	non-critical <location of delta CRL>
CRL Number	non-critical <The CA operator assigned unique number>
ExpiredCertsOnCRL	non-critical <GerneralizedTime of Bootstrap of the CitizenCA>

'nextUpdate' is the latest time that the CRL can be used by the certificate holder.

2.2 Δ CRL Profile

Version	v2
signature	Sha256RSA
Issuer	<subject CA>
thisUpdate	<creation time>
nextUpdate	<creation time> + 7 days
RevokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
CRL Reason Code	certificateHold(6) (for suspended certificates) removeFromCrl(8) (to unsuspend certificates) Note: otherwise not included

crlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <The CA operator assigned unique number>
Delta CRL Indicator	critical <base CRL Number>
ExpiredCertsOnCRL	non-critical < GerneralizedTime of Bootstrap of the CitizenCA >

'nextUpdate' is the latest time that the delta CRL can be used by the certificate holder.

2.3 CRL Issuance Frequency

Each Citizen / Foreigner CA issues a CRL every three hours. Each Citizen / Foreigner CA also issues a ΔCRL certificate corresponding to the previous CRL every three hours.

3. CA configuration settings

The table below specifies the configuration settings on the CA's these configuration settings are explained hereafter

CA configurations settings								
Setting	Auto-revocation	Unique DN check	Group	Variable validity	Delta CRL creation			
eID hierarchy								
Operational CA certificates								
Citizen CA	A	A	G1[11]	A	A			
Foreigner CA	NA	A	G1	A	A			

3.1 Auto-revocation

Auto-revocation is the configuration setting which automatically revokes a certificate which has been suspended for more than a week after being active. Certificates which are created get the suspend status upon creation; called initial suspend. Certificates with the initial suspend status are not revoked after one week because these certificates were never active before.

3.2 Unique DN check

The Subject Distinguished Name (DN) consists of a set of selected certificate subject fields which is used to uniquely identify the subject of a certificate. The Unique DN check guarantees that only one certificate with a specific DN can be active at a time.

The unique DN check is carried out when a certificate is:

1) Un-suspended
2) Generated with a 'Valid' status.

The unique DN check applies to all certificates issued under the CA's belonging to the same unique DN group.

[11] Citizen CA and Foreigner CA are included in the same unique DN group G1

3.3 Variable validity

Variable validity is the CA configuration setting which provide the possibility to change the default validity period (Start of Validity and End of Validity) of requested certificates.

The variable validity feature is only available through XKMS interface.

3.4 Delta CRL

As the creation of delta CRLs is not a requirement for all CA's it is one of the specific configuration parameters of a CA.

4. Naming conventions

This chapter reflect the latest naming conventions and are not necessarily coherent with the names used in the past. Applying the naming conventions below is mandatory for all future changes to the PKI hierarchy and certificate profiles.

4.1 Serial number to reference a CA

<Serial number>			
Characteristics	**Length**	**Format**	**Range**
Multiple versions of the same CA issued in the same year	7	<yyyy><ss> ○ <yyyy> represents the year where the CA will be used ○ <ss> represents the unique serial number to be added for that year Applicable for: ○ certificate subject or issuer field serial numbers ○ CRL and dCRL file names ○ CA certificate file names	2003 .. 9999 01 .. 99
Single version of a CA issued per year	4	<yyyy> ○ <yyyy> represents the year where the CA will be used Applicable for: ○ certificate subject or issuer field serial numbers ○ CRL and dCRL file names ○ CA certificate file names	2003 .. 9999

Remark: The CA's created for the year 2008 the following scheme with respect to the serial numbers:

- CA'S created under Belgium Root CA:
  - Citizen 200801 until 200816
  - Foreigner01 until Foreigner04
- CA's created under Belgium Root CA2:
  - Citizen 200817 until 200820
  - Foreigner200805
- >2009 created under BRCA2

4.2 CRL and delta CRL names

<CRL and delta CRL names>			
CA	**type**	**Format**	**Example**
Citizen CA	Base CRL	eidc<serial number>.crl	eidc201721.crl
	Delta CRL	eidcd<serial number>.crl	eidcd201721.crl
Foreigner CA	Base CRL	eidf<serial number>.crl	eidf201721.crl
	Delta CRL	eidfd<serial number>.crl	eidfd201721.crl

4.3 CA certificate file names

<CA certificates file name>		
CA	**Format**	**Example**
Citizen CA	citizen<serial number>.crt	citizen201721.crt
Foreigner CA	foreigner<serial number>.crl	foreigner201721.crt