Foreigner CA
Verklaring met betrekking tot de certificatiepraktijk

OID: 2.16.56.1.1.1.7
OID: 2.16.56.1.1.1.7.1
OID: 2.16.56.1.1.1.7.2
OID: 2.16.56.9.1.1.7
OID: 2.16.56.9.1.1.7.1
OID: 2.16.56.9.1.1.7.2

Inhoudstafel

1 Inleiding

1.1 Waarschuwing vooraf

Deze Verklaring met betrekking tot de Certificatiepraktijk (afgekort als "CPS" - Certification Practice Statement) omschrijft de certificatiepraktijken die van toepassing zijn op de digitale certificaten die voor de in België verblijvende vreemdelingen uitgegeven worden door de certificatiedienstverlener (afgekort als CSP) onder de naam "Foreigner CA" en op de elektronische chipkaarten voor vreemdelingen worden geplaatst (hierna “elektronische vreemdelingenkaarten” genoemd).

Deze CPS doet eveneens dienst als Certificatie Policy (afgekort als “CP”) uitgegeven door de “Foreigner CA”.

Met de in België verblijvende vreemdelingen (hierna “vreemdelingen” genoemd) worden zowel de immigranten afkomstig van binnen als buiten de Europese Unie bedoeld.

1.1.1 Goedgekeurde Entiteiten die volgens deze CPS beheerd worden

Op dit ogenblik is de CSP voor de “Foreigner CA” de “Naamloze Vennootschap CERTIPOST”, met maatschappelijke zetel te 1000 Brussel, Muntcentrum. Deze taak werd haar toegekend door de Belgische Federale Overheid bij de toewijzing van het eID project, waarvoor de volgende voorwaarden gelden:

CERTIPOST treedt op als Certificatiedienstverlener overeenkomstig de Wet van 9 juli 2001 (hierna “de Wet op de elektronische handtekeningen” genoemd) en de Europese Richtlijn 1999/93.

De « Foreigner CA » is de technische naam van de certificatie-autoriteit die identiteitscertificaten en handtekeningscertificaten voor elektronische vreemdelingenkaarten uitgeeft.

CERTIPOST is in hoofdzaak verantwoordelijk voor de “Foreigner CA” volgens een “Raamovereenkomst” van 14 november 2002 (Ref. RRN 006/2001) die ondertekend werd tussen BELGACOM, een NV naar publiek recht en de Belgische Federale Overheid. De Belgische Federale Overheid heeft deze overeenkomst overgedragen van BELGACOM aan CERTIPOST op 1 juli 2004. Volgens de vermelde Raamovereenkomst zal CERTIPOST de identiteitscertificaten en de handtekeningcertificaten leveren, uitgeven en onderhouden voor de elektronische vreemdelingenkaarten en de vertrouwensdiensten in verband met deze certificaten leveren. Deze diensten omvatten, doch zijn niet beperkt tot het uitgeven van Lijsten betreffende de intrekking van Certificaten (“CRLs”), het verlenen van OCSP (“Online Certificate Status Protocol”) diensten, archiveringsdiensten en diensten voor certificaatconsultatie. Deze diensten worden voornamelijk beperkt tot de taken die vermeld worden in delen 2 en 4 van het Bijzonder Bestek RRN 006/2001 en alle overeengekomen wijzigingsaanvragen, met uitzondering van post

10 van Deel 2 en post 9 van Deel 4 zoals beschreven in de BAFO (“Best and Final Offer”) die door de Belgische Federale Overheid aanvaard werd.

CERTIPOST vervult zowel de rol van CA (= een factory die certificaten uitgeeft voor rekening van een CSP, volgens een specifieke SLA) als van CSP, in de wetenschap dat de Belgische Federale Overheid optreedt als CSP die verantwoordelijk is voor de Belgische Root CA. Bijgevolg draagt Certipost de algemene verantwoordelijkheid voor het uitgeven van de certificaten.

Naast de CSP zijn nog andere partijen betrokken in het project voor de elektronische vreemdelingenkaarten, zoals:

1) De autoriteiten

De Registratieautoriteit (“RA”) waarmerkt in naam en voor rekening van de CSP dat een bepaalde openbare sleutel tot een bepaalde entiteit behoort (bijvoorbeeld een persoon) door een digitaal certificaat uit te geven en dit certificaat met zijn privé-sleutel te ondertekenen. Voor de elektronische vreemdelingenkaart treedt het "Rijksregister", een openbaar bestuurslichaam dat tot de Federale Overheidsdienst Binnenlandse Zaken behoort, op als RA. Het RRN[1] delegeert het merendeel van de huidige registratieverrichtingen aan de plaatselijke bevolkingsadministratie van de gemeenten, de zogenaamde Lokale registratieautoriteiten ("LRA"). Op basis van deze procedure vraagt de RA de uitgave van een certificaat aan bij de CA.

De RA is in hoofdzaak verantwoordelijk voor:

(i) de identificatie van de vreemdeling,
(ii) de registratie van de gegevens die gecertificeerd moeten worden,
(iii) de machtiging tot uitgave van een certificaat voor een bepaalde vreemdeling,
(iv) de waarborg dat de certificaten van de vreemdeling op de juiste kaart bewaard worden,
(v) de waarborg dat de vreemdeling de juiste kaart ontvangt en dat de kaart in kwestie enkel geactiveerd wordt wanneer ze naar behoren toegekend wordt aan de juiste vreemdeling,
(vi) en voor de SRA (Autoriteit voor de Schorsing en de Herroeping) : de entiteit die de certificaten schorst en/of herroept overeenkomstig de Wet op de elektronische handtekeningen.

2) Kaartenproducent (Card Manufacturer):

De Kaartenproducent (“CM” [2]) is het bedrijf ZETES. Deze taak werd haar toegekend door de Belgische Federale Overheid bij de toewijzing van het eID project. ZETES is hierbij verantwoordelijk voor de productie, personalisatie, initialisatie en distributie van de elektronische vreemdelingenkaarten. De certificaten worden in deze kaarten aangebracht door de CM die ook de sleutelparen voorziet. De activiteiten worden voornamelijk beperkt tot de activiteiten die vermeld worden in deel 1 en deel 3 van het Bijzonder Bestek RRN 006/2001.

1.1.2 Relaties tussen entiteiten onderhevig aan deze CPS

De relatie tussen CERTIPOST als de CSP voor “Foreigner CA” en de certificaathouders, m.a.w. de vreemdelingen, is geregeld door de Wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten, gewijzigd door de wet van 25 maart 2003, hierna "de Wet op Identiteitskaarten" genoemd en de Wet van 15 december 1980 betreffende de toegang tot het

[1] RRN is het acroniem voor “Rijksregister-Registre National”. Het RRN is een administratie binnen de Federale Overheids Dienst Binnenlandse Zaken, verantwoordelijk voor het beheer van o.a. het Nationaal Register van natuurlijke personen.

[2] CM : afkorting van Card Manufacturer

grondgebied, het verblijf, de vestiging en verwijdering van vreemdelingen en hierna “de vreemdelingenwet” genoemd. CERTIPOST licht de certificaathouders in over hun rechten en plichten en zal hiervoor afstemmen met de Federale Overheid betreffende de wijze van communiceren.

De CA, RA en CM zijn overeengekomen dat CERTIPOST zal optreden als CSP en de volledige verantwoordelijkheid zal dragen ten aanzien van de bevolking.

In overeenstemming met de norm ETSI 104.456 ter ondersteuning van de Europese Richtlijn (Richtlijn 1999/93 van het Europees Parlement en de Raad van 13 december 1999 houdende het gemeenschapskader voor elektronische handtekeningen) inzake elektronische handtekeningen, waarborgt CERTIPOST het beheer van de CSP- activiteiten door middel van een PKI Management Board die over alle nodige deskundigheid beschikt.

Deze CPS onderschrijft de volgende normen en brengt ze tot uitvoering:

- RFC 2527: Internet X.509 Openbare Sleutel Infrastructuur – Certificaatbeleiden en Certificatiepraktijken
- RFC 2459: Internet X.509 Openbare Sleutel Infrastructuur – Certificaat- en CRL-Profiel. Vertrouwende Partijen
- RFC 3039: Internet X.509 Openbare Sleutel Infrastructuur – Gekwalificeerd Certificatenprofiel.
- RFC 2560: X.509 Internet

Door officieel deel te nemen aan de wekelijkse eID progress meetings, waarop alle bovengenoemde partijen behoorlijk vertegenwoordigd worden, verzamelt CERTIPOST alle nodige informatie en stelt CERTIPOST deze partijen alle relevante vragen om haar verantwoordelijkheid als CSP op te nemen. De aangelegenheden en vragen worden binnen de PKI Management Board geanalyseerd en indien nodig worden voorstellen/correcties naar voren gebracht op de vergadering betreffende de vorderingen.

De coördinator van de PKI Management Board zal, ten aanzien van de eID CSP Stuurgroep geleid door FEDICT, elke aangelegenheid uitdiepen die niet opgelost kan worden door middel van deze procedure. De eID CSP Stuurgroep kan externe deskundigen oproepen om bijkomend advies te geven en heeft de verantwoordelijkheid geschillen te beslechten.

1.2 Voorwerp van deze CPS

Een Verklaring betreffende de certificatiepraktijk (CPS) is een unilaterale verklaring van de praktijken die een CSP uitvoert wanneer ze certificeringdiensten verleent. Een CPS is een veelomvattende beschrijving van de manier waarop de CA haar diensten beschikbaar stelt. Deze CPS kan enkel gebruikt worden binnen het bevoegdheidsgebied verleend door de CA[3]. De CPS heeft als doel het bevoegdheidsgebied af te bakenen waarbinnen certificeringdiensten verleend worden aan de vreemdelingen en aan vertrouwende partijen[4] binnen het bevoegdheidsgebied van de CA. Verder schetst deze CPS ook de relatie tussen de “Foreigner CA” en andere Certificatieautoriteiten binnen de PKI-hiërarchie van de Belgische Federale Overheid, zoals de Belgische Root CA (BRCA)[5]. De verklaring beschrijft ook de relatie tussen de CSP en de andere instellingen die betrokken zijn bij de levering van de certificaten voor de elektronische vreemdelingenkaarten in België (hierna “de certificaten” genoemd).

De CPS beschrijft operationele richtlijnen die van toepassing zijn op alle vreemdelingen en vertrouwende partijen, inclusief natuurlijke personen of rechtspersonen in en buiten België. Deze CPS voorziet ook in operationele PKI best practices voor andere Certificatieautoriteiten, zoals de BRCA, die behoren tot de PKI-hiërarchie van de Belgische Federale Overheid binnen het rechtskader voor elektronische handtekeningen en elektronische vreemdelingenkaarten in België. Bovendien beschrijft deze CPS de relaties tussen de CSP en alle andere entiteiten die een rol spelen in de context van de elektronische vreemdelingenkaart, zoals de Kaartpersonalisator en de Kaartinitialisator. De Belgische Federale Overheid verwerft deze diensten door middel van Raamovereenkomsten. Tot slot voorziet deze CPS informatie inzake accreditatie en toezicht voor controleautoriteiten, accreditatieorganen, geaccrediteerde accountants, enz. met betrekking tot de activiteiten van de CSP.

[3] De CA verleent binnen het bevoegdheidsgebied certificeringdiensten. De toepassingen die gebruik maken van de certificaten, enz. behoren bijvoorbeeld niet tot dit bevoegdheidsgebied.

[4] Zie punt 1.7.7 (Vertrouwende Partijen: entiteiten die afhankelijk zijn van een certificaat)

[5] De BRCA is de CA die de “Foreigner CA” gecertificeerd heeft. Vertrouwen in de BRCA, betekent automatisch een impliciet vertrouwen in de “Foreigner CA”.

Openbare Sleutel Infrastructuur – Online Certificate Status Protocol - OCSP

- ETSI TS 101 456: Beleidsvereisten voor Certificatieautoriteiten die gekwalificeerde certificaten uitgeven.
- ETSI TS 101 862: Gekwalificeerd Certificatenprofiel.
- ETSI TS 102 042: Beleidsvereisten voor Certificatieautoriteiten die openbare sleutelcertificaten uitgeven (Enkel genormaliseerd niveau).
- Normen gelijkaardig aan de ISO 1-7799 veiligheids- en infrastructuurnorm.

De CPS beschrijft in detail de technische, procedurele en organisatorische richtlijnen en praktijken van de CA die betrekking hebben op alle certificeringsdiensten aangeboden gedurende de volledige levensloop van de certificaten uitgegeven door de “Foreigner CA”. Naast deze CPS is het mogelijk dat ook andere documenten met betrekking tot het certificeringproces in acht genomen moeten worden. Deze documenten zullen beschikbaar zijn in het repertorium van de CSP op: http://repository.eid.belgium.be.

Deze CPS wordt beschikbaar gemaakt in het repertorium van de CSP op het adres http://repository.eid.belgium.be.

Opmerkingen over deze CPS kunnen overgemaakt worden aan de CSP op het volgend adres: CSP voor “Foreigner CA” p/a CERTIPOST, Muntcentrum, 1000 Brussel.

Deze CPS voldoet aan de formele vereisten van de Internet Engineering Task Force (IETF) RFC 2527, versie van 12 juli 2001 inzake vorm en inhoud. De structuur van de CPS volgt deze van de RFC 2527. De hoofdstukken die niet van toepassing zijn voor de uitvoering van certificeringdiensten van de CSP voor de “Foreigner CA” krijgen de benaming “Hoofdstuk niet van toepassing”. In deze CPS werden kleine redactionele veranderingen van RFC 2527 voorschriften aangebracht om de RFC 2527 structuur geschikter te maken voor de behoeften van dit toepassingsgebied.

Meer informatie over deze CPS en de CSP is te verkrijgen bij de CSP voor “Foreigner CA” p/a CERTIPOST, Muntcentrum, 1000 Brussel.

1.3 De certificaten op de elektronische vreemdelingenkaarten

De Belgische Wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten, gewijzigd door de wet van 25 maart 2003, hierna "de Wet op Identiteitskaarten", de vreemdelingenwet en de koninklijke besluiten ter uitvoering van deze wetten, introduceren de elektronische kaart voor vreemdelingen. De elektronische vreemdelingenkaart is een kaart waarop informatie in grafische vorm weergegeven wordt en die ook informatie in elektronische vorm bevat op een chip in de kaart. De wet reguleert het kader voor de uitgave en het gebruik van de elektronische vreemdelingenkaart. Om als CSP voor de “Foreigner CA” te kunnen optreden moet CERTIPOST op de eerste plaats de wetsvoorschriften naleven.

De elektronische vreemdelingenkaarten bevatten twee soorten van digitale certificaten waarmee de houders van de vreemdelingenkaarten afhankelijk van hun leeftijd (i) zichzelf kunnen identificeren en (ii) een elektronische handtekening kunnen gebruiken:

- Een identiteitscertificaat: de houder van de elektronische vreemdelingenkaart kan dit certificaat gebruiken om zich te identificeren bij elektronische verrichtingen indien bij aanvraag van de elektronische vreemdelingenkaart de leeftijd van 6 jaar werd bereikt. Het identiteitscertificaat bevat de identiteit van de houder en de openbare sleutel die overeenkomt met de privé-sleutel. Deze privé-sleutel mag enkel gebruikt worden voor gebruikersidentificatie.
- Een Gekwalificeerd Certificaat voor elektronische handtekeningen (of ehandtekeningen): dit certificaat bevat de identiteit van de houder en de elektronische handtekeningen en de Europese Richtlijn 1999/93 en kan op de vreemdelingenkaart geactiveerd worden zodra de vreemdeling de leeftijd van 18 jaar heeft bereikt.

Omwille van technologische veiligheidsvereisten is het aan te raden om de certificaten voor identiteit niet te gebruiken voor elektronische handtekeningen, maar hiervoor een afzonderlijk

openbare sleutel die overeenkomt met de privé-sleutel, die enkel gebruikt mag worden om een elektronische handtekening te maken. Het Gekwalificeerd Certificaat voor elektronische handtekeningen voldoet aan de bepalingen van de Wet op

gekwalificeerd certificaat te gebruiken. Het Identiteitscertificaat kreeg daarom niet de status van een gekwalificeerd certificaat, zodat alle betrokken partijen een duidelijk onderscheid kunnen maken tussen het Identiteitscertificaat en het Gekwalificeerd Certificaat voor elektronische handtekeningen.

De activering van de certificaten op de elektronische vreemdelingenkaart is facultatief voor de vreemdeling, die er dus voor kan kiezen het gebruik van de sleutels en certificaten op zijn/haar vreemdelingenkaart al dan niet te activeren. Wanneer de vreemdeling de certificaten op zijn/haar elektronische vreemdelingenkaart activeert, ontstaat er een contractuele relatie met CERTIPOST in de hoedanigheid van CSP voor de “Foreigner CA”.

De technologie die gebruikt wordt voor de certificeringsdiensten voor deze certificaten is “PKItechnologie”. PKI, ”Public Key Infrastructure”, is een acroniem voor een systeem van openbare sleutel cryptografie in combinatie met een infrastructuur die ontworpen is om een veiligheidsniveau voor gecommuniceerde en opgeslagen informatie te voorzien dat voldoende hoog is om het vertrouwen dat ondernemingen, consumenten, overheden en rechtbanken hebben in dergelijke informatie te rechtvaardigen.

Het orgaan dat certificaten uitgeeft, heet Certificatieautoriteit (CA), terwijl het orgaan dat verantwoordelijk is voor de identificatie van de persoon die een certificaat aanvraagt de Registratieautoriteit (RA) is. In deze context treedt CERTIPOST op als uitgever van certificaten. RRN[6] treedt op als RA. Wat de elektronische vreemdelingenkaart betreft, kan enkel de RA de “Foreigner CA” vragen om een certificaat uit te geven aan een vreemdeling.

De RA staat niet zelf in voor de rechtstreekse identificatie van de aanvrager, maar delegeert deze verantwoordelijkheid aan Lokale registratieautoriteiten (LRA's). Deze rol wordt opgenomen door de gemeenten. In die hoedanigheid is de gemeente de tussenpersoon tussen de aanvrager, m.a.w. de vreemdeling, en de RA.

1.4 Relatie van deze CPS met andere documenten

Zoals hierboven beschreven, is deze CPS een unilaterale verklaring voor het algemeen publiek over de praktijken waaraan de CSP voor de “Foreigner CA” voldoet wanneer het certificeringsdiensten verleent. Het is een uitgebreide beschrijving van de manier waarop de CSP haar diensten beschikbaar maakt.

Zoals verder uitvoerig beschreven wordt, treedt het RRN samen met de gemeenten op als de RA binnen het bevoegdheidsgebied van de CSP met uitsluiting van alle andere. Enkel het RRN en de gemeenten kunnen beslissen over de uitgave van een certificaat volgens deze CPS. Het RRN kan echter één of meerdere derde partijen aanstellen om RA-activiteiten te vervullen binnen het bevoegdheidsgebied van de CSP.

Enkel het RRN, de gemeenten of de CSP kan/kunnen beslissen over de schorsing en herroeping van een certificaat volgens deze CPS.

De relatie tussen de Belgische Federale Overheid en de CSP voor de “Foreigner CA” wordt gereguleerd door een Raamovereenkomst. In geval van enige tegenstrijdigheid tussen deze CPS en de Raamovereenkomst gelden de bepalingen van de Raamovereenkomst. Uit deze CPS vloeien voor de Belgische Federale Overheid, CERTIPOST, ZETES of enige andere partij die betrokken is bij de uitgave en het beheer van de elektronische vreemdelingenkaart geen bijkomende rechten en verplichtingen voort. De CPS is voornamelijk bedoeld om de wettelijke en contractuele bepalingen verder te preciseren en alle belanghebbende partijen in te lichten over de activiteiten van de CSP voor de “Foreigner CA”.

1.5 Positie van de “Foreigner CA” in de CA-Hiërarchie

Om de elektronische vreemdelingenkaart zonder beperkingen te kunnen gebruiken, dient zowel de identiteit van de vreemdeling als de identiteit van de technische infrastructuur gewaarborgd te worden. Met technische infrastructuur worden bijvoorbeeld de servers bedoeld die nodig zijn voor toepassingen van de Belgische Federale Overheid. Daarom is het nodig verscheidene

[6] Rijksregister – Registre National

soorten certificaten te gebruiken naast de certificaten voor vreemdelingen. De “Foreigner CA” behoort tot een overkoepelende groep van certificatieautoriteiten van de Belgische Federale Overheid. Om de opbouw van vertrouwen tussen de verschillende deelnemende Certificatieautoriteiten te vergemakkelijken, heeft de Belgische Federale Overheid een PKIhiërarchie opgesteld.

Bovenaan deze hiërarchie bevindt zich een “Belgische Root CA (BRCA)”. Het doel hiervan is onder meer vertrouwen te scheppen tussen de verschillende Certificatieautoriteiten binnen het overheidsdomein. De (zelfondertekende) BRCA heeft elke privé-sleutel van de Certificatieautoriteiten in het overheidsdomein gecertificeerd, inclusief die van de “Foreigner CA”. Door het certificaat van een dergelijke CA te bevestigen, kan het vertrouwen in de BRCA ook toegepast worden op de CA die de BRCA gecertificeerd heeft. Het certificaat van een eindgebruiker is dus betrouwbaar in die mate dat de BRCA betrouwbaar is.

Het vertrouwen in de BRCA op gebied van software toepassingen wordt ook bepaald door de “root sign” waarvoor een derde partij leverancier instaat (Digicert cybertrust global). Het Rootcertificaat van Digicert cybertrust global wordt algemeen erkend in toepassingsoftware.

De BRCA-praktijken zijn terug te vinden in een CPS die specifiek hierop gericht is. Deze CPS is beschikbaar op het volgend adres: http://repository.eid.belgium.be.

Het vertrouwen in de certificaten voor vreemdelingen kan als volgt geverifieerd worden:

1. Trusted path building (Opbouw van het Vertrouwde Pad)

Eerst wordt gecontroleerd of het certificaat uitgegeven werd door de “Foreigner CA”. Dan wordt conform gecontroleerd of het certificaat van de “Foreigner CA” uitgegeven werd door de BRCA. Indien het resultaat van deze controles positief is, kan het vertrouwen in de BRCA overgedragen worden op het gepersonaliseerde certificaat voor de vreemdeling via het “Foreigner CA” certificaat.

Verificatie van het BRCA-certificaat:

In het algemeen wordt het BRCA-certificaat in het geheugen van toepassingscertificaten aangeduid als een betrouwbaar certificaat. In het onwaarschijnlijke geval dat een eindgebruiker gewaarschuwd wordt dat het BRCA-certificaat niet meer geldig is, volstaat het dat de eindgebruiker het BRCA-certificaat uit het certificatengeheugen verwijdert. Op die manier wordt dat domein verwijderd uit de betrouwbare domeinen zodat men duidelijk ziet dat dit gedeelte van de verificatie ontbreekt.

2. De verificatie van het “Foreigner CA” certificaat kan bepaald worden door de volgende stappen te volgen:

   - 2.1 Controle van de geldigheid van het “Foreigner CA” certificaat (o.a. controle van de validiteitsperiode)
   - 2.2 Controle van de status van het “Foreigner CA” certificaat (o.a. controle op staat van schorsing of herroeping).[7]

3. De verificatie van het certificaat kan bepaald worden door de volgende stappen te volgen:
   - 3.1 Controle van de geldigheid van het certificaat (o.a. controle van de validiteitsperiode).
   - 3.2 Controle van de status van het certificaat (o.a. controle op staat van schorsing of herroeping).

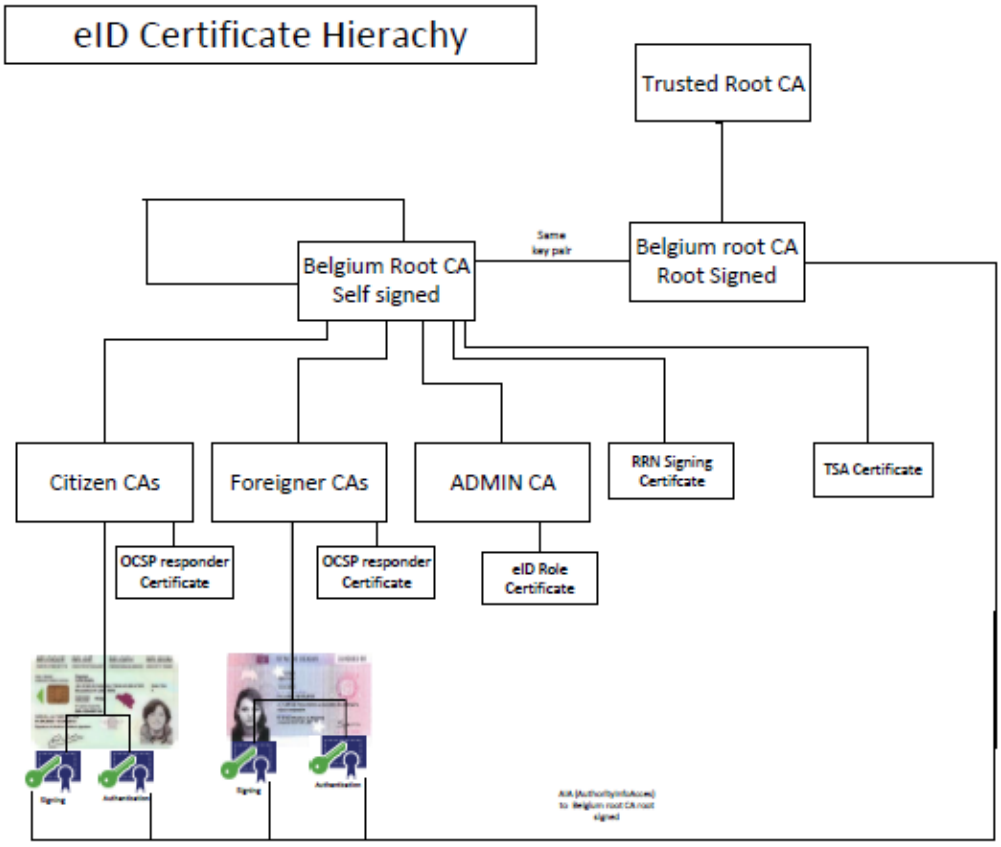
In het algemeen worden de meeste of alle verrichtingen automatisch uitgevoerd door de toepassing waarvoor het certificaat gebruikt wordt. Hierbij dient de eindgebruiker nauwelijks of

niet tussen te komen.

De vertrouwenshiërarchie van certificaten voor vreemdelingen volgt de onderstaande structuurpremissen:

1. Een beperkte hiërarchie waarvoor alle nodige informatie om de certificaten off-line te bevestigen, op de kaart opgeslagen kan worden.

2. Een sterke voorkeur voor automatisch vertrouwen in certificaten die uitgegeven worden door de infrastructuur van de Belgische Federale Overheid. Voor on-line verificatie is geen tussenkomst van de eindgebruiker nodig. Deze meer complexe hiërarchie wordt in Figuur 1 beschreven:



Figuur 1: PKI-hiërarchie

Om aan beide vereisten te voldoen, voorziet de hiërarchie een combinatie van een tweeledig en een drieledig model.

In het tweeledig model vormen de “Foreigner CA” en de Zelfondertekende Belgische Root-CA[7] een hiërarchie, waarmee het off-line mogelijk is de certificaten voor handtekening en

[7] Een zelfondertekend certificaat is een certificaat dat ondertekend wordt met de privé-sleutel van de gecertificeerde entiteit. Indien dat zelfondertekende certificaat niet betrouwbaar is, kan op dat certificaat of op enig certificaat dat zich lager in de hiërarchie bevindt, geen vertrouwen gebouwd worden. Er is immers geen hoger vertrouwenspunt bovenaan de

identificatie te bevestigen. De sleutel van de Belgische Root-CA wordt in dit model zelf ondertekend. In dat geval kan de partij die de bevestiging geeft (bv. Douanebeambte, Politieagent, enz.) het zelfondertekend BRCA-certificaat van de eigen elektronische Identiteitskaart gebruiken om het “Foreigner CA” certificaat en de certificaten van de kaart van de vreemdeling te bevestigen.

In het drieledig model wordt de hiërarchie gevormd door de “Foreigner CA”, de Belgische Root-CA met ondertekende Root en de Digicert cybertrust global Root-CA. In dit model wordt dezelfde privé-sleutel als die voor de Zelfondertekende Belgische Root CA dit keer gecertificeerd door de Digicert cybertrust global Root-CA. Deze aanpak maakt de automatische bevestiging mogelijk binnen de meest algemeen gebruikte toepassingen, zoals browsers, omdat deze browsers het Digicert cybertrust global Top Root-CA certificaat reeds erkend hebben en het in hun lijst van vertrouwde certificaten verschijnt. Net zoals de “Foreigner CA” vertrouwen krijgt via de BRCA, krijgt de BRCA vertrouwen via de Digicert cybertrust global Root-CA. Dit drieledig model sluit de noodzaak uit om het Zelfondertekende Belgische Root CA certificaat individueel in te voeren.

Omdat de Zelfondertekende Belgische Root-CA en de Belgische Top Root-CA met ondertekende Root hetzelfde sleutelpaar gebruikt, zij het met twee verschillende certificaten, kan een certificaat dat ondertekend wordt met de privé-sleutel van dat sleutelpaar bevestigd worden met beide Belgische Rootcertificaten.

De maker van de toepassing zal meestal één of beide modellen voorzien en de eindgebruiker zal niet tussen de twee modellen moeten kiezen.

1.6 Documentnaam en -identificatie

Deze CPS kan ook door enige partij geïdentificeerd worden door de volgende OID's[8]:

- De OID 2.16.56.1.1.1.7.1. voor het certificaat voor de elektronische handtekening.
- De OID 2.16.56.1.1.1.7.2 voor het Identiteitscertificaat .

1.7 PKI deelnemers

Deze PKI-hiërarchie bestaat uit verschillende deelnemende partijen. De partijen die hieronder vermeld worden, inclusief alle Certificatieautoriteiten, de RA, LRA's (de gemeenten), de vreemdelingen en afhankelijke partijen, worden gezamenlijk PKI deelnemers genoemd.

1.7.1 Certificatieautoriteit voor de Foreigner CA

Een certificatieautoriteit (CA) is een instelling die digitale certificaten uitgeeft die gebruikt worden in het openbaar domein of in een zaken- of verrichtingscontext. De “Foreigner CA” is zulk een Certificatieautoriteit.

De CA is gemachtigd om certificaten voor vreemdelingen uit te geven. Deze machtiging werd verleend door de Belgische Root Certificatieautoriteit (hierna BRCA).

De CA waarborgt van alle diensten in verband met de certificaten, inclusief de uitgave, de herroeping, de statusverificatie en het aanbrengen van tijdstempels, naargelang ze beschikbaar of vereist zijn bij specifieke toepassingen.

De CA wordt in navolging van Artikel 20 van de Wet op elektronische handtekeningen gecontroleerd.

Vertrouwenshiërarchie. Het is echter uiterst onwaarschijnlijk dat dit geval zich voordoet.

[8] Object IDentificator

De CA is in België gevestigd en kan gecontacteerd worden op het adres dat elders in deze CPS vermeld wordt. De CSP heeft een veiligheidsplan en een noodvoorzieningenplan in België voorzien om de continuïteit van de CA diensten te kunnen verzekeren. Onder deze diensten vallen de uitgave, de schorsing, de herroeping, de vernieuwing en de statusverificatie van certificaten.

Het verantwoordelijkheidsdomein van de CA omvat het algemeen beheer van de levensduur van de certificaten, inclusief:

- Uitgave;
- Schorsing / opheffen van schorsing;
- Herroeping;
- Statusverificatie (Dienst voor Certificaatstatus);
- Adressendienst.

1.7.2 Leverancier van de Root Sign

De leverancier van de root sign waarborgt het vertrouwen in de BRCA bij algemeen gebruikte toepassingen. Hij waarborgt verder ook dat dergelijke toepassingen zijn Root blijven vertrouwen en hij brengt de RA op de hoogte van enig voorval dat het vertrouwen in zijn eigen Root beïnvloedt. De leverancier van de root sign van de BRCA is digicert cybertrust global (http://cybertrust.omniroot.com/repository/).

1.7.3 Registratieautoriteiten en Lokale registratieautoriteiten

Het RRN (Rijksregister) is samen met de gemeenten de RA binnen het domein van de CSP voor de “Foreigner CA” met uitsluiting van alle andere. Het RRN is gevestigd volgens en onderhevig aan de Wet op het Rijksregister en de Wet op de identiteitskaarten.

Enkel het RRN, de gemeenten kunnen beslissen over de uitgave van een certificaat volgens deze CPS. Het RRN kan een derde partij aanstellen om de RA taken verder uit te voeren binnen het “Foreigner CA” domein.

Enkel het RRN, de gemeenten of de CSP kan/kunnen beslissen over de schorsing en herroeping van een certificaat volgens deze CPS.

De plaatselijke overheden of gemeenten treden binnen het domein van de CSP voor de “Foreigner CA” op als exclusief aangestelde LRA's. Deze LRA's registreren en verifiëren de gegevens van de vreemdelingen namens de RA. Wat de registratie betreft, hebben de LRA's geen rechtstreeks contact met de “Foreigner CA”.

De RA dient de nodige gegevens in om de certificaten voor de “Foreigner CA” op te stellen of te herroepen.

De LRA's (de gemeenten) staan rechtstreeks in contact met de vreemdelingen om openbare certificeringdiensten aan de vreemdelingen als eindgebruiker af te leveren. De taken van de LRA's zijn voornamelijk de volgende:

- De vreemdeling indien vereist schriftelijk uitnodigen om naar het gemeentebestuur te komen, bijvoorbeeld wanneer de vreemdelingenkaart aan vervanging toe is;
- Alle nodige procedures volgen om het basisdocument[9] te vervolledigen, waarna de vreemdeling het basisdocument goedkeurt. Vervolgens stuurt de LRA de gegevens van het basisdocument op beveiligde wijze naar de Kaartpersonalisator, zodat de certificaataanvraag verder behandeld wordt. De Kaartpersonalisator geeft enkel een vreemdelingenkaart uit na goedkeuring van

[9] Het basisdocument wordt gebruikt om gegevens te verzamelen die gebruikt worden om een identiteitskaart uit te geven. De Federale Overheids Dienst Binnenlandse Zaken bezorgt de gemeenten het model van dit document.

de RA. Deze goedkeuring wordt aangegeven door een aanvraag van de Kaartpersonalisator;

- Het proces aanvatten om een statusverandering van een certificaat via de RA aan te vragen bij de CA;
- De uitgegeven elektronische vreemdelingenkaart aan de vreemdeling te bezorgen.

De RA staat onrechtstreeks in contact met de vreemdelingen en rechtstreeks met de CA om openbare certificeringdiensten aan de eindgebruiker te verlenen. De RA houdt zich specifiek bezig met het volgende:

- Het inrichten van een hulpdienst waar de houder van een elektronische vreemdelingenkaart het verlies, de diefstal of de vernieling van zijn/haar elektronische vreemdelingenkaart kan melden wanneer dit niet mogelijk is bij de gemeente of bij de politie. Deze hulpdienst wordt hierna de “RA Helpdesk” genoemd;
- Het registreren van vreemdelingen voor certificeringdiensten;
- Na de goedkeuring van een aanvraag, de CA vragen een certificaat uit te geven;
- Het proces aanvatten om een certificaat te herroepen en de herroeping of schorsing van een certificaat aan te vragen bij de CA.

De RA voorziet de “Foreigner CA” van de nodige gegevens om de certificaten op te stellen. De RA voorziet voor elk certificaat de identiteit van de houder en het serienummer van het aangevraagd certificaat, samen met de openbare sleutel die overeenkomt met de vreemdeling die in dat certificaat opgenomen moet worden.

Alle communicatie tussen de LRA, RA en CA in verband met eender welke fase in de levensduur van de certificaten wordt beveiligd met encryptie- en ondertekeningstechnieken die gebaseerd zijn op PKI. Zo wordt de vertrouwelijkheid en de wederzijdse identificatie verzekerd. Ook communicatie in verband met aanvragen, de uitgave, de schorsing, de opheffing van een schorsing en de herroeping van certificaten valt hieronder.

1.7.4 Kaartpersonalisator

De Kaartpersonalisator past niet gepersonaliseerde smart cards aan de gepersonaliseerde elektronische vreemdelingenkaarten aan door de identiteitsgegevens van de vreemdeling samen met een foto op de kaart te drukken. Verder is de Kaartpersonalisator verantwoordelijk voor het beveiligd versturen van deze gepersonaliseerde kaarten naar de Kaartinitialisator. Momenteel treedt de N.V. ZETES op als Kaartpersonalisator, volgens een Raamovereenkomst met de Belgische Federale Overheid.

1.7.5 Kaartinitialisator

De Kaartinitialisator voorziet de volgende diensten:

- Het aanmaken van de benodigde sleutelparen in de kaart;
- Het opslagen van beide certificaten op de kaart;
- Het aanmaken van de persoonlijke activeringscodes van de aanvrager en de gemeente, alsook de initiële PIN code van de aanvrager;
- Het laden van de actieve Rootcertificaten van de overheid op de kaart;
- Het leveren van de elektronische vreemdelingenkaart aan de gemeente; • Het voorzien van de persoonlijke activeringscode en de PIN code aan de aanvrager;
- Het opnemen van de gegevens in het vreemdelingenregister.

Momenteel treedt de N.V. ZETES op als Kaartinitialisator, volgens een Raamovereenkomst met de Belgische Federale Overheid .

1.7.6 Abonnees

De abonnees van de CA diensten in het “Foreigner CA” domein zijn de vreemdelingen die in het bezit zijn van een elektronische vreemdelingenkaart met geactiveerde certificaten, in overeenkomst met de Wet op de identiteitskaarten en de vreemdelingenwet. In de rest van dit document kan de term abonnee vervangen worden door de term "vreemdeling". Deze vreemdelingen:

- worden geïdentificeerd in beide certificaten;
- zijn in het bezit van de privé-sleutels die overeenkomen met hun publieke–sleutels die in hun respectieve certificaten opgenomen zijn.

De vreemdelingen zijn gerechtigd aan het begin van de aanvraag voor een elektronische vreemdelingenkaart aan te geven of ze certificaten willen gebruiken. Wanneer de elektronische vreemdelingenkaart aan de vreemdeling geleverd wordt, zijn de certificaten erin geladen. Voor vreemdelingen die de certificaten niet wensen te gebruiken, worden deze certificaten herroepen.

Voor vreemdelingen die de leeftijd van 6 jaar nog niet hebben bereikt worden bij aanvraag van een elektronische vreemdelingenkaart de certificaten voor identificatie en elektronische handtekening automatisch herroepen.

Voor vreemdelingen, die de leeftijd van 18 jaar nog niet hebben bereikt wordt bij aanvraag van een elektronische vreemdelingenkaart het certificaat voor elektronische handtekening automatisch herroepen.

1.7.7 Vertrouwende Partijen

Vertrouwende partijen zijn entiteiten, inclusief natuurlijke personen of rechtspersonen, die vetrouwen stellen in een certificaat en/of een digitale handtekening die geverifieerd kan worden door middel van een openbare sleutel die opgenomen is in het certificaat van een vreemdeling.

Vertrouwende partijen dienen de geldigheid van een digitaal certificaat dat ze ontvangen steeds te verifiëren steunend op de validiteitsperiode van het certificaat en de geldigheidsverklaring van het certificaat door de CA Dienst (via OCSP, CRL, delta CRL of web interface) alvorens te vertrouwen op informatie die in een certificaat opgenomen is.

1.8 Het gebruik van Certificaten

Het gebruik van de certificaten op de elektronische vreemdelingenkaart is aan bepaalde beperkingen onderhevig.

Het Identiteitscertificaat dat door de “Foreigner CA” uitgegeven wordt, kan gebruikt worden voor specifieke verrichtingen met elektronische identificatie die toegang verschaffen tot websites en andere on-line inhoud, e-mails, ed., ter beschikking gesteld door de Belgische Federale Overheid. Omwille van technologische veiligheidsvereisten is het aan te raden om de Identiteitscertificaten niet voor elektronische handtekeningen te gebruiken. De “Foreigner CA” wijst daarom alle aansprakelijkheid ten aanzien van vertrouwende partijen van de hand in alle gevallen waarin het Identiteitscertificaat gebruikt wordt voor toepassingen die het gebruik van dit certificaat toelaten om elektronische handtekeningen aan te maken.

1.9 Adminsitratief beheer

Het administratief beheer valt onder de CSP voor de "Foreigner CA", p/a CERTIPOST, Muntcentrum, 1000 Brussel.

1.10 Definities en Acroniemen

Aan het einde van deze CPS kunt u een lijst vinden met definities en acroniemen.

2 Verantwoordelijkheid inzake Publicatie en Bewaring

De CSP publiceert informatie over de digitale certificaten die het uitgeeft. Deze informatie is terug te vinden in een of meerdere on-line archieven onder het Internet domein belgium.be en is voor het publiek toegankelijk. De CA behoudt zich het recht voor informatie betreffende de status van een certificaat te publiceren in verwijzigen van derden.

De CSP legt een on-line repertorium aan met documenten waarin bepaalde aspecten van de activiteiten en procedures en de inhoud van bepaalde beleidsvormen bekend gemaakt worden. Dit geldt ook voor de CPS, die beschikbaar is op http://repository.eid.belgium.be. De CA reserveert het recht informatie beschikbaar te stellen en te publiceren in verband met de beleidsvormen en dit op eender welke manier die de CA gepast acht.

PKI deelnemers worden op de hoogte gebracht van het feit dat de CA de informatie die zij rechtstreeks of onrechtstreeks aan de CA meedelen, kan publiceren in bestanden die toegankelijk zijn voor het publiek, voor zover dit enkel bedoeld is om informatie te verschaffen over de status van elektronische certificaten. De CA publiceert regelmatig informatie over de status van digitale certificaten, zoals aangegeven in deze CPS.

De CA legt een repertorium aan met alle certificaten dat het uitgegeven heeft en zorgt eveneens voor het onderhoud van dit repertorium. In het repertorium wordt tevens de status van het uitgegeven certificaat aangegeven.

De CA publiceert regelmatig CRL's[10] op http://crl.eid.belgium.be. De CA publiceert regelmatig "Delta CRL's" die alle wijzigingen bevatten sinds de publicatie van de vorige CRL of Delta CRL. Elke nieuwe CRL die gepubliceerd wordt, bevat alle bijwerkingen van de delta CRL's die tot op dat ogenblik gepubliceerd werden.

De CA stelt een OCSP[11] server ter beschikking op http://ocsp.eid.belgium.be. Deze server informeert over de status van een certificaat dat door de CA op aanvraag van een afhankelijke partij uitgegeven wordt, in navolging van IETF RFC 2560. De status van een certificaat kan ook online via het Internet adres http://status.eid.belgium.be gecheckt worden. De status van elk certificaat dat in een CRL of in een CRL opgesomd wordt, moet in overeenstemming zijn met de informatie die door de OCSP server geleverd wordt.

De CA bewaart de CRL en de informatie op deze URL tot elk certificaat dat de CRL bevat, vervalt. Goedgekeurde versies van documenten die in het Archief gepubliceerd moeten worden, zullen binnen 24 uur in het repertorium geplaatst worden.

De CA stelt sommige onderdelen en elementen van dergelijke documenten, inclusief bepaalde veiligheidscontroles, procedures in verband met de werking van inter alia registratieautoriteiten, intern veiligheidsbeleid, enz. niet beschikbaar voor het publiek, aangezien deze elementen erg gevoelig zijn. Toch zijn dergelijke documenten en gedocumenteerde activiteiten voorwaardelijk beschikbaar voor controle door aangestelde partijen waaraan de CA verplichtingen heeft.

2.1 Controle op toegang tot archieven

[10] Een CRL of Lijst van herroepen certificaten is een lijst die door een CA uitgegeven wordt en digitaal ondertekend wordt en die seriële nummers van de herroepen en geschorste certificaten bevat. Dergelijke lijsten dienen steeds geraadpleegd te worden door afhankelijke partijen alvorens te vertrouwen op informatie die in een certificaat opgenomen is.

[11] Het On-line Protocol voor Certificaatstatus (RFC 2560) is een rechtstreekse bron voor statusinformatie, die gebruikt wordt om de huidige status van een digital certificaat te bepalen zonder beroep te doen op CRL's.

Hoewel de CSP tracht de toegang tot de gepubliceerde gegevens kostenvrij te houden, kan het uit hoofde van het contract met de Belgische Federale Overheid, bepaalde diensten aanrekenen, zoals het publiceren van statusinformatie in databanken van derde partijen, privé-bestanden, enz.

De OCSP dienst, een web interfacedienst voor verificatie van de certificaatstatus, het certificaatarchief, de CRL's en Delta CRL's zijn beschikbaar voor het publiek op de website van de CA en via de netwerken van de Belgische Federale Overheid.

In het kader van het contract met de Belgische Federale overheid is de toegang tot deze diensten die door de CSP verleend worden als volgt beperkt:

Via de openbaar beschikbare interface tot het certificaatrepertorium kan slechts één certificaat per opvraging geleverd worden. Voor de RA wordt hierop een uitzondering gemaakt.

De CA kan redelijke maatregelen treffen ter bescherming tegen misbruik downloaddiensten in verband met de OCSP, Web interface statusverificatie, CRL en delta CRL.

De CA kan met name de frequentie van OCSP aanvragen door één persoon beperken tot 10 aanvragen per dag indien de CA kan aantonen dat de gebruiker misbruik maakt van het systeem. De CA kan de verwerking van OCSP aanvragen niet beperken voor enige partij die, op grond van haar activiteiten, genoodzaakt is regelmatig de OCSP status te verifiëren. De CA kan de frequentie van aanvragen voor de verificatie van Web interface certificaatstatussen door één gebruiker beperken tot 10 aanvragen per dag.

3 Identificatie en Authenticiteit

3.1 Benaming

De regels omtrent de benaming en de identificatie van de vreemdelingen voor certificaten zijn dezelfde als de wetsbepalingen die van toepassing zijn op de benaming en de identificatie van vreemdelingen op de vreemdelingenkaarten.

3.2 Initiële Geldigheidsverklaring van Identiteit

De identificatie van de vreemdeling die een elektronische vreemdelingenkaart aanvraagt, gebeurt in overeenkomst met de procedures en de regelgeving die van toepassing zijn op de levering van de elektronische vreemdelingenkaarten. De RA specificeert de procedures die de LRA's tot uitvoer moeten brengen.

3.3 Identificatie en Authenticiteit voor Aanvragen van nieuwe Sleutels

De identificatie en authenticiteit voor aanvragen van nieuwe sleutels door vreemdelingen worden uitgevoerd in overeenkomst met de procedures die gespecificeerd werden door de RA en toegepast worden door de LRA's.

3.4 Identificatie en Authenticiteit voor Aanvragen tot Herroeping en Schorsing

De identificatie van de vreemdeling die een herroeping of schorsing van zijn certificaten aanvraagt, gebeurt in overeenkomst met de procedures en regelgeving die van toepassing zijn op de levering van elektronische vreemdelingenkaarten.

De identificatie en authenticiteit van houders die de herroeping of schorsing van hun certificaten wensen, gebeuren door de entiteit die de aanvraag ontvangt. Deze entiteiten kunnen de volgende zijn:

- De gemeente;
- De politie;
- De RA Helpdesk die hiervoor door de RA ingericht wordt.

Deze entiteit stuurt vervolgens alle aanvragen tot herroeping via de RA door naar de CA. De RA is het enige contactpunt waarlangs de CA een aanvraag tot schorsing kan ontvangen.

4 OPERATIONELE VEREISTEN VOOR DE LEVENSDUUR VAN CERTIFICATEN

Alle entiteiten binnen het bevoegdheidsgebied van de CSP, inclusief de LRA's, vreemdelingen, vertrouwende partijen en/of andere deelnemende partijen, hebben de voortdurende verplichting de RA rechtstreeks of onrechtstreeks op de hoogte te stellen van alle wijzigingen van de informatie die in een certificaat opgenomen wordt. Dit geldt voor de gehele operationele periode van dergelijk certificaat of van enig ander feit dat de geldigheid van een certificaat materieel kan beïnvloeden. De RA zal in dat geval de geschikte maatregelen treffen om te waarborgen dat de situatie gecorrigeerd wordt (bv. door de herroeping van de bestaande certificaten en het aanmaken van nieuwe certificaten met de correcte gegevens aan te vragen bij de CA.

De CA gaat enkel over tot de uitgave, de herroeping of de schorsing van certificaten op aanvraag van de RA met uitsluiting van alle andere, tenzij de RA of de CSP uitdrukkelijk andere instructies geeft.

Om haar taken uit te voeren, doet de CSP een beroep op de diensten van agenten als derde partij. De CSP neemt ten aanzien van de vreemdelingen en de afhankelijke partijen de volledige

aansprakelijkheid en verantwoordelijkheid op zich voor handelingen of verzuim van alle agenten als derde partij waarop beroep gedaan wordt om certificeringdiensten te verlenen.

4.1 Certificaataanvraag

Het inschrijvingsproces dat de vreemdeling moet doorlopen om de certificaten aan te vragen, maakt integraal deel uit van de procedures voor elektronische vreemdelingenkaart van de gemeente, m.a.w. de LRA. De procedure die de LRA hanteert voor de inschrijving van de vreemdeling wordt voorzien door de RA.

4.2 Verwerking van Certificaataanvraag

Wanneer een certificaat aangevraagd wordt, dient de LRA de identiteit van de aanvrager te bevestigen conform het proces voor de aanvraag van de elektronische vreemdelingenkaart. De procedures die van toepassing zijn voor de geldigheidsverklaring van de identiteit van de aanvrager worden in een specifiek document beschreven.

Wanneer een certificaat aangevraagd wordt, kan de LRA de aanvraag voor een elektronische vreemdelingenkaart goedkeuren of weigeren. Dit brengt ook de goedkeuring of weigering van de certificaataanvraag met zich mee. Indien de aanvraag goedgekeurd wordt, stuurt de LRA de registratiegegevens door naar de RA. De RA gaat dan over tot de goedkeuring of de weigering van de aanvraag.

4.3 Uitgave van Certificaten

Na de goedkeuring van een certificaataanvraag vraagt de RA de uitgave van het certificaat aan bij de CA. De CA verifieert de volledigheid, integriteit en het uniek karakter van de gegevens die de RA indient niet, maar vertrouwt er volledig op dat de RA alle gegevens correct indient. De CA verifieert enkel of het serienummer van het certificaat dat de RA aan de certificaataanvraag toewijst daadwerkelijk een uniek serienummer is dat niet eerder voor enig ander certificaat gebruikt werd. Is dit het geval, brengt de CA de RA hiervan op de hoogte.

Alle aanvragen van de RA worden goedgekeurd op voorwaarde dat:

- het formaat ervan geldig is;
- ze via het geschikt, veilig communicatiekanaal ingediend worden;
- alle verificaties behoorlijk uitgevoerd werden conform de bepalingen van het CA contract.

De CA verifieert de identiteit van de RA op basis van de voorgelegde credentials (bewijsstukken).

De CA waarborgt dat het uitgegeven certificaat alle gegevens bevat die hiervoor opgegeven worden in de aanvraag van de RA. De CA waarborgt met name dat de RA een serienummer aan het certificaat toewijst.

Na de uitgave van een certificaat, kondigt de CA dit aan in een Archief en schorst de CA het certificaat. Vervolgens wordt het certificaat aan de RA overhandigd.

De RA vraagt de Kaartinitialisator de certificaten op de elektronische vreemdelingenkaart te laden, waarna de Kaartinitialisator de elektronische vreemdelingenkaart met de certificaten veilig aan de LRA levert.

4.4 Aanvaarding van Certificaten

De LRA laat de elektronische vreemdelingenkaart in aanwezigheid van de vreemdeling activeren in de database van de vreemdelingenkaarten van de RA, aangezien de kaart op dat ogenblik niet geactiveerd is. Zowel de vreemdeling als de RA hebben de activeringsgegevens voor de kaart nodig. Deze gegevens worden veilig geleverd door de Kaartinitialisator. De kaart kan enkel geactiveerd worden door de gegevens van de RA te combineren met die van de vreemdeling.

Enkel de vreemdeling (bij aanvraag van een elektronische vreemdelingenkaart vanaf 12 jaar) of de persoon / personen die het ouderlijk gezag uitoefent / uitoefenen over een kind onder de 12 jaar (bij aanvraag van een elektronische vreemdelingenkaart tot 12 jaar) kan / kunnen beslissen of de certificaten al dan niet geactiveerd worden. Indien de certificaten niet worden geactiveerd, kan de toegang tot bepaalde diensten die de Belgische Federale Overheid en andere leveranciers als derde partij voorzien, beperkt worden op basis van de eID infrastructuur in België en in het buitenland.

Teneinde de certificaten te activeren, dient een aanvraag tot opheffing van schorsing via de RA ingediend te worden bij de CA. Na de activering van de certificaten, kan de vreemdeling de certificaten testen en de inhoud ervan bevestigen.

Een certificaat kan geweigerd worden indien de vreemdeling gegevens bijvoorbeeld onjuist zijn of de vreemdeling de rechtmatige leeftijd voor het gebruik van het certificaat niet heeft bereikt. De RA dient via de LRA op de hoogte gesteld te worden van bezwaren tegen de aanvaarding van een uitgegeven certificaat, zodat aan de CA gevraagd kan worden om de certificaten te herroepen.

4.5 Sleutelparen en het Gebruik van Certificaten

De verantwoordelijkheden in verband met het gebruik van sleutels en certificaten worden hieronder beschreven.

4.5.1 Verplichtingen van de vreemdeling

Tenzij deze CPS anders vermeldt, zijn de verplichtingen van de vreemdeling de volgende:

- Een certificaat niet te vervalsen;
- Certificaten enkel voor wettelijke en toegelaten doeleinden te gebruiken, conform de CPS;
- Een certificaat op een redelijke manier te gebruiken overeenkomstig de omstandigheden;
- Risico's, verlies, onthulling, wijziging of enig ander onbevoegd gebruik van de privésleutels te vermijden.

4.5.2 Verplichtingen van Vertrouwende Partijen

Partijen die afhangen van een certificaat zullen:

- Een certificaat valideren door gebruik te maken van een CRL, Delta CRL, OCSP of door middel van een geldigheidsverklaring die gebaseerd is op het Internet, conform de procedure voor geldigheidsverklaring van het certificaatpad;
- Een certificaat enkel vertrouwen indien het niet geschorst of herroepen werd;
- Op een certificaat vertrouwen, zoals dat redelijk is volgens de omstandigheden.

4.6 Vernieuwing van Certificaten

Certificaten worden vernieuwd indien:

- de elektronische vreemdelingenkaart vernieuwd wordt,

- nieuwe sleutels worden aangevraagd na herroeping van certificaten.

4.7 Nieuwe Sleutels

Na herroeping kunnen de certificaten niet meer geactiveerd worden en moeten dus steeds door nieuwe certificaten vervangen worden. Op aanvraag van de vreemdeling zal de LRA een nieuw sleutelpaar genereren op de elektronische vreemdelingenkaart en de herroepen certificaten vervangen door nieuwe certificaten.

4.8 Wijziging van Certificaten

Hoofdstuk is niet van toepassing.

4.9 Herroeping en Schorsing van Certificaten

Certificaten in een elektronische vreemdelingenkaart blijven in toestand van schorsing totdat de vreemdeling ze aanvaardt of weigert. Een certificaat moet voor de eerste keer geactiveerd worden binnen een maand na de uitgave. De RA en de LRA's treden meteen op om aan deze vereiste te voldoen.

Om de herroeping of schorsing van een certificaat aan te vragen moet de vreemdeling contact opnemen met een LRA, de politie of de RA Helpdesk. De openingsuren van een LRA zijn beperkt, maar de RA Helpdesk is 24 uur per dag en 7 dagen per week geopend.

De politie, LRA of RA Helpdesk vraagt via de RA onmiddellijk de schorsing van de certificaten aan, nadat:

- een kennisgeving ontvangen werd van de vreemdeling, waarin gesteld wordt dat er een vermoeden bestaat dat de privé-sleutel of één van de of beide certificaten verloren, gestolen, gewijzigd of op onbevoegde wijze onthuld of in gevaar gebracht werden;
- De naleving van een verplichting van de LRA volgens deze CPS vertraagd of verhinderd werd door een natuurramp, een computerdefect of een fout in de communicatie, of door enige andere oorzaak die buiten de redelijke controle van de persoon ligt en bijgevolg het vermoeden bestaat dat de informatie van een andere persoon materieel bedreigd of in gevaar gebracht werd;
- Kennisgeving ontvangen werd van de vreemdeling, waarin gesteld wordt dat diens privé-sleutel of één van de of beide certificaten verloren, gestolen, gewijzigd of op onbevoegde wijze onthuld of in gevaar gebracht werden;
- De informatie die een certificaat bevat, gewijzigd werd;
- De naleving van een verplichting van de RA volgens deze CPS vertraagd of verhinderd werd door een natuurramp, een computerdefect of een fout in de communicatie, of door enige andere oorzaak die buiten de redelijke controle van de persoon ligt en bijgevolg de informatie van een andere persoon materieel bedreigd of in gevaar gebracht werd;

De CA schorst of herroept de certificaten op aanvraag van de RA of de CSP.

De RA herroept het geschorste paar certificaten na een termijn van een week indien geen kennisgeving van de vreemdeling ontvangen wordt om de schorsing van de certificaten op te heffen.

In bepaalde omstandigheden (bv. het vermijden van een ramp, risico voor een CA sleutel, een inbreuk op de veiligheid,…), kan de CSP de schorsing en/of herroeping van certificaten aanvragen.

De CSP zal de eID CSP stuurgroep toelating vragen dergelijke herroepingen uit te voeren. Afhankelijk van de graad van dringendheid is het echter mogelijk dat de eID CSP stuurgroep na de beëindiging van het proces op de hoogte gebracht wordt. De RA zorgt ervoor dat de betrokken vreemdelingen op de hoogte gesteld worden van dergelijke schorsing/herroeping.

Afhankelijke partijen moeten om de status van certificaten te controleren gebruik maken van on-line hulpmiddelen die de CA beschikbaar stelt via het archief, alvorens deze certificaten te vertrouwen. De CA werkt de OCSP, de Web interface dienst voor verificatie van certificaatstatus, CRL's en Delta CRL's dienovereenkomstig bij. CRL's worden regelmatig bijgewerkt, met een minimum interval van drie uur.

De CA verleent toegang tot OCSP hulpmiddelen en een website waarop inlichtingenaanvragen over de status van certificaten ingediend kunnen worden.

4.9.1 Termijn en Beëindiging van Schorsing en Herroeping

Een schorsing kan ten hoogste zeven kalenderdagen duren om de omstandigheden te bepalen die aanleiding gaven tot de aanvraag tot schorsing. In het geval van onvoldoende bewijsmateriaal voor dergelijke omstandigheden, kan de vreemdeling de reactivering (de opheffing van de schorsing) van de certificaten aanvragen. Hiervoor moet aan de volgende voorwaarden voldaan worden:

- De vreemdeling moet er zeker van zijn dat het vermoeden dat de privé-sleutel of een van de of beide certificaten verloren, gestolen, gewijzigd of op onbevoegde wijze onthuld of in gevaar gebracht warden, onjuist was;
- Er mag geen enkele andere reden bestaan die aanleiding geeft tot twijfel over de betrouwbaarheid en de vertrouwelijkheid van de privé-sleutels of beide certificaten.

Om de opheffing van schorsing van een certificaat aan te vragen, dient de vreemdeling contact op te nemen met zijn/haar LRA (de gemeente waar hij/zij verblijft).

De LRA vraagt via de RA onmiddellijk de opheffing van de schorsing van een paar certificaten aan, nadat:

- Kennisgeving ontvangen werd van de vreemdeling, waarin gesteld wordt dat een vermoeden bestaat dat de privé-sleutel of één van de of beide certificaten verloren, gestolen, gewijzigd of op onbevoegde wijze onthuld of in gevaar gebracht werden, onmiskenbaar onjuist was;
- Het vermoeden dat de informatie van een andere persoon materieel bedreigd of in gevaar zou zijn door het feit dat de naleving van een verplichting van de RA volgens deze CPS vertraagd of verhinderd werd door een natuurramp, een computerdefect of een fout in de communicatie, of door enige andere oorzaak die buiten de redelijke controle van de persoon ligt, onmiskenbaar onjuist blijkt te zijn;
- Op vraag van de RA , schort de CA een paar certificaten op, of herroept ze;

De CA herroept automatisch een geschorst certificaat na een termijn van een week indien ondertussen geen kennisgeving van de RA ontvangen wordt om de schorsing van het certificaat op te heffen. De CA stelt de RA op de hoogte van alle herroepingen die uitgevoerd worden. De CA publiceert kennisgevingen van geschorste of herroepen certificaten in het Archief.

4.10 Diensten voor Certificaatstatus

De CA stelt diensten om de certificaatstatus te controleren beschikbaar, inclusief CRL's, Delta CRL's, OCSP en geschikte Web interfaces.

CRL en Delta CRL's http://crl.eid.belgium.be

In een Delta CRL worden toevoegingen opgenomen die sinds de publicatie van de laatste basis CRL gemaakt werden.

CRL's en Delta CRL's worden door de CA ondertekend en van een tijdsaanduiding voorzien.

Een CRL wordt elke 24 uur op een overeengekomen tijdstip uitgegeven. Een Delta CRL wordt elke 3 uur uitgegeven, conform een overeengekomen tijdsschema.

De CA stelt alle CRL's en Delta CRL's die in de vorige 12 maanden uitgegeven werden op de Website beschikbaar.

OCSP http://ocsp.eid.belgium.be

De CA stelt OCSP antwoorden beschikbaar voor de Belgische Overheid om deze via de eigen Overheidsnetwerken te gebruiken.

De OCSP dienst van de CSP wordt aangevuld met de OCSP dienst van de BRCA.

Web interface voor dienst voor statusverificatie http://status.eid.belgium.be

Dankzij een eenvoudige web interface voor diensten voor statusverificatie kan een gebruiker informatie over de status van een certificaat verkrijgen. De CA stelt deze web interfaces voor diensten voor statusverificatie beschikbaar aan de Belgische Overheid voor gebruik via en binnen de eigen Overheidsnetwerken.

Met uitzondering van de onderhoudsvensters, mag per kalendermaand de totale tijd waarin de volgende CA diensten onbeschikbaar zijn, uitgedrukt in minuten, over de hele maand niet meer zijn dan 0,5% van het totaal aantal minuten van die kalendermaand:

- OCSP verificatie van certificaatstatus als gevolg van een aanvraag door het RRN, een abonnee of een afhankelijke partij.
- Het downloaden van CRL's of delta CRL's via het Internet of de overheidsnetwerken
- Web interface voor diensten voor de verificatie van certificaatstatussen.

Indien de OCSP dienst, CRL en delta CRL downloaddienst en de Web interface voor de dienst voor statusverificatie onbeschikbaar is, zal ook de plaatselijke infrastructuur van de CA onbeschikbaar zijn, inclusief plaatselijke servers, netwerken en firewalls. Het Internet, of delen ervan, en de plaatselijke infrastructuur van de dienstaanvrager blijven echter wel beschikbaar.

De CA legt een intern archief aan voor de volgende items, gegevens en documenten die tot de aangeboden diensten behoren:

- CRL's en delta CRL's. CRL's en delta CRL's worden voor een periode van minstens 30 jaar na publicatie gearchiveerd.

4.11 Deponeren en recupereren van sleutels

Het is niet toegelaten sleutels te deponeren en nadien te recupereren.

5 BEHEERCONTROLES EN OPERATIONELE EN FYSISCHE CONTROLES

In dit hoofdstuk worden de niet-technische veiligheidscontroles beschreven die de CSP en andere PKI-partners gebruiken voor het aanmaken van sleutels, het identificeren van de betrokken persoon, het uitgeven van certificaten, het herroepen van certificaten, revisie en archivering.

5.1 Fysische Veiligheidscontroles

De CSP voert fysische controles uit binnen het eigen gebouw. Onder de fysische controles van de CSP operator vallen de volgende:

- De CSP operatoren waarborgen dat de gebouwen zich op een geschikte locatie bevinden voor strenge veiligheidscontroles. In deze gebouwen worden de zones genummerd en dienen gesloten kamers, kooien, kluizen en cabines aanwezig te zijn.
- De fysische toegang wordt beperkt door het gebruik van controlesystemen die gericht zijn op de toegang van één zone van de gebouwen naar een andere of op de toegang tot streng beveiligde zones, zoals de lokalisatie van de CSP-activiteiten in een veilige computerkamer met fysische bewaking en veiligheidsalarmen, waarvoor een badge en toegangscontrolelijsten gebruikt worden om zich van de ene zone naar een andere te verplaatsen.
- Overvloedige stroomvoorziening en klimaatregeling.
- De gebouwen worden beschermd tegen blootstelling aan water.
- De CSP treft maatregelen wat betreft brandveiligheid en brandpreventie.
- De media worden veilig bewaard. Er worden veiligheidskopieën van de media bewaard op een andere plaats die fysisch veilig is en beschermd is tegen brand- en waterschade.
- Het afval wordt op een veilige manier verwijderd opdat gevoelige gegevens niet ongewenst onthuld zouden worden.
- De CSP zorgt voor een gedeeltelijke off-site veiligheidskopie.

De CSP beschikt op haar sites over de geschikte infrastructuur om de CSP diensten te verlenen. De CSP zorgt voor eigen veiligheidscontroles op haar sites, waaronder toegangscontrole, inbraakdetectie en bewaking. De toegang tot de sites wordt beperkt door bevoegd personeel. De lijst waarop dit personeel is opgenomen is beschikbaar voor controle.

Voor alle gebieden die uiterst gevoelig materiaal en uiterst gevoelige infrastructuur bevatten, geldt een strenge toegangscontrole. Hiertoe behoren het materiaal en de infrastructuur die nodig zijn voor het ondertekenen van certificaten, CRL's en delta CRL's, OCSP en archieven.

5.2 Procedurecontroles

De CSP volgt het personeel en de beheerspraktijken voldoende om met redelijke zekerheid de betrouwbaarheid en bekwaamheid van de personeelsleden te waarborgen, alsook de toereikende uitvoering van hun taken op gebied van technologieën in verband met elektronische handtekeningen.

Elk personeelslid dient een ondertekende verklaring in bij de CSP, waarin gesteld wordt dat dat personeelslid geen tegenstrijdige belangen heeft bij de CSP, dat het de vertrouwelijkheid zal bewaren en de persoonsgegevens zal beschermen.

De functie van alle personeelsleden die instaan voor het beheer van de sleutels, bestuurders, veiligheidsagenten en systeemcontroleurs of voor enige andere activiteit die dergelijke handelingen materieel beïnvloedt, wordt als betrouwbaar beschouwd.

De CSP voert een initieel onderzoek uit voor alle personeelsleden die zich kandidaat stellen om betrouwbare functies te vervullen, om binnen de mate van het redelijke te proberen hun betrouwbaarheid en bekwaamheid te bepalen.

In het geval dat een dubbele controle nodig is, moet een beroep gedaan worden op de respectieve en afzonderlijke kennis van minstens twee betrouwbare personeelsleden om de begonnen handeling voort te zetten.

De CSP waarborgt dat alle handelingen in verband met de CSP toegeschreven kunnen worden aan het systeem van de CSP en aan het CSP personeelslid dat de handeling uitvoert. Voor belangrijke CSP functies voert de CSP een dubbele controle uit.

De CSP maakt een onderscheid tussen de volgende onderscheiden werkgroepen:

- Uitvoerend CSP personeel dat verrichtingen op certificaten beheert.
- Administratief personeel dat het platform waarop de CSP steunt, organiseert.
- Veiligheidspersoneel om veiligheidsmaatregelen te treffen.

5.3 Veiligheidscontroles voor het Personeel

De CSP voert bepaalde veiligheidscontroles uit op de taken en prestaties van de personeelsleden. Deze veiligheidscontroles worden gedocumenteerd in een beleidsdocument en omvatten de onderstaande gebieden.

5.3.1 Kwalificaties, Ervaring, Vergunningen

De CSP voert controles uit om de achtergrond, kwalificaties en ervaring te bepalen die nodig is/zijn om te voldoen aan de bekwaamheidsgraad voor de specifieke functie. Dergelijke achtergrondcontroles zijn onder meer gericht op:

- Strafrechtelijke veroordelingen voor ernstige misdaden;
- Bedrieglijke handelingen van de kandidaat;
- Toepasselijkheid van referenties;
- Elke vergunning die gepast geacht wordt.

5.3.2 Achtergrondcontroles en Vergunningsprocedures

De CSP voert de relevante controles op potentiële werknemers uit door middel van statusrapporten die uitgegeven worden door een bevoegde autoriteit, verklaringen van derde partijen of ondertekende eigen verklaringen.

5.3.3 Opleidingsvereisten en -procedures

Iedere partij die deel uitmaakt van de CSP zorgt voor opleiding voor het personeel om de CSP functies te kunnen uitvoeren.

5.3.4 Bijscholingsperiode en Bijscholingsprocedures

Het personeel kan regelmatig bijgeschoold worden om voor continuïteit te zorgen en de kennis van het personeel en de procedures bij te werken.

5.3.5 Jobrotatie

Hoofdstuk is niet van toepassing.

5.3.6 Bestraffing van het Personeel

Iedere partij die deel uitmaakt van de CSP bestraft het personeel voor onbevoegde handelingen, het onbevoegd gebruik van bevoegdheid en het onbevoegd gebruik van systemen met als doel verantwoordelijkheid op te leggen aan het CSPpersoneel, naargelang gepast is volgens de omstandigheden.

5.3.7 Controles van onafhankelijke aannemers

Onafhankelijke CSP onderaannemers en diens personeel zijn onderhevig aan de zelfde achtergrondcontroles als het CSP personeel. Deze achtergrondcontroles zijn onder andere gericht op:

- Strafrechtelijke veroordelingen voor ernstige misdaden;
- Bedrieglijke handelingen van de kandidaat;
- Toepasselijkheid van referenties;
- Elke vergunning die gepast geacht wordt.
- Bescherming van de privacy;
- Vertrouwelijkheidsvoorwaarden.

5.3.8 Documentatie voor aanvankelijke opleiding en bijscholing

Iedere partij die deel uitmaakt van de CSP stelt documentatie ter beschikking van het personeel tijdens de aanvankelijke opleiding, de bijscholing of in andere gevallen.

5.4 Procedures voor Audit Logging

Onder de procedures voor audit logging vallen onder andere de event logging en de systeemcontrole. Deze procedures worden toegepast om een veilige omgeving in stand te houden. De CA voert de volgende controles uit:

Het event logging systeem van de CA registreert onder andere de volgende handelingen:

- Uitgave van een certificaat;
- Herroeping van een certificaat;
- Schorsing van een certificaat;
- Re-activatie van een certificaat;
- Automatische herroeping;
- Publicatie van een CRL of delta CRL.

De CSP controleert alle registraties betreffende de event-logging. Registraties van audit trails omvatten:

- De identificatie van de verrichting;
- De gegevens en het tijdstip van de verrichting;
- De identificatie van het certificaat dat betrokken is bij de verrichting;
- De identiteit van de aanvrager van de verrichting.

De CSP legt daarenboven interne logboeken en audit trails aan van relevante operationele handelingen in de infrastructuur, waaronder:

- Het starten en stopzetten van servers;

- Defecten en ernstige problemen;
- Fysische toegang van personeel en andere personen tot gevoelige delen van de CSP site;
- Noodkopieën en herstelling;
- Rapport van testen voor rampherstel;
- Controle-inspecties;
- Bijwerkingen van en wijzigingen aan systemen, software en infrastructuur;
- Schending van de veiligheid en pogingen tot inbraak.

Andere documenten die vereist zijn voor controle zijn:

- Plannen en beschrijvingen van infrastructuur;
- Fysische plannen en beschrijvingen van de site;
- Configuratie van hardware en software;
- Toegangscontrolelijsten voor het personeel.

De CSP waarborgt dat het aangesteld personeel de logbestanden regelmatig nakijkt en abnormale handelingen opspoort en meldt.

Logbestanden en audit trails worden voor inspectie gearchiveerd door het bevoegd personeel van de CA, de RA en aangestelde controleurs. De logbestanden dienen behoorlijk beschermd te worden door middel van een systeem voor toegangscontrole. Van de logbestanden en audit trails worden veiligheidskopieën gemaakt. Controlehandelingen worden niet gemeld.

5.5 Archivering van Registers

De CSP legt interne registers aan van de volgende items:

Alle certificaten gedurende een periode van minstens 30 jaar na de vervaldatum van dat certificaat;

Audit trails van de uitgave van certificaten gedurende minstens 30 jaar na de uitgave van een certificaat;

Audit trail van de herroeping van een certificaat gedurende de periode van minstens 30 jaar na de herroeping van een certificaat;

CRL's en Delta CRL's gedurende minstens 30 jaar na publicatie;

De CSP dient de allerlaatste veiligheidskopie van het CA archief bij te houden gedurende 30 jaar na het laatste certificaat.

De CSP bewaart de archieven in een formaat dat gemakkelijk opgezocht kan worden. De CSP waarborgt de integriteit van de fysische opslagmedia en maakt gebruik van eigen kopiesystemen om het verlies van gegevens te voorkomen.

De archieven zijn toegankelijk voor bevoegd personeel van de CA en de RA.

5.5.1 Soorten registers

De CSP bewaart op een betrouwbare manier de registers van digitale certificaten, controlegegevens en informatie over en documentatie van CSP systemen.

5.5.2 Bewaarperiode

De CSP houdt op betrouwbare manier registers bij van digitale certificaten gedurende een termijn zoals aangegeven in artikel 5.5 van deze CPS.

5.5.3 Archiefbescherming

Enkel de registerbeheerder (personeelslid dat aangesteld is voor de functie van registerbewaring) heeft toegang tot het CSP archief. Er worden maatregelen getroffen om het volgende te waarborgen:

- Bescherming tegen archiefwijzigingen, zoals het opslaan van gegevens op een eenmalig beschrijfbaar medium;
- Bescherming tegen het wissen van archieven;
- Bescherming tegen slijtage van de media waarop het archief opgeslagen wordt, zoals een vereiste dat gegevens regelmatig naar ongebruikte media verplaatst worden.

De CSP zal optreden bij een mogelijke toepassing van de procedure van artikel 14 van de Wet van 8 augustus 1983 en artikel 7 van de Wet van 12 mei 1927 door de Belgische Federale Overheid. In dergelijk geval zal de CSP optreden volgens de instructies van de persoon die aangesteld wordt door middel van een Koninklijk Besluit met betrekking tot gegevens van elektronische vreemdelingenkaarten en certificaten.

5.5.4 Procedures voor de veiligheidskopie van Archieven

Tijdens werkdagen wordt dagelijks een differentiële veiligheidskopie van de CSP archieven gemaakt.

5.5.5 Vereisten voor het aanbrengen van Tijdstempels op Registers

Hoofdstuk is niet van toepassing.

5.5.6 Archiefverzameling

Het CSP-systeem voor archiefverzameling is intern.

5.5.7 Procedures om archiefinformatie te verkrijgen en te verifiëren

Enkel CSP personeelsleden met een duidelijke hiërarchische controle en een welomlijnde functiebeschrijving kunnen archiefinformatie verkrijgen en verifiëren. De CSP bewaart registers in elektronisch formaat of op papier.

5.6 Sleuteloverdracht

Hoofdstuk is niet van toepassing.

5.7 Risico's en Rampherstel

De CSP specificeert in een afzonderlijk intern document toepasselijke procedures voor het melden en behandelen van incidenten en risico's. De CSP specificeert de herstelprocedures die gebruikt worden indien de hulpmiddelen, software en/of gegevens voor berekeningen defect zijn of indien er een vermoeden bestaat dat ze defect zijn.

De CSP bepaalt de nodige maatregelen om het volledig en automatisch herstel van de dienst in geval van ramp, defecte servers, software of gegevens te waarborgen.

Er werd een plan voor de continuïteit van de onderneming uitgewerkt om de voortzetting van de activiteiten te waarborgen na een natuurramp of ander dergelijk voorval. Al deze maatregelen zijn gelijkaardig aan de ISO-norm 1-7799.

De CSP zorgt voor:

- Hulpmiddelen voor rampherstel op twee verschillende plaatsen die voldoende ver van elkaar verwijderd zijn;
- Snelle communicatie tussen de twee sites om de integriteit van de gegevens te waarborgen;
- Een communicatie-infrastructuur vanaf beide sites naar de ondersteunende RA Internet communicatieprotocollen die gebruikt worden door de Belgische Federale Overheid.
- Infrastructuur en procedures voor rampherstel die minstens één keer per jaar getest worden.

5.8 CSP-beëindiging

Zodra de CSP van de Belgische Federale Overheid verneemt dat het contract beëindigd zal worden en/of zodra het contract voortijdig geannuleerd wordt, zal de CSP met de Belgische Federale Overheid overleggen om te bepalen welke stappen vereist zijn om (1) de vlekkeloze overdracht van de dienstverlening op een nieuwe CSP te waarborgen en om (2) de vernietiging, verwijdering, het herstel en of de beveiliging van de informatie, persoonsgegevens en bestanden die de CSP tijdens de uitvoering van haar taken als CSP ontvangen heeft te waarborgen

6 TECHNISCHE VEILIGHEIDSCONTROLES

In dit deel worden de veiligheidsmaatregelen bepaald die de CSP moet nemen om zijn cryptografische sleutel te beschermen en gegevens te activeren (vb. PIN's, paswoorden of manueel bijgehouden gedeelde sleutels).

6.1 Generatie en Installatie van Dubbele Sleutels

De CA beschermt de privé-sleutel(s) overeenkomstig deze CPS. De CA maakt alleen gebruik van privé-sleutels voor de ondertekening van certificaten, CRL's, Delta-CRL's en OCSP-responses, overeenkomstig het gepland gebruik van elk van deze sleutels.

De CA mag de privé-sleutels die gebruikt worden binnen de CA niet gebruiken voor doeleinden buiten het domein van de "Foreigner CA".

6.1.1 Generatieproces van Privé-sleutels

De CA steunt op een betrouwbaar proces voor de generatie van de privé-root key, overeenkomstig een gedocumenteerde procedure. De CA verdeelt de geheime gedeelten van de eigen privé-sleutel(s) en verkrijgt de goedkeuring van de Belgische Federale Overheid, die eigenaar is van de privé-sleutels van de CA, met het oog op de levering van cryptografische acties waarbij gebruik gemaakt worden van de privé-sleutel(s) van de CA. De CA mag deze geheime gedeelten overmaken aan geautoriseerde houders van geheime gedeelten, overeenkomstig een gedocumenteerde procedure.

6.1.1.1 Gebruik van de Privé-sleutel van de CA

De privé-sleutel van de “Foreigner CA” wordt gebruikt om uitgegeven certificaten, de lijst met in te trekken certificaten, de deltas van de lijst met in te trekken certificaten en OCSP-certificaten te ondertekenen. Andere gebruiksdoeleinden zijn onderworpen aan beperkingen.

6.1.1.2 Type Privé-sleutel van de CA

Voor de root key maakt de CA (Belgium Root CA) gebruik van het algoritme RSA SHA-1 met een sleutellengte van 2048 bit.

De eerste Belgium Root CA geheim sleutel is gecertifieerd voor een periode van 27 januari 2003 tot 27 januari 2014.

Voor de hoofdsleutel, maakt de “Foreigner CA” gebruik van het algoritme RSA SHA-1 met een sleutellengte van 2048 bit. De eerste “Foreigner CA” privé-sleutel is geldig van 27 januari 2003 tot 27 juni 2009. Nieuwe “Foreigner CA” privé-sleutels zullen een geldigheid hebben van 6 jaar. Een nieuwe sleutel vervangt de huidige sleutel vóórdat de geldigheidsperiode van de huidige sleutel korter is dan 5 jaar.

6.1.2 Generatie van een CA-Sleutel

De CA genereert en beschermt de privé-sleutel(s) aan de hand van een betrouwbaar systeem en neemt de nodige voorzorgsmaatregelen om te voorkomen dat met de sleutel geknoeid wordt of dat er misbruik van gemaakt wordt. Dit proces wordt gesuperviseerd door vertegenwoordigers van de regering en van de CSP, met het oog op de vertrouwelijkheid van de Belgische Federale Overheid bij de correcte en veilige procedure voor de generatie van CAsleutels. De CA voert generatieprocedures in en documenteert ze overeenkomstig deze CPS. De CA bevestigt openbare, internationale en Europese standaarden voor betrouwbare systemen. Er komen minstens drie betrouwbare aspecten kijken bij de generatie en installatie van privésleutels van de CA.

6.2Nieuwe generatie en installatie van een Dubbele Sleutel

Wanneer (een) geheime sleutel(s) vervangen wordt/worden door (een) nieuwe, moet de CA precies dezelfde procedure gebruiken als in het begin voor de generatie van de sleutel(s). Daarna moet de CA zonder verwijl alle sleutels die in het verleden gebruikt werden en de huidige knoeivrije inrichtingen en alle back-upkopieën van de privé-sleutels ontmantelen en vernietigen zodra ze beschikbaar worden.

6.2.1 Inrichtingen voor de Generatie van CA-sleutels

De generatie van de privé-sleutel van de “Foreigner CA” vindt plaats aan de hand van een veilige cryptografische inrichting die aan de vereisten tegemoetkomt, waaronder FIPS 140-1 niveau 3.

De generatie van de privé-sleutel van de CA vereist de controle van meer dan één geautoriseerd en betrouwbaar lid van het personeel van de CA, en minstens één Belgsich Federale Overheidsafgevaardigde en van de CSP. Meer dan één lid van het CA-management stelt een schriftelijke autorisatie op voor de generatie van de sleutel.

6.2.2 Opslag van Privé-sleutels

De CA maakt gebruik van een veilige cryptografische inrichting voor de opslag van de eigen privé-sleutel, overeenkomstig de vereisten van FIPS 140-1 niveau 3.

6.2.2.1 Controle Opslag CA-sleutels

Voor de opslag van de privé-sleutel van een CA zijn verschillende controles aangewezen die uitgevoerd worden door geautoriseerde en betrouwbare personeelsleden van de CSP. Meer dan

één lid van het CSP-management stelt een schriftelijke autorisatie op voor het aanmaken van de sleutel.

6.2.2.2 Back-up van CA-sleutels

De privé-sleutels van de CA worden bewaard, opgeslagen en opgeroepen door een groot aantal geautoriseerde en betrouwbare leden van het personeel van de CSP. Meer dan één lid van het CSP-management stelt een schriftelijke autorisatie op voor de generatie van de sleutel.

6.2.2.3 Delen van Geheimen

De geheime gedeelten (van gedeelde geheimen) van de CA worden bewaard door een groot aantal geautoriseerde houders, met het oog op de bescherming en grotere betrouwbaarheid van privé-sleutels. De CSP bewaart de privé-sleutels in meerdere inrichtingen die voorkomen dat met de sleutels geknoeid wordt. Er moeten minstens drie leden van de CSP samenwerken om de privé-sleutel van de CA te activeren.

De Privé-sleutels van de CA mogen niet in handen gegeven worden van derden. De CSP voert herstelmaatregelen in ingeval van interne rampen.

6.2.2.4 Aanvaarden van Gedeelde Geheimen

Alvorens houders van geheime gedeelten een geheim gedeelte aanvaarden, moeten zij persoonlijk aanwezig zijn bij de aanmaak, de heraanmaak en de verspreiding van het geheim of de daaropvolgende keten van de bewaring.

De houder van een gedeeld geheim ontvangt dit geheim in een fysiek medium, zoals een door de CA goedgekeurde cryptografische module. De CA houdt schriftelijke verslagen bij over de verspreiding van geheime gedeelten.

6.2.3 De Verspreiding van Privé-sleutels van de CA

De CA documenteert de eigen verspreiding van privé-sleutels. Indien de bewaarders van de tokens vervangen moeten worden, zal de CA toezicht houden op de nieuwe distributie.

6.2.4 Vernietiging van Privé-sleutels van de CA

Aan het einde van het levenscyclus worden de privé-sleutels van de CA door minstens drie betrouwbare personeelsleden van de CSP vernietigd, in aanwezigheid van een vertegenwoordiger van de Belgische Federale Overheid, teneinde te garanderen dat deze privésleutels nooit meer opgeroepen en gebruikt kunnen worden.

De sleutels van de CA worden vernietigd door de primaire en back-up opslagmedia te vernietigen, door de geheime gedeelten te wissen, en door alle hardwaremodules waarop de sleutels bewaard zijn uit te schakelen en definitief te verwijderen.

Het proces voor de vernietiging van de sleutels is gedocumenteerd en alle betrokken bestanden bevinden zich in het archief.

6.3 De bescherming van Privé-sleutels en de Controle van Cryptografische Modules

De CA maakt gebruik van cryptografische inrichtingen om de sleutels van de CA te beheren. Deze cryptografische inrichtingen worden Hardware Security Modules (HSMs) genoemd. Deze inrichtingen zijn conform de vereisten van FIPS 140-1 Niveau 3 of hoger, waarbij onder meer

gegarandeerd wordt dat het knoeien met een inrichting onmiddellijk gedetecteerd wordt en dat privé-sleutels de inrichtingen niet ongecodeerd kunnen verlaten.

Hardware- en softwaremechanismen die de privé-sleutels van de CA beschermen zijn gedocumenteerd.

HSM's verlaten de beveiligde omgeving van de CA niet. Indien HSM's onderhouden of gerepareerd moeten worden en dit kan niet in de vestiging van de CA zelf plaatsvinden, worden zij op veilige wijze naar de producent verstuurd. De privé-sleutels van de CA zijn niet aanwezig in HSM's wanneer deze de CA verlaten om voor onderhoudsdoeleinden verstuurd te worden. Tussen de gebruikssessies in, worden de HSM's in de veilige omgeving van de CA bewaard.

De privé-sleutel van de CA blijft onder controle van minstens 3 personen uit een groep van 5 personen..

De privé-sleutel van de CA kan niet in handen van derden gegeven worden.

Op het einde van een sleutelgeneratie, worden de nieuwe sleutels van de CA gecodeerd op een CD-ROM gebrand (back-upversie). De CA registreert elke stap van dit proces aan de hand van een specifiek formulier voor loginformatie.

De privé-sleutel van de CA wordt op lokaal niveau gearchiveerd in de vestiging van de CA.

De bewaarders van de CA worden belast met de activering en deactivering van privé-sleutels. De sleutel is dan voor een bepaalde tijdsperiode actief.

De privé-sleutel van de CA kan op het einde van zijn levensduur vernietigd worden.

6.4Andere Aspecten van het Beheer van Dubbele Sleutels

De CA archiveert de eigen privé-sleutel(s). De CA geeft certificaten uit met een geldigheidsperiode die op het certificaat zelf vermeld staat.

6.4.1 Computermiddelen, software, en/of beschadigde gegevens

De CA bepaalt welke maatregelen nodig zijn om borg te staan voor het volledig en automatisch herstel van de dienst ingeval van een ramp, verstoorde servers, software of gegevens. Deze maatregelen zijn conform de ISO-norm 1-7799.

De CA bepaalt herstelmiddelen die voldoende afstand nemen van de primaire bronnen, om te voorkomen dat beiden aangetast worden ingeval van een ramp. De CA zorgt verder voor voldoende snelle communicatiemiddelen tussen beide sites, met het oog op de instandhouding van de gegevens. De CA zorgt voor een goed beveiligde infrastructuur voor de communicatie tussen beide sites en de RA, het Internet en de netwerken van de Openbare Administratie.

De CA neemt de nodige maatregelen om deze herstelinfrastructuur en –procedures minstens een keer per jaar te testen.

6.4.2 De intrekking van een Privé-sleutel van de CA

Indien de privé-sleutel van een "Foreigner CA" ingetrokken werd, moet de CA onmiddellijk:

- Alle Certificatieautoriteiten waarschuwen die de sleutel gecertificeerd hebben.
- De RA waarschuwen.
- Het groot publiek op de hoogte stellen, aan de hand van verschillende kanalen:
  - Een bericht op de website van de CA.
  - Een persbericht gericht aan de Belgische media.
  - Advertenties in de belangrijkste Belgische dagbladen.
- Het certificaat van de "Foreigner CA" opnemen in CRL's en delta-CRL's.
- De status van het certificaat aanpassen in de Webinterfacedienst.
- Alle certificaten intrekken die ondertekend werden met het ingetrokken certificaat.

- Na gepeild te hebben naar de reden van de intrekking, maatregelen genomen te hebben om te voorkomen dat dit in de toekomst herhaald en de goedkeuring van de RA te hebben bekomen, mag de CA:
- Een nieuwe dubbele sleutel en bijhorend certificaat aanmaken.
- Alle ingetrokken certificaten opnieuw uitgeven.

6.4.3 Privé-sleutel van de CA waarmee geknoeid werd

Indien met de privé-sleutel van de CA geknoeid werd, moet het overeenkomstig certificaat onmiddellijk ingetrokken worden. De CA neemt overigens alle maatregelen beschreven bij punt 6.4.2.

6.5 Activatiegegevens

De CA bewaart en archiveert of veilige wijze activatiegegevens die verband houden met de eigen privé-sleutel en handelingen.

6.6 Veiligheidscontroles Computermateriaal

De CA voert een aantal veiligheidscontroles voor het computermateriaal in.

6.7 Veiligheidscontroles Levenscyclus

De CA voert regelmatig ontwikkelingscontroles en veiligheidscontroles van het management uit.

6.8 Veiligheidscontroles van het Netwerk

De CA beschikt over een hoog veiligheidsniveau van het systeemnetwerk, inclusief firewalls. Intrusies in het netwerk worden gecontroleerd en opgespoord. Meer bepaald:

Alle communicatie tussen de CA en de RA-operator met betrekking tot een van de fasen van de levenscyclus van een certificaat, wordt beveiligd met PKI-gebaseerde technieken voor de codering en ondertekening, met het oog op de vertrouwelijkheid van de informatie en de wederzijdse authentificatie. Dit behelst communicatie over de aanvraag van certificaten, uitgiftes, schorsingen, het teniet doen van schorsingen en de intrekking.

De website van de CA biedt gecodeerde verbindingen dankzij een Secure Socket Layer (SSL) protocol en een bescherming tegen virussen.

Het CA-netwerk wordt beschermd door een beheerde firewall en systeem voor het opsporen van intrusies.

Het is verboden toegang te hebben tot gevoelige CA-bronnen, waaronder CA-databanken extern aan het eigen netwerk van de CA-operator.

De internetsessies voor de aanvraag en afgifte van informatie zijn gecodeerd.

7 CERTIFICAAT- EN CRL-PROFIELEN

In dit deel wordt dieper ingegaan op het formaat van certificaten, CRL en OCSP.

7.1 Profiel van een Certificaat

7.1.1 Identiteitscertificaat

De beschrijving van de velden van dit certificaat wordt in de onderstaande tabel weergegeven. In dit certificaat mogen geen pseudoniemen gebruikt worden.

Foreigner Authentication Certificate					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the RRN	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 5 years and 3 months[12]	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Foreigner CA	Fixed
SerialNumber		X		<yyyy><ss>[13]	
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	

[12] maximum certificate validity period, shorter certificate validity periods can be applied

[13] <yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field.

CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under BRCA(1) 2.16.56.1.1.1.7.2 Certificates issued under BRCA2 2.16.56.9.1.1.7.2	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
					Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
digitalSignature				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/eidf<yyyy><ss>[14].crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslClient - smime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		Certificates issued under BRCA(1) http://certs.eid.belgium.be/belgiumrs.crt Certificates issued under BRCA2 http://certs.eid.belgium.be/belgiumrs2.crt	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be	

[14] <yyyy> represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field

7.1.2 Handtekeningscertificaat

De beschrijving van de velden van dit certificaat wordt in de onderstaande tabel weergegeven. In dit certificaat mogen geen pseudoniemen gebruikt worden.

Foreigner Signature Certificate					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the RRN	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 5 years and 3 months[15]	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Foreigner CA	Fixed
SerialNumber		X		<yyyy><ss>[16]	
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under the BRCA(1) 2.16.56.1.1.1.7.1 Certificates issued under the BRCA2 2.16.56.9.1.1.7.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed

[15] maximum certificate validity period, shorter certificate validity periods can be applied.

[16] <yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field.

Qualifier		X		http://repository.eid.belgium.be	Fixed
Qualified Certificate Statement					
qcStatement	{ id-etsi-qcs 1 }	X		0.4.0.1862.1.1	
KeyUsage	{id-ce 15}	X	TRUE	N/a	
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/eidf<yyyy><ss>[17].crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sMime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		Certificates issued under the BRCA(1) http://certs.eid.belgium.be/belgiumrs.crt Certificates issued under the BRCA2 http://certs.eid.belgium.be/belgiumrs2.crt	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be	

7.1.3 Certificaat “Foreigner CA”

Dit certificaat wordt door de BRCA gepubliceerd om de CA aan de hand van een digitale handtekening te identificeren. De beschrijving van de velden van dit certificaat wordt in de onderstaande tabel weergegeven.

Foreigner CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	

[17] <yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field.

SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years and 8 months	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Certificate issued under the BRCA(1): Belgium Root CA Certificates issued under the BRCA2: Belgium Root CA2	Fixed
Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Foreigner CA	Fixed
SerialNumber		X		<yyyy><ss>	
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under the BRCA(1): 2.16.56.1.1.7.2	Fixed
				Certificates issued under the BRCA2: 2.16.56.9.1.7.2	
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
CrlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
DistributionPoint					
FullName		X		Certificates issued under the BRCA(1): http://crl.eid.belgium.be/belgium.crl Certificates issued under the BRCA2: http://crl.eid.belgium.be/belgium2.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		

	2.16.840.1.113730.1.1			SslCA – smimeCA – ObjectSigning CA	Fixed

7.2 Profiel van een CRL

Overeenkomstig IETF PKIX RFC 2459, ondersteunt de CA CRL's conform:

- Versienummers ondersteund voor CRL's.
- De inhoud van CRL's en de extensies van CRL's en hun kritikaliteit.

Het profiel van een CRL, of Lijst voor de Intrekking van een Certificaat, wordt in de onderstaande tabel weergegeven:

Version	v2
Signature	sha1RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time+7 days >
RevokedCertificates	
UserCertificate	<certificate serial number>
RevocationDate	<revocation time>
CrlEntryExtensions	
CRL Reason Code	Certificate Hold(6) (for suspended certificates) Note: Otherwise NOT included!
CrlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <CA assigned unique number>

Het profiel van de delta-CRL voor de intrekking van een certificaat wordt in de onderstaande tabel weergegeven:

Version	v2
signature	sha1RSA
Issuer	<subject CA>
thisUpdate	<creation time>
nextUpdate	<creation time> +7 days
RevokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
CRL Reason Code	Certificate Hold(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 <CA assigned unique number>
Delta CRL Indicator	<base CRL Number>

De CRL's en Delta CRL's van de CA ondersteunen de velden en hun extensies, nader bepaald in hoofdstuk 5 van RFC 2459: "Internet X.509 Openbare Sleutelinfrastructuur en CRL-profiel".

7.3 Profiel van een OCSP

Het profiel van een OCSP volgt IETF PKIX RFC2560 OCSP v1. Geen enkele OCSP-extensie wordt ondersteund. De CA ondersteunt verschillende certificaatstatussen in een enkele OCSPaanvraag, voor zover die ondertekend worden door dezelfde CA. De respons van de OCSP wordt ondertekend door een geheime sleutel waarvan de overeenstemmende publieke sleutel gecertificeerd wordt door alle Foreigner CA's.

Dit certificaat wordt gepubliceerd door de Root-CA van de Belgische Federale Overheid, met het oog op de certificering van de OCSP-responders. De beschrijving van de velden van dit certificaat wordt in de onderstaande tabel weergegeven.

Belgium OCSP Responder					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Generated by the CA at Key Generation Process Time	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 1 Year and 3 months	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		[Issuing CA]	Fixed
SerialNumber		X		<yyyy><ss>[18]	

[18] <yyyy>: is het jaar waarin de CA voor het eerst wordt gebruikt b.v. 2006; <ss>: uniek serieel nummer gebruikt om CA certificaten, enkel gebruikmakend van dit veld, op te zoeken ter ondersteuning van toepassingen.

Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }			Belgium OCSP Responder	Fixed
Standard Extensions	OID	Include	Critical	Value	
KeyUsage	{id-ce 15}	X	TRUE	N/a	
DigitalSignature				Set	Fixed
enhancedKeyUsage			FALSE		
ocspSigning	1.3.6.1.5.5.7.3.9	X			
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
ocspNoCheck	{ id-pkix-ocsp 5 } 1.3.6.1.5.5.7.48.1.5		FALSE		
Null		X			

8 AUDIT VAN DE OVEREENKOMSTIGHEID EN ANDERE BEOORDELINGEN

Wat het Gekwalificeerd handtekeningcertificaat betreft, gaat de CSP te werk volgens de voorwaarden van artikel 17, Sectie 1 van de Wet van 9 juli 2001 die het wettelijk kader bepaalt voor elektronische handtekeningen in België. De CSP komt tegemoet aan de vereisten opgesomd in de ETSI-beleidsdocumenten die verwijzen naar handtekeningcertificaat, waaronder:

- TS 101 456 Beleidsvereisten voor certificatieautoriteiten die gekwalificeerde handtekeningcertificaat uitgeven;
- TS 101 862 Profiel van gekwalificeerde handtekeningcertificaten.

Wat het identiteitscertificaat betreft, komt de CSP tegemoet aan de vereisten opgesomd in de ETSI-beleidsdocumenten die verwijzen naar openbare sleutelcertificaten, waaronder:

- TS 101 042 Beleidsvereisten voor certificatieautoriteiten die openbare sleutelcertificaten uitgeven (Genormaliseerd niveau).

De CSP aanvaardt conformiteitsaudits, om na te gaan of de vereisten, standaarden, procedures en dienstniveaus overeenkomstig deze CPS zijn. De CSP aanvaardt deze audits op de eigen praktijken en procedures, voor zover dit niet indruist tegen bepaalde voorwaarden zoals de vertrouwelijkheid van de informatie, zakelijke geheimen, enz. Dergelijke controles worden hetzij rechtstreeks uitgevoerd, hetzij door bemiddeling van:

- De autoriteit die toezicht houdt op de Certificatiedienstverlener in België, handelend onder de autoriteit van de Belgische Federale Overheid.
- De Belgische Federale Overheid, of een derde partij aangesteld door de Belgische Federale Overheid

De CSP evalueert de resultaten van deze audits, vooraleer ze verder in te voeren.

Om de audits uit te voeren, wordt een onafhankelijke controleur aangesteld die noch rechtstreeks noch onrechtstreeks verband houdt met de CSP of om het even welke andere CA, en waarbij er bijgevolg geen sprake is van belangenconflicten.

Bij de audit wordt op de volgende elementen gelet:

- Overeenkomstigheid van de bedrijfsprocedures en –principes van de CSP met de procedures en dienstniveaus bepaald in de CPS; • Beheer van de infrastructuur die de CSP-diensten invoert;
- Beheer van de fysieke infrastructuur van de site.
- Aanhankelijkheid aan de CPS;
- Respect voor de betrokken Belgische wetten;
- Bevestiging van de overeengekomen dienstniveaus;
- Inspectie van auditsporen, logs, relevante documenten, enz.;
- De reden waarom de hierboven vermelde voorwaarden niet nageleefd werden.

Indien afwijkingen vastgesteld worden, overhandigt de CSP een verslag aan de auditeur. In dit verslag worden de maatregelen opgesomd die genomen zullen worden om de situatie weer in goede banen te leiden en om wel overeenkomstig de voorwaarden te handelen. Indien de voorgestelde maatregelen niet volstaan, wordt overgegaan tot een tweede audit.

Certipost NV voldoet aan de huidige versie van de basisvereisten voor de uitgifte en het beheer van openbaar-vertrouwde certificaten ("Baseline Requirements") gepubliceerd op

http://www.cabforum.org. In het geval van enige tegenspraak tussen dit document en deze vereisten, hebben die vereisten voorrang op dit document.

9 ANDERE ZAKELIJKE EN WETTELIJKE KWESTIES

9.1 Vergoedingen

De Wet op de Identiteitskaarten bepaalt het bedrag van de vergoeding die de vreemdeling verschuldigd is voor de certificaten op zijn elektronische vreemdelingenkaart.

De CA rekent geen vergoeding aan voor de publicatie en de afhaling van deze CPS.

De CA biedt gratis de volgende diensten:

- De publicatie van certificaten;
- De intrekking van certificaten;
- De schorsing van certificaten;
- De publicatie van CRL's en Delta CRL's.

De Belgische Federale Overheid heeft gratis toegang tot de volgende middelen:

- Verificatie van de OCSP status;
- Downloaden van CRL's en Delta CRL's;
- Verificatie van de certificaatstatus;
- Certificaatdirectory.

Aan de hand van speciale procedures, stelt de CA gratis de volgende diensten op aanvraag ter beschikking van de gebruiker:

Dienst	Gratis
Verificatie OCSP-status	10 aanvragen per gebruiker per dag
Download CRL	1 download per gebruiker per week
Download Delta CRL	8 downloads per gebruiker per dag
Certificaatdirectory	30 downloads per week
Verklaring Certificatiepraktijk	2 downloads per gebruiker per dag

De CA voert mechanismen in die voorkomen dat deze diensten misbruikt worden. Indien vaker dan hierboven vermeld gebruik gemaakt wordt van een welbepaalde dienst, dan kan de CSP dit aanrekenen aan de klant, in het kader van de overeenkomst tussen de CSP en de Belgische Federale Overheid.

9.2 Aansprakelijkheid

De aansprakelijkheid van de CSP ten opzichte van de intekenaar of een hiermee vertrouwende partij beperkt zich tot het betalen van een schadevergoeding tot 2500 € per transactie.

9.2.1 Gekwalificeerde certificaten

Wat de publicatie van de Gekwalificeerde Certificaten inzake handtekeningen (handtekeningcertificaat) betreft, regelt artikel 14 van de Wet op de elektronische handtekeningen de aansprakelijkheid van de CSP.

Volgens deze bepaling, is de CSP aansprakelijk voor de schade die hij toebrengt aan elke instelling of natuurlijke persoon of rechtspersoon die redelijkerwijze vertrouwen stelt in het certificaat, voor wat betreft:

(a) de juistheid van alle gegevens die in het gekwalificeerd certificaat opgenomen zijn op de datum dat het werd afgegeven en de vermelding, in dit certificaat, van alle voorgeschreven gegevens voor een gekwalificeerd certificaat;

(b) de garantie dat de in het gekwalificeerd certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, de gegevens bevat voor het aanmaken van de handtekening, in overeenstemming met de in het certificaat vermelde of geïdentificeerde gegevens voor het verifiëren van de handtekening;

(c) de garantie dat de gegevens voor het aanmaken en de gegevens voor het verifiëren van een handtekening complementair gebruikt kunnen worden;

De CSP is aansprakelijk voor schade toegebracht aan een entiteit of wettelijke of rechtspersoon die redelijkerwijs rekent op het certificaat, ingeval de intrekking van het certificaat niet geregistreerd werd, tenzij de CSP kan bewijzen dat hij niet nalatig geweest is.

9.2.2 Certificaten die niet als gekwalificeerd beschouwd worden

De algemene aansprakelijkheidsregels zijn van toepassing op schade toegebracht aan een entiteit of natuurlijke persoon of rechtspersoon die redelijkerwijs vertrouwen stelt in een certificaat uitgegeven door de CSP.

De CSP wijst uitdrukkelijk elke aansprakelijkheid af ten opzichte van vertrouwende partijen, in alle gevallen waarin een identiteitscertificaat gebruikt wordt voor het aanmaken van elektronische handtekeningen.

9.3 Vertrouwelijk Karakter van de Informatie

In het kader van de geleverde diensten, treedt de CA- en RA-operator (RRN) op voor de controle van de behandeling van persoonsgegevens, krachtens artikel 16 van de Wet van 8 December 1992, terwijl de gemeentebesturen optreden voor de behandeling van de persoonsgegevens.

De CSP respecteert de regels met betrekking tot het vertrouwelijk karakter van de persoonsgegevens, zoals beschreven in deze CPS. Vertrouwelijke informatie behelst:

- Elk persoonlijke en identificeerbare informatie over vreemdelingen, verschillend van de informatie opgenomen in een certificaat.
- De precieze reden voor de intrekking of schorsing van een certificaat
- Audit trails.
- Loginformatie met het oog op het opstellen van verslagen, zoals de logs aangevraagd door de RA.
- Briefwisseling met betrekking tot de diensten van de CA.
- Privé-sleutels van de CA.

De volgende elementen zijn geen vertrouwelijke informatie:

- Certificaten en hun inhoud.
- De status van een certificaat.

De CSP mag geen vertrouwelijke informatie openbaar maken zonder een authentieke en gegronde aanvraag, waarin wordt vermeld:

- De partij waartegenover de CA zich geëngageerd heeft tot het bewaren van vertrouwelijke informatie. De CA heeft deze plicht ten opzichte van de RA en gaat onmiddellijk in op dergelijke aanvragen;
- Een bevel van de rechtbank.

In het kader van de Raamovereenkomst tussen de CSP en de Belgische Federale Overheid, mag de CSP een administratieve vergoeding aanrekenen voor de verwerking van dergelijke openbaarmakingen.

Partijen die vertrouwelijke informatie vragen en krijgen, hebben de toestemming deze informatie te gebruiken, op voorwaarde dat ze voor de vermelde doeleinden gebruikt worden, dat ze geen voorwerp uitmaken van een compromis en dat ze niet aan derden overgemaakt of bekendgemaakt worden.

Deze partijen zijn verplicht persoonlijke gegevens geheim te houden, overeenkomstig de wetgeving terzake.

9.3.1 Voorwaarden betreffende de Openbaarmaking

Niet vertrouwelijke informatie kan openbaar gemaakt worden aan elke vreemdeling en vertrouwende partij, op de hierna volgende voorwaarden:

- De status van een enkel certificaat wordt geleverd op aanvraag van een vreemdeling of vertrouwende partij;
- De vreemdelingen hebben inzage in de niet vertrouwelijke informatie die de CSP over hen bewaart.

Vertrouwelijke informatie wordt door de CSP niet openbaar gemaakt aan vreemdelingen of vertrouwende partijen, met uitzondering van informatie over:

- Henzelf;
- Personen onder hun voogdij.

Alleen de RA heeft inzage in de vertrouwelijke informatie.

De CSP beheert de openbaarmaking van informatie aan het personeel van de CSP.

De CA bevestigt zelf de openbaarmaking van informatie aan elke partij die dit vraagt, door:

- Tegemoet te komen aan aanvragen van OCSP, CRL's en delta-CRL's.

De CA codeert alle mededelingen van vertrouwelijke informatie, inclusief:

- De mededelingen tussen de CA en de RA;
- Zittingen waarbij certificaten worden overhandigd.

Naast de informatie in het bezit van de CSP, beschikt de RA ook over informatie met betrekking tot de certificaten, meer bepaald in het Register van de vreemdelingenkaarten. De Wet op het Rijksregister regelt de toegang tot het Register van de vreemdelingenkaarten en andere gegevens over de vreemdelingen waarover de RRN beschikt.

9.3.2 Privacy van Persoonlijke Informatie

De CSP handelt in het kader van de Belgische wet van 8 december 1992 houdende de Bescherming van de Privacy met betrekking tot de Behandeling van Persoonsgegevens, gewijzigd door de wet van 11 december 1998 waarbij de Europese richtlijn 1995/46 wordt ingevoerd houdende de Bescherming van het Individu met betrekking tot de Behandeling van Persoonsgegevens en het Vrij Verkeer van deze Gegevens. De CSP bevestigt tevens de Europese richtlijn 2002/58 betreffende de Behandeling van Persoonsgegevens en de Bescherming van de Privacy in de Sector van de elektronische communicatie.

De CSP bewaart geen andere gegevens over certificaten of vreemdelingen verschillend van de gegevens waarvan het in bezit gekomen is en die geautoriseerd zijn door de RA. Zonder de toelating van de persoon waarop de gegevens betrekking hebben of zonder een uitdrukkelijke wettelijke toestemming, worden de persoonsgegevens behandeld door de CSP niet voor andere doeleinden gebruikt.

9.3.3 Intellectuele Eigendomsrechten

De Belgische Federale Overheid is eigenaar van alle intellectuele eigendomsrechten die verband houden met de eigen databases, websites, de CA digitale certificaten en om het even welke andere publicatie die uitgaat van de CSP, inclusief deze CPS.

De CSP is eigenaar van alle intellectuele eigendomsrechten die verband houden met de eigen infrastructuur, databases, website, enz.

Elke software en documentatie ontwikkeld door de CSP in het kader van het project voor de Belgische elektronische vreemdelingenkaart, zijn de exclusieve eigendom van de Belgische Federale Overheid.

9.4 Vertegenwoordigingen en Garanties

Binnen het domein van de CSP, waaronder de CA zelf, staan de RA, de CM, de LRA's en de vreemdelingen garant voor de instandhouding van hun respectieve privé-sleutel(s). Indien een partij het vermoeden heeft dat een privé-sleutel in het gedrang gekomen is, dan wordt hun LRA (gemeentebestuur), de politie of de RA Helpdesk onmiddellijk op de hoogte gebracht.

9.4.1 Plichten van de vreemdeling

Tenzij anders vermeld in deze CPS, hebben de vreemdelingen de volgende plichten:

- Ze moeten zich ervan weerhouden met een certificaat te knoeien.
- Ze mogen certificaten alleen gebruiken voor wettelijke en toegestane doeleinden, overeenkomstig de CPS.
- Een nieuwe elektronische vreemdelingenkaart (en dus certificaat) aanvragen ingeval van wijzigingen aan de informatie die in het certificaat opgenomen is;
- De openbare sleutel van de vreemdeling niet gebruiken om in het kader van een gepubliceerd certificaat andere certificaten te verkrijgen;
- Een certificaat op redelijke wijze gebruiken, volgens de omstandigheden;
- Voorkomen dat de privé-sleutels in het gedrang komen, verloren gaan, openbaar gemaakt worden, wijzigingen ondergaan of op oneigenlijke wijze gebruikt worden;
- De politie, het gemeentebestuur of de RA Helpdesk contacteren voor een aanvraag tot schorsing van een certificaat, ingeval van een evenement dat het vermoeden doet rijzen dat de materiële integriteit van het certificaat in het gedrang gekomen is. Met dergelijke evenementen wordt bedoeld verlies, diefstal, wijziging, niet geautoriseerde openbaarmaking of een andere aantasting van de privé-sleutel of een of beiden van de certificaten;

- De politie, het gemeentebestuur of de RA Helpdesk contacteren voor een aanvraag tot intrekking van een certificaat, ingeval van een evenement dat het vermoeden doet rijzen dat de materiële integriteit van het certificaat in het gedrang is gekomen. Met dergelijke evenementen wordt bedoeld het verlies, de diefstal, de wijziging, de niet geautoriseerde openbaarmaking of een andere aantasting van de privé-sleutel of een of beiden van de certificaten, of ingeval de controle van de private sleutel niet meer verzekerd is wegens het ingevaarbrengen van de activatiegegevens (bv. PIN code);
- Verplichting het sleutelpaar te gebruiken om een elektronische handtekening aan te brengen overeenkomstig alle andere beperkingen die aan de gebruiker zijn opgelegd;
- Verplichting er redelijk zorg voor te dragen dat er geen niet-geautoriseerd gebruik wordt gemaakt van de private sleutels;
- Na ingevaarbrenging, de verplichting om onmiddellijk en definitief elk gebruik van de private sleutels te staken;
- Het sleutelpaar enkel gebruiken in overeenstemming met de beperkingen die hem ter kennis werden gebracht;
- Verplichting zijn private sleutel te allen tijde te beschermen tegen verlies, openbaarmaking aan een andere partij, niet-gewettigde wijziging en niet-gewettigd gebruik;
- De RA Helpdesk RA onmiddellijk op de hoogte te brengen indien de controle over de private sleutel verloren werd doordat de PIN code gecompromitteerd werd ;
- Verplichting onmiddellijk en definitief elk gebruik van de private sleutel stop te zetten zodra deze gecompromitteerd werd.

9.4.2 Plichten van de Vertrouwende Partijen

Een partij die vertrouwt op een CA-certificaat moet:

- Voldoende geïnformeerd zijn over het gebruik van digitale certificaten en PKI;
- Mededelingen ontvangen en de voorwaarden van deze CPS en de voorwaarden voor vertrouwende partijen naleven;
- Een certificaat valideren met behulp van een CRL, delta CRL, OCSP of webgebaseerde validatie van een certificaat, overeenkomstig de procedure voor de validatie van een certificatie;
- Alleen vertrouwen stellen in certificaten tijdens de geldigheidsperiode die niet geschorst of ingetrokken werden;
- Op redelijke wijze vertrouwen stellen in een certificaat, in functie van de omstandigheden.

De vertrouwende partijen die toegang hebben tot de informatie die beschikbaar gesteld wordt in de CA-bronnen en website, hebben de verantwoordelijkheid deze informatie te beoordelen en erop te vertrouwen.

Indien een vertrouwende partij vaststelt of vermoedt dat er werd geknoeid met een privésleutel, dan moet hij de RA helpdesk hiervan onmiddellijk op de hoogte brengen.

9.4.3 Aansprakelijkheid van de vreemdeling ten opzichte van de Vertrouwende Partijen

Een vreemdeling die in het bezit is van een elektronische vreemdelingenkaart met geactiveerde sleutels voor de authentificatie en handtekeningen, is aansprakelijk ten opzichte van de vertrouwende partijen voor elk gebruik dat van deze kaart gemaakt wordt, inclusief de sleutels en certificaten, tenzij hij kan bewijzen dat met deze sleutel geknoeid werd en dat hij alle nodige maatregelen genomen heeft om zijn certificaten tijdig te laten intrekken.

9.4.4 Gebruiksvoorwaarden van het Opvraagcentrum en de Website

Alle partijen, inclusief de vreemdelingen en vertrouwende partijen, die toegang hebben tot het opvraagcentrum en de website van de CA, gaan akkoord met de bepalingen van deze CPS en de andere gebruiksvoorwaarden. De vreemdelingen en vertrouwende partijen geven blijk van hun goedkeuring van de gebruiksvoorwaarden en deze CPS, door een aanvraag in te dienen betreffende de status van een digitaal certificaat, of door gebruik te maken van en te vertrouwen op dergelijke geleverde informatie of diensten. Het opvraagcentrum van de CA raadplegen kan op de volgende manier:

- Informatie bekomen als het resultaat van het zoeken naar een digitaal certificaat;
- Controleren of de status van digitale handtekeningen gecreëerd met een privésleutel overeenstemmen met een openbare sleutel bevat in een certificaat;
- Informatie bekomen die gepubliceerd is op de website van de CA;
- Andere diensten die de CA via zijn site aanbiedt of promoot.

9.4.4.1 Vertrouwen op Eigen Risico

De partijen die toegang hebben tot de informatie bevat in het opvraagcentrum en de website hebben de verantwoordelijkheid deze informatie te beoordelen en er gebruik van te maken.

9.4.4.2 Juistheid van de Informatie

De CSP stelt alles in het werk om ervoor te zorgen dat de partijen die toegang hebben tot het opvraagcentrum kunnen beschikken over nauwkeurige, recente en juiste informatie. De CSP kan evenwel niet aansprakelijk gesteld worden buiten de limieten bepaald in artikel 9.2 van deze CPS.

9.4.5 Plichten van de CSP

In de mate gespecificeerd in de relevante delen van de CPS, moet de CSP:

- Deze CPS en amendementen respecteren, zoals die gepubliceerd worden op de site http://repository.eid.belgium.be;
- Een infrastructuur en certificatiediensten voorzien, inclusief de opstelling en werking van het opvraagcentrum en de website van de CSP voor de werking van openbare certificatiediensten;
- Vertrouwensmechanismen voorzien, inclusief een mechanisme voor het genereren van sleutels, de bescherming van deze sleutels en procedures voor het delen van geheimen met betrekking tot de eigen infrastructuur;
- De RA onmiddellijk informeren ingeval geknoeid werd met de eigen privé-sleutel(s);
- Elektronische certificaten uitgeven overeenkomstig deze CPS en de hierin vermelde plichten vervullen;
- De RA informeren indien de CSP niet in staat is de toepassing te valideren overeenkomstig deze CPS;
- Na ontvangst van een geauthentiseerde aanvraag van de RA, snel handelen om een certificaat uit te geven overeenkomstig deze CPS;
- Na ontvangst van een geauthentiseerde aanvraag vanwege de RA tot intrekking van een certificaat, snel handelen om het certificaat in te trekken overeenkomstig deze CPS;

- Na ontvangst van een geauthentiseerde aanvraag vanwege de RA tot schorsing van een certificaat, snel handelen om het certificaat overeenkomstig deze CPS te schorsen;
- Na ontvangst van een geauthentiseerde aanvraag vanwege de RA tot het tenietdoen van de schorsing van een certificaat, snel handelen om de schorsing van het certificaat teniet te doen overeenkomstig deze CPS;
- Certificaten publiceren overeenkomstig deze CPS.
- Regelmatig CRL's, delta CRL's en OCSP-responsen publiceren van alle geschorste en ingetrokken certificaten, overeenkomstig deze CPS;
- Gepaste dienstniveaus leveren, overeenkomstig wat bepaald werd in het kader van de overeenkomst van de CSP met de Belgische Federale Overheid;
- Een kopie maken van deze CPS en de van toepassing zijnde beleiden die beschikbaar zijn op de website;
- Handelen overeenkomstig de Belgische wetgeving. De CSP moet in het bijzonder tegemoetkomen aan alle wettelijke vereisten die verbonden zijn met het profiel van gekwalificeerde certificaten voortvloeiend uit de Belgische wet van 9 juli 2001 met betrekking tot de elektronische handtekeningen, en de Europese Richtlijn 1999/93 in het communautair kader van de elektronische handtekeningen.

Indien de CSP vaststelt of vermoedt dat er geknoeid werd met een privé-sleutel, dan moet hij de RA hiervan onmiddellijk op de hoogte brengen.

Wanneer een beroep gedaan wordt op een derde persoon, moet bijzonder gelet worden op de financiële verantwoordelijkheid en aansprakelijkheid van deze contractant.

De CSP heeft een verantwoordelijkheid ten opzichte van de vreemdelingen en vertrouwende partijen, voor de volgende daden of voor het volgend verzuim:

- Het uitgeven van digitale certificaten die geen gegevens bevat voorgelegd door de RA;
- Wanneer met een privé-sleutel van de CA geknoeid werd;
- Het verzuim om een geschorst certificaat na een periode van een week in te trekken;
- Het verzuim een geschorst of ingetrokken certificaat op te nemen in een CRL of delta CRL;
- Het verzuim vanwege de OCSP-responder om een certificaat op te geven als zijnde geschorst of ingetrokken;
- Wanneer een Webinterface geen informatie weergeeft over de status van een certificaat;
- De niet geautoriseerde openbaarmaking van vertrouwelijke informatie of persoonlijke gegevens, overeenkomstig 9.3 en 9.4.
- Verantwoordelijk zoals gedefineerd in 9.2

De CSP verklaart geen verdere plichten te hebben in het kader van deze CPS.

9.4.6 Meting van het Dienstniveau

De Belgische Federale Overheid, tesamen met de eID-partners, legt controles op teneinde de conformiteit van de eID verbonden diensten met het Service Level Agreements bepaald in deze CPS te garanderen.

9.4.7 Plichten Registratieautoriteit (van toepassing op RRN)

De RA die actief is in het domein van de CA moet:

- Correcte en precieze informatie leveren in de communicaties met de CA;
- Ervoor zorgen dat de openbare sleutel afgeleverd aan de CA overeenkomt met de gebruikte privé-sleutel;
- Certificaataanvragen creëren overeenkomstig deze CPS.
- Alle controle- en authenticiteithandelingen uitvoeren voorgeschreven door de procedures van de CA en deze CPS;
- De aanvraag van de kandidaat in een ondertekend bericht overmaken aan de CA;
- Alle aanvragen tot intrekking, schorsing en teniet doen van de schorsing van een certificaat ontvangen, controleren en overmaken aan de CA, overeenkomstig de procedures van de CA en deze CPS;
- De juistheid en authenticiteit controleren van de informatie door de vreemdelingen geleverd op het moment dat het certificaat wordt vernieuwd, overeenkomstig deze CPS.

Wanneer de RA vaststelt of vermoedt dat geknoeid werd met een privé-sleutel, dan wordt dit onmiddellijk meegedeeld aan de CA.

Het RRN treedt op als enige RA in het domein van de CA, maar heeft niettemin het recht om de registratie te delegeren aan de LRA's, zoals de gemeentebesturen.

De RA is verantwoordelijk voor de directory's in zijn bezit, inclusief certificaatdirectory's. De RA is verantwoordelijk voor alle uitgevoerde controles, de resultaten van deze controles en hieruit voortvloeiende aanbevelingen.

De RA is via de LRA verantwoordelijk voor de juistheid van de vreemdelingengegevens en alle andere gegevens die aan de CA worden meegedeeld. De RA, niet de CA, is aansprakelijk voor schade die het gevolg is van niet gecontroleerde gegevens die opgenomen werden in een certificaat.

De RA handelt overeenkomstig de Belgische wetgeving en regelingen met betrekking tot de werking van de RRN.

De RA is aansprakelijk voor de eigen daden en verzuim, overeenkomstig de Belgische wetgeving.

9.4.8 Plichten van de kaartpersonalisator en -initialisator (CM)

De producent van de elektronische vreemdelingenkaarten (CM) is verantwoordelijk voor de initialisatie, personalisatie en de distributie van de vreemdelingenkaarten die de 2 certificaten bevat.

De initialisatie omvat de volgende verrichtingen in de chip:

- de generatie van de drie sleutelparen,
- het opnemen van de identificatiegegevens en van de certificaten,
- de authentificatie van de gegevens, alsook de initialisatie van de verschillende bestanden.

De CM zal op een veilig manier de basisdocumenten, de oproepingsbrieven, de nieuwe gepersonaliseerde en de geïnitialiseerde vreemdelingenkaarten verdelen, alsmede de gepersonaliseerde beveiligde brieven die bestemd zijn voor de vreemdelingen en die de PIN- en PUK1-codes bevatten.

Verwezenlijking van een beveiligd systeem voor de inzameling bij de gemeentebesturen van de vervallen of geannuleerde kaarten en voor de vernietiging ervan.

9.5 Afwijzing van de Garanties

In dit deel wordt ingegaan op de afwijzing van expresgaranties.

9.5.1 Uitsluiting van Bepaalde Schadeaspecten

Binnen de limieten van de Belgische wetgeving, kan de CSP in geen geval (behalve ingeval van fraude of een opzettelijk vergrijp) aansprakelijk gesteld worden voor:

- Winstderving;
- Verlies van gegevens;
- Indirecte of bestraffende schade die het gevolg is van of in verband staat met het gebruik, de levering, de licentie en de uitgifte of niet uitgifte van certificaten of digitale handtekeningen;
- Andere schade.

9.6 Duur en Beëindiging

Deze CPS blijft van kracht tot de CSP hier anders over beslist op de site http://repository.eid.belgium.be.

Bekendgemaakte wijzigingen worden aangegeven door een versienummer.

9.7 Individuele mededelingen en communicatie met deelnemers

Mededelingen in verband met deze CPS worden gericht aan : CSP voor de “Foreigner CA” p/a CERTIPOST, Muntcentrum, 1000 Brussel.

9.8 Afdwingbaarheid

Indien een bepaling van deze CPS ongeldig is of niet uitgevoerd kan worden, dan wordt de rest van de CPS op een dusdanige wijze geïnterpreteerd dat de oorspronkelijke intenties van de partijen verwezenlijkt worden.

9.9 Amendementen

Minder belangrijke aanpassingen aan deze CPS die geen materiële invloed hebben op het zekerheidsniveau van deze CPS, krijgen een versienummer met een decimale (vb. versie 1.0 wijzigt naar versie 1.1), terwijl belangrijke aanpassingen een versienummer krijgen met een geheel getal (vb. versie 1.0 wijzigt naar versie 1.1).

Minder belangrijke aanpassingen van de CPS hoeven niet veranderd te worden in de CPS OID of de CPS-index (URL) die door de CSP meegedeeld kan worden. Voor belangrijke aanpassingen die de aanvaardbaarheid van certificaten voor welbepaalde doeleinden materieel kunnen veranderen, moeten de CPS OID of CPS-index (URL) mogelijk aangepast worden.

9.10 Procedures voor het Oplossen van Geschillen

Alle geschillen in verband met deze CPS worden betwist overeenkomstig de Belgische Wetgeving.

9.11 Toepasselijk Recht

De CSP levert zijn diensten overeenkomstig de bepalingen van de Belgische Wetgeving.

9.12 Diverse bepalingen

De CSP neemt bij wijze van referentie de volgende informatie op in elk digitaal certificaat dat uitgegeven wordt:

- Voorwaarden beschreven in deze CPS.;
- Elk ander toepasselijk certificaatbeleid, zoals vermeld op een uitgegeven certificaat;
- De verplichte elementen van de toepasselijke standaarden;
- Alle niet verplichte maar gebruikelijke elementen van de toepasselijke standaarden
- De inhoud van de extensies en uitgebreide benaming die nergens anders vermeld wordt;
- Elke andere informatie die thuishoort in een veld van een certificaat.

Om informatie bij wijze van referentie op te nemen, gebruikt de CA computer- en tekstgebaseerde indexen, waaronder URL's en OID's.

10 Lijst met Definities

Accreditatie	Een formele verklaring van een goedkeurende autoriteit dat een bepaalde functie/entiteit aan specifieke formele vereisten tegemoetkomt.
Authority Information Access (AIA)	Is een informatieveld dat als extensie in het certificaat werd opgenomen om automatisch het pad op te bouwen ter verificatie van de vertrouwenshiërarchie binnen de meest algemeen gebruikte toepassingen, zoals browsers.
Archief	Om documenten te bewaren voor doeleinden zoals veiligheid, back-up of audit.
Audit	Procedure gebruikt om na te gaan of de formele criteria of controles nageleefd worden.
Authentificatie	Een proces waarbij de identiteit van een persoon bevestigd wordt of waarbij de integriteit van een specifieke informatie aangetoond wordt, door deze in de juiste context te plaatsen en het verband te onderzoeken.
Betrouwbaar Systeem	Computerhardware, software en procedures die een aanvaardbaar niveau van veiligheid, beschikbaarheid, betrouwbaarheid en correcte werking bieden en het veiligheidsbeleid kracht bijzetten.
Betrouwbare Positie	Een rol binnen een CA met toegang tot of controle over de cryptografische handelingen die een bevoorrechte toegang bieden tot de publicatie, het gebruik, de schorsing of intrekking van certificaten, inclusief de handelingen die de toegang tot een bron beperken.
Opvraagcentrum	Een databank en/of directory (bestandenlijst) met digitale certificaten en andere betrokken informatie die online toegankelijk is.

Certificaat	Een elektronische bevestiging die de gegevens voor het verifiëren van de handtekening koppelt aan een natuurlijke persoon of een rechtspersoon en de identiteit van die persoon bevestigt.
Certificaatbeheer	Acties die verband houden met het beheer van certificaten, zoals de opslag, de verspreiding, de publicatie, de intrekking en de schorsing.
Certificaatextensie	Een veld van het digitaal certificaat dat gebruikt wordt om bijkomende informatie in te voeren over kwesties zoals: de openbare sleutel, de gecertificeerde persoon, de gecertificeerde uitgever en/of het gecertificeerd proces.
Certificaathiërarchie	Een op niveaus gebaseerde opvolging van certificaten van een (root) CA en ondergeschikte entiteiten waaronder de Certificatieautoriteiten en de vreemdelingen.
Certificate Policy Of CP	Een bepaald geheel van regels die de toepasbaarheid aangeven van een Certificaat op een specifieke gemeenschap en/of een toepasbaarheidsklasse met gemeenschappelijke vereisten inzake veiligheid.
Certificatieautoriteit Of CA	Een entiteit die een openbare sleutel verenigt met de informatie over het subject, bevat in het certificaat, door dit certificaat met een privésleutel te ondertekenen. Tenzij uitdrukkelijk vermeld, is de hierin beschreven CA de Foreigner Certificatieautoriteit.
Certificatiediensten	Diensten verbonden met de levenscyclus van het Certificaat. Certificatiediensten zijn openbare diensten.
Certificatieketen	Een hiërarchische certificatielijst die een eindgebruikercertificaat en CA-certificaten bevat.
Cryptografie Openbare Sleutel	Cryptografie die gebruik maakt van een sleutelpaar van mathematisch gerelateerde cryptografische sleutels.
DIENST Certificaatstatus	Dienst die het de vertrouwende partijen en anderen mogelijk maakt om de status van certificaten te controleren.
Digitale handtekening	Dient voor het coderen van een bericht aan de hand van een asymmetrisch systeem van cryptografie en een analysefunctie, zodat de persoon die in het bezit is van het oorspronkelijk bericht en de openbare sleutel van de ondertekenaar nauwkeurig kan bepalen of de transformatie gecreëerd werd met de privé-sleutel die overeenkomt met de openbare sleutel van de ondertekenaar, en of het oorspronkelijk bericht sinds de verzending wijzigingen heeft ondergaan.
eID	Het compleet systeem van de elektronische identiteitskaart, inclusief de organisatie, de infrastructuur, de procedures, de contacten en alle nodige middelen die verband houden met de identiteitskaarten.
Elektronische handtekening	Gegevens in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens die als authentificatiemiddel gebruikt worden.
Europese Richtlijn	De Europese richtlijn 1999/93 van het Europees Parlement en de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen.
Gedeeld Geheim	Een deel van een cryptografisch geheim dat werd verdeeld onder een aantal fysieke kentekens, zoals smart cards enz.
Gekwalificeerd Certificaat	Een Certificaat dat uitsluitend gebruikt wordt ter ondersteuning van elektronische handtekeningen en voldoet aan de vereisten van Bijlage I van de Europese Richtlijn 1999/93 en afgeleverd door een Certificatiedienstverlener die voldoet aan Bijlage II van de Europese Richtlijn 1999/93, met verwijzing naar de Belgische wet van 09 juli 2001, de technische standaard ETS TS 101 456, de technische standaard ETSI TS 101 862 “Profiel Gekwalificeerd Certificaat” en de RFC 3039 “Internet X.509 Openbare Sleutelinfrastructuur Profiel Gekwalificeerd Certificaat”
Genereren Van Een Dubbele Sleutel	Een vertrouwensproces om wiskundig verbonden (vb. volgens het algoritme van de RSA) openbare en privé-sleutels te creëren.

Genormaliseerd Certificaat	Een certificaat dat gebruikt wordt ter ondersteuning van elk gebruik verschillend van de handtekeningcertificaat van een cryptografisch dubbele sleutel waarvan de overeenkomstige openbare sleutel gecertificeerd werd. De gecertificeerde sleutel kan op de volgende manieren gebruikt worden: codering, authentificatie, handtekeningen die niet automatisch dezelfde waarde hebben als een handgeschreven handtekening, enz. Een Genormaliseerd Certificaat wordt uitgegeven volgens de vereisten van de technische standaard ETSI TS 102 042.
Geschorst Certificaat	Een tijdelijk uitgesloten certificaat, dat niettemin gedurende een week stand-by wordt gehouden tot de RRN de definitieve intrekking of de reactivering van het certificaat bekendmaakt aan de CA.
Handtekening	Een methode die gebruikt of aangenomen wordt door een documentopsteller om zichzelf te identificeren, die aanvaard wordt door de bestemmeling of gebruikelijk is in bepaalde omstandigheden.
Houder Van Een Gedeeld Geheim	Een persoon die in het bezit is van een gedeeld geheim.
Hsm	Een HSM (Hardware Security Module) is een Hardware gebaseerd security device dat cryptografische sleutels genereert, opslaat en beveiligt.
Intekenaar	De persoon wiens identiteit en openbare sleutel gecertificeerd werden in een certificaat.
Intrekken Van Een Certificaat	Om de operationele periode van een certificaat permanent te beëindigen vanaf een gespecificeerd tijdstip in de toekomst.
Intrekking Certificaat	Een dienst on line gebruikt om een digitaal certificaat definitief uit te schakelen vóór de vervaldatum.
Kenmerkende Naam	Een reeks van gegevens ter identificatie van een reële entiteit, zoals een persoon in een context op computerbasis
Lijst Intrekking Certificaten (CRL)	Een lijst die uitgegeven wordt en digitaal ondertekend wordt door een CA en ingetrokken en geschorste certificaten bevat. Deze lijst kan door de vertrouwende partijen op elk moment geraadpleegd worden, vooraleer vertrouwen te stellen in de informatie die in een certificaat vermeld wordt.
Lokale Registratieautoriteit of LRA:	Een LRA is een entiteit (organisatie) die optreedt bij machtiging van een RA en de aanvragen tot digitale certificaten registreert. Een LRA registreert andere entiteiten en kent hen een relatieve onderscheiden waarde toe, zoals een unieke naam of een analysefunctie die uniek is in dat domein.
Mededeling	Het resultaat van een bekendmaking aan de partijen waarop de CAdiensten betrekking hebben, overeenkomstig deze CPS.
Objectidentificator (OID)	Een reeks van integere componenten die toegewezen kunnen worden aan een geregistreerd object en de eigenschap heeft uniek te zijn onder alle objectidentificators binnen een welbepaald domein.
Ondertekenaar	Een persoon die controle heeft over de inrichting voor het aanmaken van handtekeningen, gebruikt voor de generatie van digitale handtekeningen.
Online Certificaat Statusprotocol (OCSP)	Het Online Certificaat StatusProtocol (RFC 2560) is een real-time statusinformatiebron die gebruikt wordt om de huidige status te bepalen van een digitaal certificaat, zonder een beroep te doen op CRL's.
Openbare Certificaatdiensten CA	Een digitaal certificatiesysteem beschikbaar gesteld door de CA en de entiteiten die behoren tot het domein van de CA, zoals beschreven in deze CPS.
Openbare Sleutel	Een wiskundige sleutel die openbaar beschikbaar kan gesteld worden en die gebruikt wordt om de handtekeningen gecreëerd met de overeenkomstige privé-sleutel te controleren. Afhankelijk van het algoritme, kunnen openbare sleutels ook gebruikt worden om berichten of bestanden te coderen, die vervolgens ontcijferd kunnen worden met behulp van de overeenkomstige privé-sleutel.
Openbare Sleutelinfrastructuur (OSI)	De architectuur, de organisatie, de technieken, de praktijken en procedures voor de collectieve invoering en werking van een certificaatgebaseerde systeem voor de codering van openbare sleutels.

Opnemen Per Referentie	Een document opnemen in een ander document, door het op te nemen document te identificeren aan de hand van informatie die de bestemmeling toegang biedt tot heel het opgenomen document en waarbij duidelijk gemaakt wordt dat het deel uitmaakt van een ander document. Een dergelijk opgenomen document heeft hetzelfde effect als het zou hebben indien het volledig in het bericht vermeld werd.
PKI - Hiërarchie	Een reeks van Certificatieautoriteiten waarvan de functies georganiseerd zijn volgens het principe van de delegatie van autoriteit en onderling verbonden zijn als ondergeschikte en hogere CA.
Privé-Sleutel	Een wiskundige sleutel om digitale handtekeningen te creëren en soms (afhankelijk van het algoritme) berichten te ontcijferen in combinatie met de overeenkomstige openbare sleutel.
Publicatie Certificaat	Uitgifte van X.509 v3 digitale certificaten betreffende de identificatie en digitale handtekeningen gebaseerd op persoonlijke gegevens en de openbare sleutels geleverd door de RA, overeenkomstig de CPS
Registratieautoriteit of RA	Een entiteit die verantwoordelijk is voor de identificatie en authentificatie van vreemdelingen. De RA geeft geen certificaten uit. Binnen het domein van de CA, is de RRN de RA.
Root Signing	Een handeling waarbij een hiërarchisch hogere autoriteit vertrouwen stelt in een hiërarchisch lagere autoriteit. In het kader van de Belgische elektronische vreemdelingenkaart, is Digicert cybertrust global een root sign autoriteit waarbij de CA kan profiteren van dezelfde vertrouwenspositie voor softwaretoepassingen als de certificaten van Digicert cybertrust global.
Schorsing Certificaat	Een digitaal certificaat tijdelijk uit te schakelen en het automatisch in te trekken indien binnen een bepaalde termijn geen aanvraag ingediend wordt om het certificaat te herstellen.
Serienummer Certificaat	Een volgnummer dat op unieke wijze een certificaat identificeert in het domein van een CA.
Sleutelpaar	Een privé-sleutel en de overeenkomstige openbare sleutel, in een asymmetrische codering.
Statusverificatie	Een online dienst gebaseerd op vb. de Online Certificate Status Protocol (RFC 2560) die gebruikt wordt om de huidige status van een digitaal certificaat zonder CRL's te bepalen. Binnen de eID infrastructuur zijn verschillende mechanismen beschikbaar om deze status na te gaan, inclusief CRL's, Delta CRL's, OCSP en webinterfaces.
Uitgever Van Een Gedeeld Geheim	Een persoon die een gedeeld geheim, zoals een CA, creëert en verspreidt.
Validatie Certificaatketen	Het valideren van het certificaat van de eindgebruiker en van ieder cerificaat hoger in de vertrouwensketen.
Verklaring Certificatiepraktijk of CPS	Een verklaring van de praktijken voor het beheer van de certificaten gedurende hun hele levensduur.
Vertrouwelijkheid	De voorwaarde om gegevens openbaar te maken aan uitsluitend geselecteerde en geautoriseerde partijen.
Vertrouwende Partij	Elke entiteit die zich verlaat op een certificaat, voor de uitoefening van enige actie.
Vervaldatum Certificaat	Het einde van de geldigheid van een digitaal certificaat.
X.509	De standaard van de ITU-T (International Telecommunications UnionT) voor digitale certificaten.

11 Lijst met acroniemen

BRCA: Belgium Root CA
CA: Certification Authority
CM: Card Manufacturer
CP : Certificate Policy
CPS: Certificate Practise Statement
CRL: Certificate Revocation List
HSM: Hardware Security Module

LRA: Local Registration Authority
OID: Object Identifier
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RA: Registration Authority
SRA: Suspension and Revocation Authority
OID: Object Identifier
URL: Uniform Resource Locator
PIN: Personal Identification Number
PUK: Personal Unblocking Key
Belgische Root-CA
Certificatieautoriteit
Kaartproducent
Certificate Policy
Verklaring Certificatiepraktijk
Lijst Intrekking Certificaten
Hardware Module voor secure handtekening generatie Lokale Registratieautorit eit
Objectidentificator
Online Certificaat Statusprotocol
Openbare Sleutelinfrastructuur
Registratieautoriteit
Autoriteit voor de Schorsing en de Herroeping
Object identificator
Uniforme bron zoeker
Persoonlijk identificatie nummer
Persoonlijke deblokkeringssleutel