Belgisch Certificaatbeleid & Verklaring met betrekking tot de Praktijk voor eID PKI-infrastructuur Citizen CA

OIDs: **2.16.56.1.1.1.2**
2.16.56.9.1.1.2
2.16.56.10.1.1.2
2.16.56.12.1.1.2

Bedrijf:	*Certipost*
Versie:	*4.4*
Status:	*Definitief*
Rel. Date:	*16/05/2019*

Documentcontrole

Datum	Versie	Opsteller	Wijziging
13/2/2017	3.0	Bart Eeman	Oorspronkelijke versie 1.0
15/3/2017	3.1	Bart Eeman	Oorspronkelijke versie 1.1
24/3/2017	3.2	Don Giot	Bijgewerkte versie 1.2
10/4/2017	3.3	Bart Eeman	Toevoeging Zetes
13/4/2017	3.4	Bart Eeman	Opmerkingen RRN
4/9/2017	4.0	Don Giot / Cristof Fleurus	eIDAS Bijwerking en QA
29/5/2018	4.1	Bart Eeman / Don Giot	Bijgewerkte versie 4.1 & QA
13/7/2018	4.2	Bart Eeman	Revisie definitieve versie 2018
8/4/2019	4.4	Bart Eeman/Bono Vanderpoorten/Guillaume Nguyen	Update 2019

Disclaimer

Deze disclaimer is van toepassing op de “Certification Practice Statement” en de “PKI Disclosure Statement”. Dit document is een vertaling naar het Nederlands van het originele, Engelstalige document gepubliceerd op https://repository.eid.belgium.be/. Dit Nederlandstalige document dient als een informatieve bron. De Engelstalige versie van het CPS-document is de enige officiële versie van de CPS en is het enige document dat juridisch bindende verplichtingen kan creëren. In het geval dit Nederlandstalig document afwijkt van de Engelstalige CPS, in het geval van twijfel, of in het geval dit document een oudere versie van de gepubliceerde Engelstalige CPS bevat, zal steeds de laatst gepubliceerde versie van het Engelstalige CPS voorrang hebben.

Inhoudstafel

1 Inleiding

Deze Verklaring met betrekking tot de Certificatiepraktijk (hierna afgekort als "CPS" - Certification Practice Statement) omschrijft de certificatiepraktijken die van toepassing zijn op de digitale certificaten die voor de Belgische Burgers uitgegeven worden door de Certificatiedienstverlener (hierna afgekort als TSP - Trust Service Provider) onder de naam "Citizen CA" (hierna "de CA's" genoemd) en die geïnstalleerd zijn op de elektronische chipkaarten voor burgers (hierna “elektronische identiteitskaarten” genoemd).

Deze CPS is een unilaterale verklaring voor het algemene publiek over de praktijken waaraan de "Citizen CA" voldoet wanneer het certificeringsdiensten verleent en beschrijft uitvoerig hoe de "Citizen CA" zijn diensten beschikbaar maakt.

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 “Citizen CA”.

Certipost nv voegt zich naar de huidige versie van de "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (“Baseline Requirements”) die werden gepubliceerd op http://www.cabforum.org. In geval van tegenstrijdigheid tussen dit document en die "Requirements", zullen die "Requirements" de overhand hebben.

1.1 Overzicht

Op dit ogenblik is de TSP voor "Citizen CA" “CERTIPOST nv” (hierna “Certipost” genoemd), met maatschappelijke zetel te 1000 Brussel, Muntcentrum; deze taak werd haar opgedragen door de Belgische Federale Overheid in haar hoedanigheid van aanbestedende overheidsdienst voor het eID-project, waarvoor de volgende voorwaarden gelden:

CERTIPOST treedt op als verlener van vertrouwensdiensten (“TSP”) in de zin van de Wet van 21 juli 2016, de Europese verordening nr. 910/2014 van het Europees Parlement en van de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. CERTIPOST vervult in naam en voor rekening van de Belgische Federale Overheid zowel de rol van CA als van TSP voor de “Citizen CA's” en is in die hoedanigheid verantwoordelijk voor de Burgercertificaten die worden uitgegeven onder deze CA’s.

Deze CPS kan enkel gebruikt worden binnen het bevoegdheidsgebied verleend door de CA. De CPS heeft als doel het bevoegdheidsgebied af te bakenen waarbinnen certificeringdiensten verleend worden aan de burgers en aan vertrouwende partijen binnen het bevoegdheidsgebied van de CA. Verder schetst deze CPS ook de relatie tussen de Certificatieautoriteit (CA) en andere Certificatieautoriteiten binnen de PKI-hiërarchie van de Belgische Federale Overheid, zoals de Belgische Root Certificate Authority (BRCA). De verklaring beschrijft ook de relatie tussen de TSP en de andere instellingen die betrokken zijn bij de levering van de certificaten voor de Elektronische Identiteitskaarten in België (hierna “Burgercertificaten”).

Deze CPS voorziet in operationele richtlijnen voor alle burgers en vertrouwende partijen, inclusief natuurlijke personen of rechtspersonen in België of in het buitenland. Deze CPS voorziet eveneens in operationele richtlijnen voor andere Certificatie-autoriteiten, zoals de BRCA, die behoren tot de PKI-hiërarchie van de Belgische Federale Overheid binnen het rechtskader voor elektronische handtekeningen en elektronische identiteitskaarten in België. Bovendien beschrijft deze CPS de relaties tussen de “Citizen CA” en alle andere entiteiten die een rol spelen in de context van de Elektronische Identiteitskaart van de Belgische burgers, zoals de Kaartproducent. De Belgische Federale Overheid verwerft deze diensten door middel van passende overeenkomsten met deze derden-leveranciers.

Tot slot voorziet deze CPS informatie inzake accreditatie en toezicht voor controleautoriteiten, accreditatieorganen, auditeurs enz. met betrekking tot de activiteiten van de TSP.

Deze “Citizen CA CPS” onderschrijft de volgende standaarden en brengt ze tot uitvoering:

- ETSI EN 319 411-1: Beleids- en veiligheidsvereisten voor Trust Service Providers die certificaten uitgeven, Deel 1: Algemene vereisten
- ETSI EN 319 411-2: Beleids- en veiligheidsvereisten voor Trust Service Providers die certificaten uitgeven, Deel 2: Vereisten voor Trust Service Providers die EU-gekwalificeerde certificaten uitgeven
- ETSI EN 319 412-5: Beleids- en veiligheidsvereisten voor Trust Service Providers die certificaten uitgeven, Deel 5: QCStatements.
- RFC 3647: Internet X.509 Openbare Sleutelinfrastructuur – Certificaatpolicy’s en Certificatiepraktijken
- RFC 5280: Internet X.509 Openbare Sleutelinfrastructuur – Certificaat- en CRL-Profiel.
- RFC 6818: Update van de RFC 5280.
- RFC 3739: Internet X.509 Openbare Sleutelinfrastructuur – Gekwalificeerd Certificatenprofiel.
- RFC 6960: X.509 Internet Openbare Sleutelinfrastructuur – Online Certificate Status Protocol - OCSP
- De ISO-IEC 270001 informatieveiligheids- en infrastructuurnorm.

De CPS behandelt in detail de organisatorische, procedurele en technische policy’s en praktijken van de CA met betrekking tot alle certificatiediensten die ze verleent en gedurende de volledige levensduur van door de “Citizen CA” uitgegeven certificaten. Naast deze CPS is het mogelijk dat ook andere documenten met betrekking tot het certificeringproces in de context van de Belgische Elektronische Identiteitskaart in acht genomen moeten worden. Deze documenten zullen beschikbaar zijn in het repertorium van de CA (cf. § 1 **Fout! Ongeldige bladwijzerverwijzing.**).

Deze CPS voldoet inzake vorm en inhoud aan de formele vereisten van de Internet Engineering Task Force (IETF) RFC 3647. Hoewel sommige hoofdstuktitels zijn opgenomen volgens de structuur van RFC 3647, is het onderwerp niet noodzakelijkerwijze van toepassing voor de uitvoering van de certificeringdiensten van de “Citizen CA”. Deze hoofdstukken krijgen de benaming "Hoofdstuk niet van toepassing". In deze CPS werden kleine redactionele

veranderingen van RFC 3647-voorschriften aangebracht, om de structuur van RFC 3647 beter af te stemmen op dit toepassingsgebied.

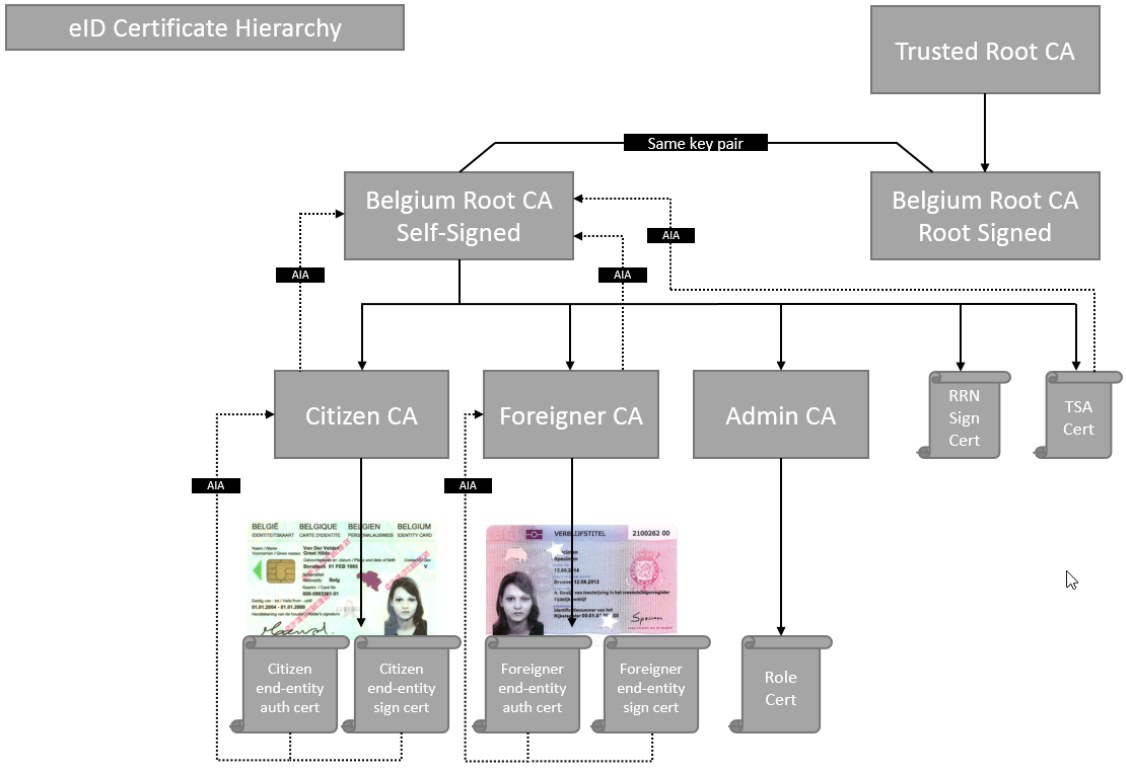
Deze CPS dient eveneens te worden beschouwd als de Certificaatpolicy (CP) voor de door de "Citizen CA" uitgegeven certificaten.

Wat betreft de andere CA's waarop de Belgische Federale Overheid een beroep doet, verwijzen we naar de volgende website met daarop een link naar elke CPS:

- Citizen CA https://repository.eid.belgium.be
- Foreigner CA https://repository.eid.belgium.be
- Belgium Root CA https://repository.eid.belgium.be

Opmerking: Elke CA heeft zijn eigen CP/CPS.

1.2 De eID Hiërarchie



Afbeelding: PKI-hiërarchie Belgische eID

1.3 Documentnaam en Identificatie

Naam van dit document	*Belgische Certificaatpolicy & Verklaring met betrekking tot de Praktijk voor eID PKI-infrastructuur voor "Citizen CA"*
Documentversie	***2.16.56.12.1* – v4.04** *Dit Certificatiebeleid wordt geïdentificeerd aan de hand van de naam en het versienummer.*
	Dit OID-document vervangt de volgende OID's: ***2.16.56.1.1*** ***2.16.56.9.1*** ***2.16.56.10.1*** *Vanaf de datum van de publicatie ervan vervangt deze Citizen CP/CPS alle andere "Citizen CP/CPS"-versies.*
OID die naar dit document verwijst	*De identificatiemiddelen onder controle van Certipost:* ***BRCA (1)*** *OID: 2.16.56.1.1.1.2 – Citizen CA* *OID: 2.16.56.1.1.1.2.1 – Handtekeningcertificaat voor Burgers* *OID: 2.16.56.1.1.1.2.2 – Authenticatiecertificaat voor Burgers*
	BRCA 2 *OID: 2.16.56.9.1.1.2 – Citizen CA* *OID: 2.16.56.9.1.1.2.1 – Handtekeningcertificaat voor Burgers* *OID: 2.16.56.9.1.1.2.2 – Authenticatiecertificaat voor Burgers*
	BRCA 3 *OID: 2.16.56.10.1.1.2 – Citizen CA* *OID: 2.16.56.10.1.1.2.1 – Handtekeningcertificaat voor Burgers* *OID: 2.16.56.10.1.1.2.2 – Authenticatiecertificaat voor Burgers*
	BRCA 4 *OID: 2.16.56.12.1.1.2 – Citizen CA* *OID: 2.16.56.12.1.1.2.1 – Handtekeningcertificaat voor Burgers* *OID: 2.16.56.12.1.1.2.2 – Authenticatiecertificaat voor Burgers*

1.4 Deelnemers PKI

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

1.4.1 Certificatieautoriteiten

Een Certificatieautoriteit is een instelling die digitale certificaten die overeenkomen met digitale identiteit uitgeeft en beheert.

De Certificatieautoriteit verleent de diensten die nodig zijn om de geldigheid van de uitgegeven certificaten te controleren.

CERTIPOST vervult in naam en voor rekening van de Belgische Federale Overheid zowel de rol van CA als van TSP voor de Citizen CA's en is in die hoedanigheid verantwoordelijk voor de burgercertificaten die worden uitgegeven onder de Citizen CA. De Belgische Federale Overheid is de TSP die verantwoordelijk is voor de Belgische Root CA's en voor de CA-certificaten uitgegeven onder de Belgische Root CA.

De "Citizen CA" is een Certificatieautoriteit die gemachtigd is om Burgercertificaten uit te geven. Deze machtiging werd verleend door de BRCA.

De "Citizen CA" waarborgt de beschikbaarheid van alle diensten in verband met de certificaten, inclusief de uitgifte, de herroeping, de statusverificatie, naargelang ze beschikbaar of vereist zijn bij specifieke toepassingen.

De "Citizen CA" is gevestigd in België. Er kan contact mee worden opgenomen op het adres dat verderop in deze CPS zal worden vermeld. De "Citizen CA" werkt vanuit een veilige locatie en heeft een noodvoorzieningslocatie in België om de CA-diensten te leveren. Onder deze diensten vallen de uitgifte, de schorsing, de herroeping, de vernieuwing en de statusverificatie van certificaten.

Het verantwoordelijkheidsdomein van de "Citizen CA" omvat het algemeen beheer van de levenscyclus van de certificaten, waaronder:

- Uitgave;
- Schorsing / Opheffen van schorsing;
- Herroeping;
- Statusverificatie (Dienst voor Certificaatstatus);
- Documentenopslagplaats.

1.4.2 Registratie-Autoriteiten

Het Rijksregister (RR) is samen met de gemeenten de RA binnen het domein van de “Citizen CA”, met uitsluiting van enige andere. Het RR werd opgericht volgens en handelt krachtens de bepalingen van de Wet op het Rijksregister en de Wet op de Identiteitskaarten.

De Registratieautoriteit (“RA”) die, in naam van de TSP, verklaart dat een bepaalde openbare sleutel tot een bepaalde entiteit (d.i. een natuurlijke persoon) behoort door een digitaal certificaat uit te geven en dit certificaat met zijn privésleutel te ondertekenen. Voor de Belgische Elektronische Identiteitskaart vervult het "Rijksregister", een openbaar bestuurslichaam dat tot de Federale Overheidsdienst Binnenlandse Zaken behoort, de rol van “RA”. Het merendeel van de huidige registratieverrichtingen wordt uitgevoerd door de plaatselijke administratieve diensten in de gemeenten, de zogenaamde Lokale Registratie-Autoriteiten ("LRA"). Op basis van dit proces vraagt de RA de uitgifte van een certificaat aan bij de CA.

De RA en de LRA zijn in het bijzonder verantwoordelijk voor:

i. de geldigheidsverklaring van de identiteit van de burgers;

ii. de registratie van de gegevens die gecertificeerd moeten worden;

iii. de machtiging tot uitgifte van een certificaat voor een bepaalde burger;

iv. de waarborg dat de certificaten van de burger op de juiste identiteitskaart worden opgeslagen;

v. de waarborg dat de burger de juiste kaart ontvangt en dat de kaart in kwestie enkel geactiveerd wordt wanneer ze naar behoren toegekend wordt aan de juiste burger;

vi. de SRA (Autoriteit voor de Schorsing en de Herroeping): de entiteit die de certificaten schorst en/of herroept overeenkomstig de opgegeven ETSI-standaarden.

1.4.3 Inschrijver & Abonnee

Certipost, dat de rol van TSP vervult voor de "Citizen CA's", heeft een contractuele overeenkomst met de Belgische Federale Overheid. Als dusdanig kunnen we de Overheid beschouwen als de "inschrijver" op de CA-diensten binnen het domein van de "Citizen CA".

De abonnees van de CA-diensten binnen het domein van de “Citizen CA” zijn burgers die in het bezit zijn van een Elektronische Identiteitskaart met geactiveerde certificaten, in overeenstemming met de Wet op Identiteitskaarten. In de rest van dit document kan de term abonnee vervangen worden door de term “burger”. Deze burgers:

- worden geïdentificeerd in beide Burgercertificaten;
- zijn in het bezit van de privésleutels die overeenkomen met de openbare sleutels die in hun respectieve Burgercertificaten opgenomen zijn.

De burgers zijn gerechtigd aan het begin van de procedure voor de aanvraag van een Elektronische Identiteitskaart aan te geven of ze Certificaten willen. Wanneer de Elektronische Identiteitskaart aan de burger geleverd wordt, zijn de Burgercertificaten erin geladen. Voor burgers die de Burgercertificaten niet willen hebben, kunnen er op de eID-kaart

geen of één certificaat aanwezig zijn. We verwijzen naar het document **EID-DEL-004 EID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)** voor bijkomende informatie.

Voor burgers jonger dan zes jaar wordt het authenticatiecertificaat niet op de kaart geplaatst. Voor burgers jonger dan achttien jaar wordt het certificaat voor elektronische handtekening niet op de kaart geplaatst.

	Authenticatiecertificaat	Certificaat voor Elektronische Handtekening
0 – 6 jaar	0	0
6 – 18 jaar	X	0
+18 jaar	X	X

In de tabel hierboven staat voor elke leeftijdscategorie aangegeven op welke certificaten ze recht hebben.

1.4.4 Vertrouwende Partijen

Vertrouwende partijen zijn entiteiten, inclusief natuurlijke personen of rechtspersonen, die 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 burger, vertrouwen.

1.4.5 Andere Deelnemers

1.4.5.1 Kaartproducent

De Kaartproducent voor "**Error! Unknown document property name.**" is "Zetes nv/sa", met maatschappelijke zetel in 1130 Brussel, Straatsburgstraat 3. Deze taak werd haar opgedragen door de Belgische Overheid in haar hoedanigheid van aanbestedende overheidsdienst voor het eID-project.

De Kaartproducent past niet-gepersonaliseerde smartcards aan gepersonaliseerde Elektronische Identiteitskaarten aan door de identiteitsgegevens van de burger samen met een foto op de kaart te drukken.

De Kaartproducent voorziet ook de volgende diensten:

- Het aanmaken van de benodigde sleutelparen in de kaart;
- Het opslaan van beide eID-Burgercertificaten op de kaart;
- Het aanmaken van de persoonlijke activeringscodes van de aanvrager en de gemeente, alsook de initiële pincode van de aanvrager;
- Het laden van de actieve Rootcertificaten van de overheid op de kaart;
- Het leveren van de Elektronische Identiteitskaart aan de gemeente;

- Het bezorgen van de persoonlijke activeringscode en de pincode aan de aanvrager;
- Het opnemen van de gegevens in het Register van Identiteitskaarten.

1.4.5.2 Leverancier van de Root Sign

De leverancier van de root sign waarborgt het vertrouwen in de BRCA bij algemeen gebruikte browsers en toepassingen. De leverancier van de root sign waarborgt dat dergelijke browsers en toepassingen zijn "Root Certificatie-Autoriteit" blijven vertrouwen en hij brengt de RA op de hoogte van voorvallen die het vertrouwen in zijn eigen "Root Certificatie-Autoriteit" beïnvloeden. De leverancier van de root sign van alle actieve BRCA's is Digicert. De Certificatiepolicy en de Certificatieprofielen van Digicert zijn terug te vinden op: https://www.digicert.com/ssl-cps-repository.htm

1.4.5.3 Onderaannemer

Certipost doet een beroep op een onderaannemer die de TSP ondersteunt wat betreft operationele taken en verantwoordelijkheden. De onderaannemer biedt technische ondersteuning voor de volgende diensten:

- Uitgave van Certificaten
- Herroeping en Schorsing van Certificaten
- Validering van Certificaten
    - OCSP
    - CRL en Delta CRL

Er bestaat een SLA (service level agreement) tussen de overheid, Certipost en de onderaannemer waarin de kwaliteit van deze geleverde diensten op het vlak van performantie en beschikbaarheid is vastgelegd. De onderaannemer brengt maandelijks verslag uit van zijn gemeten performantie-indicatoren om zo te bewijzen dat hij de SLA naleeft. De onderaannemer biedt ook organisatorische ondersteuning tijdens "sleutelceremonies".

1.5 Het gebruik van Certificaten

Het gebruik van de certificaten op de Elektronische Identiteitskaart is aan bepaalde beperkingen onderhevig.

De "Citizen CA" geeft twee types elektronische certificaten uit, waarbij elk een specifiek gebruik kent:

- Authenticatiecertificaat: Dit certificaat wordt gebruikt voor elektronische

  authenticatietransacties die de toegang tot websites en andere online content ondersteunen.

- Gekwalificeerd elektronisch handtekeningcertificaat: Dit certificaat wordt gebruikt om gekwalificeerde elektronische handtekeningen aan te maken.

Elke aan een burger bezorgde eID kan zowel een authenticatiecertificaat als een gekwalificeerd handtekeningcertificaat bevatten, aangezien de meest geavanceerde veiligheidsvereisten voorschrijven om authenticatiecertificaten niet te gebruiken voor elektronische handtekening-doeleinden. De “Citizen CA” wijst daarom alle aansprakelijkheid ten aanzien van vertrouwende partijen af in alle gevallen waarin het authenticatiecertificaat werd gebruikt voor het aanmaken van elektronische handtekeningen.

1.6 Administratief beheer

1.6.1 Organisatie die het Document beheert

Het administratief beheer valt onder CERTIPOST dat bereikbaar is via:

- de post:

  Certipost nv
  Administratief Beheer – Citizen CA
  Muntcentrum
  1000 Brussel

- e-mail:

  Aan: eid.cps@bpost.be
  Onderwerp: Administratief Beheer – Citizen CA

1.6.2 Contactpersoon

Voor de voornaamste contactpersoon in geval van vragen of voorstellen met betrekking tot de Citizen CA CP/CPS, zie § 1.6.1 ORGANISATIE DIE HET DOCUMENT beheert

Alle feedback, positieve zowel als negatieve, is welkom. Om te garanderen dat deze feedback passend en tijdig wordt behandeld, dient hij naar het hierboven vermelde e-mailadres te worden verzonden.

1.6.3 Persoon die de CPS-Geschiktheid voor het beleid bepaalt

In overeenstemming met de standaard ETSI 319 411-2 ter ondersteuning van de Europese Richtlijn (Richtlijn 910/2014), beheert Certipost zijn TSP-taken via een PKI Management

Board (CEPRAC) die over alle nodige deskundigheid beschikt.

Door officieel deel te nemen aan de regelmatig gehouden eID voortgangsvergaderingen, waarop alle bovengenoemde partijen vertegenwoordigd zijn, verzamelt CERTIPOST alle nodige informatie en stelt ze deze partijen alle relevante vragen om zijn verantwoordelijkheid als TSP 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 voortgangsvergadering.

De PKI Management Board zal aan de eID-stuurgroep die door de Belgische Federale Overheid wordt geleid, elke kwestie doorgeven die niet opgelost kon worden door middel van dit proces. Deze stuurgroep kan een beroep doen op externe deskundigen om bijkomend advies in te winnen en heeft de verantwoordelijkheid geschillen te beslechten.

1.7 Definities en Acroniemen

1.7.1 Definities

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

1.7.2 Acroniemen

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

2 Verantwoordelijkheid inzake Publicatie en Bewaring

2.1 Repertoria

De “Citizen CA” houdt een up-to-date online repertorium bij met documenten waarin ze bepaalde bekendmakingen doet omtrent haar praktijken, procedures en de inhoud van sommige van haar beleidsdocumenten met inbegrip van haar CPS. Dit repertorium is terug te vinden onder http://repository.eid.belgium.be. De CA behoudt zich het recht voor informatie beschikbaar te stellen en te publiceren in verband met de beleidsvormen en dit

op eender welke manier die de CA gepast acht.

Het Repertorium is beschikbaar op de volgende website: https://repository.eid.belgium.be.

2.2 Publicatie van Certificatie-informatie

De CA publiceert een repertorium met alle uitgegeven Digitale Certificaten en alle Digitale Certificaten die werden herroepen. De locatie van het repertorium en de Online Certificaat

Statusprotocol-responders (hierna “OCSP-responders” genoemd) worden opgegeven in de individuele Certificaatprofielen, waarover meer informatie in **EID-DEL-004 eID PKI-Hiërarchie Certificaatprofiel (cf. Appendix C).** 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 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 TSP verplichtingen heeft.

De “Citizen CA” publiceert informatie over de certificaten in een of meerdere voor het publiek toegankelijke online repertoria onder het internetdomein “eid.belgium.be”. De CA behoudt zich het recht voor om informatie over de status van de certificaten te publiceren

in repertoria van derde partijen.

2.3 Tijdstip of Frequentie van Publicatie

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 de certificaten, zoals aangegeven in deze CPS.

Goedgekeurde versies van documenten die in het archief gepubliceerd moeten worden, worden geüpload volgens het veranderingsbeheerproces.

2.4 Controle op Toegang tot Archieven

Hoewel de “Citizen CA” 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, privébestanden, enz.

De OCSP-dienst, een webinterfacedienst voor verificatie van de certificaatstatus, het certificaatarchief en de Lijsten met Ingetrokken Certificaten (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 “Citizen CA” 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 van downloaddiensten in verband met de OCSP, Webinterface statusverificatie, CRL en Delta-CRL.
- De CA kan de behandeling van OCSP-aanvragen niet beperken voor enige partij die, op grond van haar activiteiten, genoodzaakt is regelmatig de OCSP-status te verifiëren.

3 Identificatie en Authenticatie

3.1 Benaming

De regels omtrent de benaming en de identificatie van de burgers voor burgercertificaten zijn dezelfde als de wetsbepalingen die van toepassing zijn op de benaming en de identificatie van burgers op identiteitskaarten.

3.1.1 Soorten Namen

Kenmerken van onderwerpsvelden in eindgebruikerscertificaten staan beschreven in het document **EID-DEL-004 EID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C).**

3.1.2 Namen moeten Zinvol Zijn

Zie hoofdstuk 3.1.1

3.1.3 Anonimiteit of Pseudonimiteit van de Abonnees

Hoofdstuk is niet van toepassing.

3.1.4 Regels voor het Interpreteren van Verschillende Naamvormen

Zie hoofdstuk 3.1.1

3.1.5 Uniek karakter van Namen

De DN van een eindgebruikerscertificaat moet uniek zijn

3.1.6 Erkenning, Authenticatie en Rol van Handelsmerken

Hoofdstuk is niet van toepassing.

3.2 Initiële Geldigheidsverklaring van Identiteit

De identificatie van de burger die een Elektronische Identiteitskaart aanvraagt, gebeurt in overeenkomst met de procedures en de regelgeving die van toepassing zijn op de levering van de Elektronische Identiteitskaarten. De RA specificeert de procedures die de LRA's ten uitvoer moeten brengen.

De toepasselijke procedures zijn terug te vinden op:

Nederlands: www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/reglementering/

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

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

3.2.1 Methode om het Bezit van een Privésleutel te Bewijzen

In overeenstemming met de Europese en Belgische Wet op de Handtekeningen, worden privésleutels gegenereerd op beveiligde smartcards. De Kaartproducent is verantwoordelijk voor het beveiligen van de smartcard waarop zich de "Qualified Signature Creation Device" (QSCD) bevindt met een Persoonlijk Identificatienummer (PIN). De Certificaathouder, de burger, is verantwoordelijk voor het geheimhouden van de pin van zijn smartcard. Certipost verifieert twee keer per jaar dat de Belgische eID kaart staat op de EU QSCD lijst.

3.2.2 Authenticatie Identiteit Organisatie

Hoofdstuk is niet van toepassing

3.2.3 Authenticatie Individuele Identiteit

Zie hoofdstuk 3.2

3.2.4 Niet-Gecontroleerde Informatie over de Abonnee

Hoofdstuk is niet van toepassing.

3.2.5 Geldigheidsverklaring van Autoriteit

Zie hoofdstuk 3.2

3.2.6 Criteria voor Interoperabiliteit

Hoofdstuk is niet van toepassing.

3.3 Identificatie en Authenticatie voor Aanvragen van nieuwe Sleutels

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

De toepasselijke procedures zijn terug te vinden op:

Nederlands: www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/reglementering/

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

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

3.3.1 Identificatie en Authenticatie voor Aanvragen van nieuwe Sleutels

Zie hoofdstuk 3.3

3.3.2 Identificatie en Authenticatie voor Aanvragen van nieuwe Sleutels na Herroeping

Zie hoofdstuk 3.3

3.4 Identificatie voor Aanvragen tot Herroeping

De identificatie van de burger die een herroeping van zijn Burgercertificaat aanvraagt, gebeurt in overeenkomst met de procedures en regelgeving die van toepassing zijn op de levering van Elektronische Identiteitskaarten.

De identificatie en authenticatie van houders die de herroeping van hun Burgercertificaten wensen, gebeuren door de entiteit die de aanvraag ontvangt. Deze entiteiten kunnen de volgende zijn:

- de gemeente;
- de politie;
- DOCSTOP 00800 2123 2123 or +32 2 518 2123

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

De RA stuurt de digitaal ondertekende aanvraag tot herroeping over een beveiligd netwerk naar de CA. De CA bevestigt de herroeping aan de RA.

4 Operationele Vereisten Voor De Levensduur Van Certificaten

Voor De Levensduur Van Certificaten Alle entiteiten binnen het bevoegdheidsgebied van de TSP, inclusief de LRA's, burgers, 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 passende 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 uitgifte, de herroeping of de schorsing van certificaten op aanvraag van de RA of de TSP, met uitsluiting van alle andere, tenzij de RA uitdrukkelijk andere instructies geeft.

Om haar taken uit te voeren, doet de TSP een beroep op de diensten van een derde partij. De TSP neemt ten aanzien van de burgers en de vertrouwende partijen de volledige aansprakelijkheid en verantwoordelijkheid op zich voor handelingen of verzuim van alle agenten als derde partij waarop een beroep gedaan wordt om certificeringdiensten te verlenen.

4.1 Certificaataanvraag

4.1.1 Wie kan een Certificaataanvraag indienen?

Het inschrijvingsproces, dat door de gemeenten (d.w.z. de LRA) wordt geïnitieerd om certificaten voor de abonnees (de burgers) aan te vragen, maakt integraal deel uit van het aangevraagde inschrijvingsproces voor de Elektronische Identiteitskaart. De procedure die de LRA hanteert voor de inschrijving van de burger wordt voorzien door de RA.

4.1.2 Inschrijving: Proces en Verantwoordelijkheden

Na de goedkeuring van een certificaataanvraag vraagt de RA de uitgifte van het certificaat aan bij de CA. De CA verifieert de volledigheid, integriteit en het unieke karakter van de gegevens die de RA indient niet, maar vertrouwt wat betreft de juistheid van de gegevens volledig op de RA. 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 Burgercertificaat gebruikt werd. Is dit wel het geval, dan 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 geschikte, veilige communicatiekanaal ingediend worden;
- alle passende verificaties uitgevoerd werden conform de bepalingen van het CA-contract.

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

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

Na de uitgifte van een certificaat, kondigt de CA een uitgegeven certificaat aan in een archief en schorst ze het certificaat. Vervolgens wordt het certificaat aan de RA bezorgd.

De RA vraagt de Kaartproducent om de Burgercertificaten op de Elektronische Identiteitskaart te laden. De Kaartproducent levert de Elektronische Identiteitskaart met de Burgercertificaten veilig aan de LRA.

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 Identiteitskaart. 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 Identiteitskaart 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.

De toepasselijke procedures zijn terug te vinden op:

Nederlands: www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/reglementering/

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

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

4.2.1 Uitvoeren van Identificatie- en Authenticatiefuncties

Hoofdstuk is niet van toepassing.

4.2.2 Goedkeuring of Weigering van Certificaataanvragen

Hoofdstuk is niet van toepassing.

4.2.3 Tijd voor het Verwerken van de Certificaataanvragen

Hoofdstuk is niet van toepassing.

4.3 Uitgave van Certificaten

Na de goedkeuring van een certificaataanvraag vraagt de RA de uitgifte van het certificaat aan bij de CA. De CA verifieert de volledigheid, integriteit en het unieke karakter van de gegevens die de RA indient niet, maar vertrouwt wat betreft de juistheid van de gegevens volledig op de RA. 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 Burgercertificaat gebruikt werd. Is dit wel het geval, dan 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 geschikte, veilige communicatiekanaal ingediend worden;
- alle passende verificaties uitgevoerd werden conform de bepalingen van het CA-contract.

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

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

Na de uitgifte schorst de CA het certificaat. Vervolgens wordt het certificaat aan de RA bezorgd.

De RA vraagt de Kaartproducent om de Burgercertificaten op de Elektronische Identiteitskaart te laden. De Kaartproducent levert de Elektronische Identiteitskaart met de Burgercertificaten veilig aan de LRA.

4.3.1 Acties van de CA bij de Uitgifte van het Certificaat

Hoofdstuk is niet van toepassing.

4.3.2 Kennisgeving aan de Inschrijver door de CA die het Certificaat Uitgeeft

Hoofdstuk is niet van toepassing.

4.4 Aanvaarding van Certificaten

Na de aanmaak ervan heeft de Elektronische Identiteitskaart de status ‘niet-geactiveerd’. De LRA activeert de Elektronische Identiteitskaart in aanwezigheid van de burger. Zowel de burger als de RA hebben de activeringsgegevens voor de kaart nodig. Deze gegevens dienen door de Kaartproducent veilig te worden bezorgd. De kaart kan enkel geactiveerd worden door de gegevens van de RA te combineren met die van de burger.

4.4.1 Gedrag dat de Aanvaarding van een Certificaat Inhoudt

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.

4.4.2 Publicatie van het Certificaat door de CA

Hoofdstuk is niet van toepassing.

4.4.3 Kennisgeving door de CA van de Uitgifte van Certificaten aan Andere Entiteiten

Hoofdstuk is niet van toepassing.

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 Privésleutel van de Abonnee en Gebruik van het Certificaat

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

- een certificaat niet te vervalsen;
- risico's, verlies, onthulling, wijziging of enig ander onbevoegd gebruik van de privésleutels te vermijden;
- certificaten alleen gebruiken voor wettelijke en toegelaten doeleinden, conform de CPS.

4.5.2 Openbare Sleutel Vertrouwende Partij en Gebruik van het Certificaat

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

4.6 Vernieuwing van Certificaten

Volgens RFC 3647 wordt een vernieuwing van een certificaat gedefinieerd als "*The issuance of a new Certificate without changing the Public Key or any other information in the Certificate".* Voor eindgebruikers van de certificaten (authenticatie en signing), wordt deze capabiliteit niet ondersteund.

4.6.1 Gevallen waarin het Certificaat moet worden vernieuwd

Vernieuwing van certificaten is niet ondersteund.

4.6.2 Wie Mag een Vernieuwing Aanvragen?

Zie hoofdstuk 4.6.1

4.6.3 Verwerken van Aanvragen voor Vernieuwing van Certificaten

Zie hoofdstuk 4.6.1

4.6.4 Kennisgeving van de Uitgifte van een Nieuw Certificaat aan de Inschrijver

Zie hoofdstuk 4.6.1

4.6.5 Gedrag dat de aanvaarding van een vernieuwd certificaat inhoudt

Zie hoofdstuk 4.6.1

4.6.6 Publicatie van het vernieuwde certificaat door de CA.

Zie hoofdstuk 4.6.1

4.6.7 Kennisgeving door de CA van de uitgifte van certificaten aan andere entiteiten

Zie hoofdstuk 4.6.1

4.7 Aanvraag Nieuwe Sleutels voor Certificaat

Volgens RFC 3647 wordt het aanvragen van nieuwe sleutels voor een certificaat gedefinieerd als *"… a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key".* In context van eID betekent dit dat de subject (de burger) een nieuw certificaat kan aanvragen met dezelfde identificatie-informatie maar andere publieke sleutels en een andere geldigheidsperiode. Due diligence, het genereren van sleutelparen, de levering en het beheer worden uitgevoerd in overeenstemming met deze CP/CPS.

4.7.1 Geval waarin er Sleutels voor Nieuwe Certificaten moeten worden Aangevraagd

Het aanvragen van nieuwe sleutels wordt ondersteund.

4.7.2 Wie mag Certificatie voor een Nieuwe Openbare Sleutel Aanvragen?

Zie hoofdstuk 4.1.1

4.7.3 Verwerken van Aanvragen voor Nieuwe Sleutels voor Certificaten

Aanvragen voor nieuwe sleutels worden op dezelfde manier verwerkt als aanvragen voor nieuwe authenticatie- of handtekeningcertificaten en in overeenstemming met de bepalingen van deze CP/CPS.

4.7.4 Kennisgeving van de Uitgifte van een Nieuw Certificaat aan de Inschrijver

Hoofdstuk is niet van toepassing.

4.7.5 Gedrag dat de Aanvaarding van Nieuwe Sleutels voor een Certificaat inhoudt

Hoofdstuk is niet van toepassing.

4.7.6 Publicatie van de Nieuwe Sleutels voor het Certificaat door de CA

Hoofdstuk is niet van toepassing.

4.7.7 Kennisgeving door de CA van de Uitgifte van Certificaten aan Andere Entiteiten

Hoofdstuk is niet van toepassing.

4.8 Wijziging van Certificaten

Hoofdstuk is niet van toepassing.

4.9 Schorsing en Herroeping van Certificaten

Wanneer een burger een nieuw eID aanvraagt wordt de kaart geleverd aan het gemeentehuis waar die burger is ingeschreven. De certificaten blijven in een geschorste staat tot de burger de eID komt ophalen.

Om de herroeping van een certificaat aan te vragen, moet een burger contact opnemen met een LRA, de politie of DOCSTOP. Gelieve op te merken dat de openingsuren van een LRA beperkt zijn, maar dat DOCSTOP 24 uur per dag en 7 dagen per week bereikbaar is.

Niet geactiveerde eID's met geschorste certificaten worden direct geleverd aan Belgische burgers die in het buitenland verblijven. Nadien kunnen ze de chip en de certificaten laten activeren bij het gemeentehuis. Deze activatieperiode is niet beperkt in tijd.

De politie, LRA, DOCSTOP of de RA vraagt via de RA onmiddellijk de herroeping van de Burgercertificaten aan, nadat:

- een kennisgeving ontvangen werd dat er een vermoeden bestaat dat de privésleutel of één van de of beide Burgercertificaten verloren, gestolen, gewijzigd of op ongeoorloofde 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 burger, waarin gesteld wordt dat diens privésleutel of één van de of beide Burgercertificaten verloren, gestolen, gewijzigd of op ongeoorloofde wijze onthuld of in gevaar gebracht werden;
- de informatie die een Burgercertificaat 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;
- er aan de RA een wettelijke verplichting werd opgelegd.

De CA herroept de Burgercertificaten op aanvraag van de RA of de TSP.

Indien de abonnee de opschorting van een certificaat aanvroeg via DOCSTOP, dan wordt hij van de gewijzigde status van het certificaat op de hoogte gebracht via een naar zijn officieel adres verzonden brief.

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

De TSP zal de eID CSP-stuurgroep toelating vragen om 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 burgers op de hoogte gesteld worden van dergelijke schorsing/herroeping.

Vertrouwende partijen moeten, om de status van certificaten te controleren, gebruikmaken van online hulpmiddelen die de CA ter beschikking stelt via het archief, alvorens deze certificaten te vertrouwen. De CA werkt de OCSP, de webinterface voor verificatie van de certificaatstatus, de CRL's en de Delta-CRL's dienovereenkomstig bij. CRL's worden regelmatig bijgewerkt, met een minimuminterval van drie uur.

De CA verleent toegang tot OCSP-hulpmiddelen en een website waarop inlichtingenaanvragen over de status van certificaten ingediend kunnen worden. Daarnaast zal de informatie over de status van de herroeping voor elk Certificaat dat onder de "Citizen CA" is uitgegeven, via de CRL beschikbaar zijn na de geldigheidsperiode van het certificaat.

4.9.1 Omstandigheden voor Herroeping

De CA publiceert kennisgevingen van geschorste of herroepen certificaten in het Archief.

4.9.2 Wie kan een Herroeping Aanvragen?

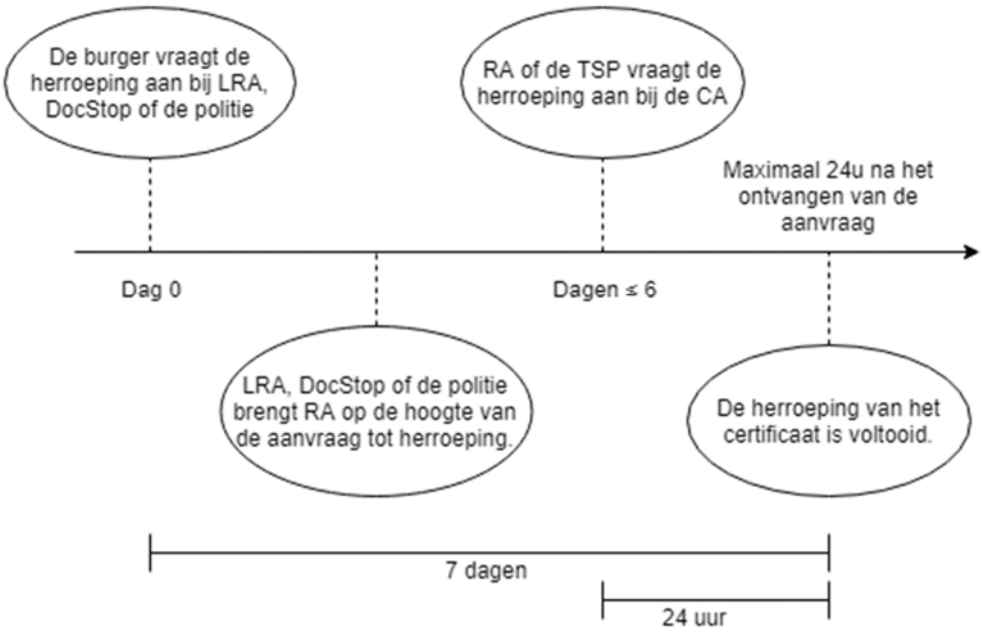
Zie hoofdstuk 4.9

4.9.3 Procedure voor Aanvragen tot Herroeping

Zie hoofdstuk 4.9

4.9.4 Wachtperiode Aanvraag tot Herroeping

De Wachtperiode voor de Aanvraag tot Herroeping is de periode vanaf wanneer de abonnee (d.i. de burger) een herroeping van een certificaat aanvroeg door contact op te nemen met de LRA, de politie of DOCSTOP totdat de herroeping van het certificaat in de diensten voor de geldigheidsverklaring van het certificaat is terug te vinden.



Figuur 1: De herroepingstijdlijn

Figuur 1: De herroepingstijdlijn toont dat er een maximum van 6 dagen tijd voorbij gaat tot de CA de aanvraag tot herroeping ontvangt, en een maximum van 24 uur vanaf dat moment tot de effectieve herroeping is verwerkt.

De wachtperiode voor het verwerken van de aanvraag tot herroeping bedraagt 7 kalenderdagen. Echter, vanaf de aanvraag tot herroepping ontvangen is door de CA, zal de geldigheid van het certificaat binnen de 3 uur worden gereflecteerd in de diensten voor certificaatstatus.

4.9.5 Tijd waarbinnen de CA de Aanvraag tot Herroeping moet Verwerken

Nadat ze het verzoek om intrekking van de RA heeft ontvangen, zal de CA een Burgercertificaat intrekken, en dat zo snel als praktisch mogelijk na de validering van het verzoek om intrekking. De maximale termijn tussen de ontvangst van een herroepingsverzoek of rapport en de beslissing om de beschikbaarheid voor alle vertrouwende partijen van de statusinformatie te veranderen, bedraagt 24 uur.

Over het algemeen worden de volgende termijnen gebruikt:

- Verzoeken om intrekking die drie of meer uur voor de uitgifte van de CRL worden ontvangen, worden verwerkt voordat de volgende CRL wordt gepubliceerd, en
- verzoeken om intrekking die minder dan drie uur voor de uitgifte van de CRL worden ontvangen, worden verwerkt voordat de volgende CRL wordt gepubliceerd.
- Verzoeken om intrekking worden binnen de drie uur na de ontvangst van het verzoek weergegeven in de OCSP-dienst voor de geldigheidsverklaring van het certificaat.

4.9.6 Vereisten voor het Controleren van de Intrekking voor Vertrouwende Partijen

Zie **EID-DEL-004 eID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

4.9.7 Frequentie Uitgifte CRL (indien van toepassing)

Zie **EID-DEL-004 eID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

4.9.8 Maximale Latentie voor CRL's (indien van toepassing)

Zie **EID-DEL-004 eID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

4.9.9 Online Herroeping /Beschikbaarheid Statuscontrole

Zie **EID-DEL-004 eID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

4.9.10 Vereisten Online Controle Herroeping

Zie **EID-DEL-004 eID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

4.9.11 Andere Vormen van Bekendmaking Gekende Schorsingen

Hoofdstuk is niet van toepassing.

4.9.12 Speciale Vereisten bij Gecompromitteerde Nieuwe Sleutels

Hoofdstuk is niet van toepassing.

4.9.13 Omstandigheden voor Schorsing

Zie hoofdstuk 4.9

4.9.14 Wie kan een Schorsing Aanvragen?

Zie hoofdstuk 4.9

4.9.15 Procedure om een Schorsing Aan te Vragen

Zie hoofdstuk 4.9

4.9.16 Limieten van Schorsingsperiode

Zie hoofdstuk 4.9

4.10 Diensten voor Certificaatstatus

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

4.10.1 CRL's en Delta-CRL's

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

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

Een CRL wordt op een overeengekomen tijdstip uitgegeven, met een minimuminterval van drie uur. Een Delta CRL wordt elke 3 uur uitgegeven, conform een overeengekomen

tijdsschema. CRL's en Delta CRL's worden door de CA ondertekend en van een tijdsaanduiding voorzien. De CRL's en Delta-CRL's zijn terug te vinden op:

http://crl.eid.belgium.be

4.10.2 OCSP

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

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

Webinterface voor diensten voor statusverificatie http://status.eid.belgium.be

De OCSP-responders zijn bereikbaar op:

http://ocsp.eid.belgium.be or http://ocsp.eid.belgium.be/2

4.10.3 Operationele Kenmerken

*Zie **EID-DEL-004 eID PKI Hiërarchie certificaatprofiel (CF. APPENDIX C)**.*

4.10.4 Beschikbaarheid van de Dienst

Diensten voor Certificaatstatus zijn bereikbaar gedurende 24 uur per dag en gedurende 7 dagen per week.

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 vertrouwende partij.
- Het downloaden van CRL's of Delta-CRL's via het internet of de overheidsnetwerken
- Webinterface voor diensten voor de verificatie van certificaatstatussen.

Indien de OCSP-dienst, CRL en Delta-CRL-downloaddienst en de webinterface 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.

4.10.5 Optionele Kenmerken

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.

4.11 Einde van het Abonnement

Hoofdstuk is niet van toepassing.

4.12 Deponeren en Recupereren van Sleutels

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

5 Facility, Management en Operationele Controles

In dit hoofdstuk worden de niet-technische veiligheidscontroles beschreven die de “Citizen CA” en andere PKI-partners gebruiken voor het aanmaken van sleutels, het identificeren van burgers, het uitgeven van certificaten, het herroepen van certificaten, audits en archivering.

5.1 Fysieke Controles

De TSP voert fysieke controles uit binnen het eigen gebouw. Onder de fysieke controles van de TSP-operator vallen:

De TSP beschikt op haar sites over de infrastructuur om de TSP-diensten te verlenen. De TSP zorgt voor eigen veiligheidscontroles op haar sites, waaronder toegangscontrole, inbraakdetectie en bewaking. De toegang tot de sites wordt beperkt tot 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.

5.1.1 Locatie en Constructie van de Site

De TSP-operatoren zorgen ervoor dat de gebouwen zijn gelegen in een gebied dat geschikt is voor verrichtingen die een hoge veiligheid vereisen. In deze gebouwen worden de zones genummerd en dienen gesloten kamers, kooien, kluizen en cabines aanwezig te zijn.

5.1.2 Fysieke Toegang

De fysieke 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 TSP-activiteiten in een beveiligde computerkamer met fysieke bewaking en veiligheidsalarmen, waarvoor een badge en toegangscontrolelijsten gebruikt worden om zich van de ene zone naar een andere te verplaatsen.

5.1.3 Stroom en Airconditioning

Overvloedige stroomvoorziening en klimaatregeling.

5.1.4 Blootstelling aan Water

De gebouwen worden beschermd tegen blootstelling aan water.

5.1.5 Brandpreventie en -Bescherming

De TSP implementeert preventie en bescherming en treft maatregelen tegen blootstelling aan brand.

5.1.6 Media-opslag

De media worden veilig bewaard. Veiligheidskopieën van de media worden bewaard op een andere plaats die fysiek veilig is en beschermd is tegen brand- en waterschade.

5.1.7 Afvoer van Afval

Het afval wordt op een veilige manier verwijderd opdat gevoelige gegevens niet ongewenst onthuld zouden worden.

5.1.8 Offsite Veiligheidskopie

De TSP zorgt voor een gedeeltelijke offsite veiligheidskopie.

5.2 Procedurecontroles

De TSP 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 het gebied van technologieën in verband met elektronische handtekeningen.

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

Alle personeelsleden die instaan voor het beheer van de sleutels, bestuurders, veiligheidsagenten en systeemauditeurs of voor enige andere activiteit die dergelijke handelingen materieel beïnvloedt, worden als betrouwbaar beschouwd.

De TSP 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.

Ingeval 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 TSP waarborgt dat alle handelingen in verband met de TSP toegeschreven kunnen worden aan het systeem van de TSP en aan het TSP-personeelslid dat de handeling heeft uitgevoerd.

5.2.1 Vertrouwde Rollen

De TSP maakt een onderscheid tussen de volgende onderscheiden werkgroepen:

- uitvoerend TSP-personeel dat verrichtingen op certificaten beheert;
- administratief personeel dat het platform waarop de TSP steunt, bedient;
- veiligheidspersoneel dat de veiligheidsmaatregelen afdwingt.

5.3 Controles van het Personeel

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

5.3.1 Kwalificaties, Ervaring en Vereiste Vergunningen

De TSP 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 Procedures voor Controles van de Achtergrond

De TSP 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

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

5.3.4 Frequentie en Vereisten inzake Bijscholing

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 Frequentie en Opeenvolging Personeelsverloop

Hoofdstuk is niet van toepassing.

5.3.6 Bestraffingen voor Onbevoegde Acties

De TSP 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 personeel van een deelnemer, naargelang gepast is volgens de omstandigheden.

5.3.7 Vereisten Onafhankelijke Aannemers

Onafhankelijke TSP-onderaannemers en diens personeel zijn onderworpen aan de zelfde achtergrondcontroles als het TSP-personeel. ZIE 5.3.1 KWALIFICATIES, ERVARING EN VEREISTE VERGUNNINGEN

5.3.8 Aan het Personeel Bezorgde Documentatie

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

5.4 Procedures voor Auditlogging

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

Het eventloggingsysteem van de CA registreert onder andere de volgende handelingen:

- uitgave van een certificaat;
- herroeping van een certificaat;
- schorsing van een certificaat;
- (her)activering van een certificaat;
- automatische herroeping;
- publicatie van een CRL of Delta-CRL.

De TSP controleert alle registraties betreffende de eventlogging. Registraties van audittrails omvatten:

- de identificatie van de verrichting;
- de datum 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 TSP legt daarenboven interne logboeken en audittrails aan van relevante operationele handelingen in de infrastructuur, waaronder, maar niet beperkt tot:

- het starten en stopzetten van servers;
- defecten en ernstige problemen;
- fysieke toegang van personeel en andere personen tot gevoelige delen van de TSP-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;
- fysieke plannen en beschrijvingen van de site;

- configuratie van hardware en software;
- toegangscontrolelijsten voor het personeel.

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

De Logbestanden en audittrails worden voor inspectie gearchiveerd door het bevoegde 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 audittrails worden veiligheidskopieën gemaakt.

Controlehandelingen worden niet gemeld.

5.4.1 Types van Bewaarde Gebeurtenissen

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

5.4.2 Frequentie van Processinglog

De CA checkt de auditlogs regelmatig op anomalieën of waarschuwingen.

5.4.3 Bewaarperiode voor Auditlog

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

5.4.4 Bescherming van Auditlog

Enkel de registerbeheerder (personeelslid dat aangesteld is voor de functie van registerbewaring) heeft toegang tot een TSP-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 TSP zal optreden bij een mogelijke toepassing van de procedure van artikel 14 van de Wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* en artikel 7 van de Wet van 12 mei 1927 *op de militaire opeisingen* door de Belgische Federale Overheid. In dergelijk geval zal de CA optreden volgens de instructies van de persoon die aangesteld wordt door middel van een Koninklijk Besluit met betrekking tot gegevens van Elektronische Identiteitskaarten en Burgercertificaten.

5.4.5 Back-upprocedures Auditlog

Op werkdagen wordt dagelijks een differentiële veiligheidskopie van de TSP-archieven gemaakt.

5.4.6 Systeem voor Auditverzameling

Het TSP-systeem voor archiefverzameling is intern.

5.4.7 Kennisgeving aan Abonnee die een Gebeurtenis Veroorzaakt

Niet van toepassing.

5.4.8 Evaluatie van de Kwetsbaarheid

Niet van toepassing.

5.5 Archivering van Registers

De TSP legt interne registers aan van de volgende items:

- alle certificaten gedurende een periode van minstens 25 jaar na de vervaldatum van dat certificaat;
- audittrails van de uitgifte van certificaten gedurende minstens 25 jaar na de uitgifte van een certificaat;
- audittrail van de herroeping van een certificaat gedurende een periode van minstens 25 jaar na de herroeping van een certificaat;
- CRL's en Delta-CRL's gedurende minstens 25 jaar na publicatie;
- de TSP dient de allerlaatste veiligheidskopie van het CA-archief bij te houden gedurende 25 jaar na de uitgifte van het laatste certificaat.

De TSP bewaart de archieven in een formaat dat gemakkelijk opgezocht kan worden.

De TSP waarborgt de integriteit van de fysieke 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 Types van Gearchiveerde Registers

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

5.5.2 Bewaarperiode voor Archief

De TSP houdt op een betrouwbare manier registers bij van digitale certificaten gedurende een termijn zoals aangegeven in artikel 5.5 van deze CPS. Deze vereiste wordt periodiek gecontroleerd.

5.5.3 Bescherming van het Archief

Enkel de registerbeheerder (personeelslid dat aangesteld is voor de functie van registerbewaring) heeft toegang tot een TSP-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 TSP zal optreden bij een mogelijke toepassing van de procedure van artikel 14 van de Wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* en artikel 7 van de Wet van 12 mei 1927 *op de militaire opeisingen* door de Belgische Federale Overheid. In dergelijk geval zal de CA optreden volgens de instructies van de persoon die aangesteld wordt door middel van een Koninklijk Besluit met betrekking tot gegevens van Elektronische Identiteitskaarten en Burgercertificaten.

5.5.4 Procedures voor de Veiligheidskopie van Archieven

Op werkdagen wordt dagelijks een differentiële veiligheidskopie van de TSP-archieven gemaakt.

5.5.5 Vereisten voor het Aanbrengen van Tijdstempels op Registers

Hoofdstuk is niet van toepassing.

5.5.6 Systeem voor Archiefverzameling (Intern of Extern)

Het TSP-systeem voor archiefverzameling is intern.

5.5.7 Procedures om Archiefinformatie te Verkrijgen en te Verifiëren

Enkel TSP-personeelsleden met een duidelijke hiërarchische controle en een welomlijnde functiebeschrijving kunnen archiefinformatie verkrijgen en verifiëren.

De TSP bewaart registers in elektronisch formaat of op papier.

5.6 Sleuteloverdracht

De "Citizen CA" heeft een schema voor de sleuteloverdracht van de afhankelijke uitgevende CA's en uitgevende CA-certificaten (de Citizen CA-certificaten kunnen worden gedownload van https://repository.eid.belgium.be):

Op het einde van elk jaar worden er een aantal "Citizen CA"-certificaten gegenereerd tijdens een "sleutelceremonie". Dit aantal wordt bepaald door de TSP en de overheid, en is gebaseerd op de verwachte vraag naar End Entity-certificaten voor het volgende jaar. Tijdens de "sleutelceremonie" worden de "Citizen CA"-certificaten uitgegeven door de BRCA's, die "long-living trust anchors" zijn van de eID PKI.

Zodra de nieuwe batch van "Citizen CA"-certificaten in de productieomgeving is geplaatst, zullen deze certificaten worden gebruikt om End Entity-certificaten uit te geven voor het lopende jaar, en zal de vorige batch van "Citizen CA"-certificaten niet langer worden gebruikt om nieuwe certificaten uit te geven. Met andere woorden, een "Citizen CA"-certificaat zal

slechts gedurende één jaar gebruikt worden om nieuwe certificaten uit te geven. Een "Citizen CA"-certificaat zal langer geldig zijn dan End-Entity-certificaten die het uitgegeven heeft.

Zodra een "Citizen CA"-certificaat is vervallen of werd ingetrokken, zal het sleutelmateriaal tijdens de volgende "sleutelceremonie" worden vernietigd.

5.7 Risico's en Rampherstel

Er werd een continuïteitsplan uitgewerkt om de voortzetting van de activiteiten te waarborgen na een natuurramp of een andere ramp.

Al deze maatregelen werden geïmplementeerd op basis van de ISO 27001.

De TSP zorgt voor:

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

5.7.1 Procedures voor het Omgaan met Incidenten en Risico's

De "Citizen CA" specificeert in een afzonderlijk intern document toepasselijke procedures voor het melden en behandelen van incidenten en risico's. De TSP 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 TSP bepaalt de nodige maatregelen om het volledig en automatisch herstel van de dienst in geval van een ramp, defecte servers, software of gegevens te waarborgen.

5.7.2 Computermiddelen, software, en/of beschadigde gegevens.

De TSP heeft specifieke 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.

5.7.3 Procedures In Gevaar Brengen Privésleutel Entiteit

Indien een "Citizen CA"-privésleutel in gevaar wordt gebracht, of indien het vermoeden daarvoor bestaat, dan worden de TSP Crisis Management-procedures bepaald volgens het "Incident Management"-proces en met de goedkeuring van het senior management van Certipost en de vertegenwoordigers van de Belgische Federale Overheid. De betrokken partijen worden op de hoogte gebracht via een communicatieplan en ingeval een intrekking van een CA-certificaat vereist is, dan wordt de status "ingetrokken" meegedeeld aan de vertrouwende partijen via de eID Repository Website of via de eID CRL Website.

5.7.4 Mogelijkheid om de Activiteit te Hervatten na een Ramp

De TSP heeft de mogelijkheid ontwikkeld om haar CA-verrichtingen te hervatten binnen de vier (4) uur na een ramp, met ondersteuning voor alle belangrijke functies, d.i. de uitgifte en de intrekking van certificaten en de publicatie van CRL-informatie.

5.8 Beëindiging CA of RA

Zodra de TSP van de Belgische Federale Overheid verneemt dat het contract beëindigd zal worden en/of zodra het contract voortijdig geannuleerd wordt, zal de TSP met de Belgische Federale Overheid overleggen om te bepalen welke stappen vereist zijn om (1) de vlekkeloze overdracht van de dienstverlening naar de nieuwe TSP te waarborgen en om (2) de vernietiging, de verwijdering, het herstel en/of de beveiliging van de informatie, de persoonsgegevens en de bestanden die de TSP tijdens de uitvoering van haar taken als TSP ontvangen heeft, te waarborgen in overeenstemming met de Europese Richtlijn 910/2014 *houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten*.

6 Technische Veiligheidscontroles

In dit deel worden de veiligheidsmaatregelen bepaald die de CA moet nemen om zijn cryptografische sleutels en activeringsgegevens te beschermen (vb. pins, wachtwoorden of manueel bijgehouden gedeelde sleutels).

6.1 Genereren en Installeren van Sleutelparen

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

De CA mag de privésleutels die gebruikt worden binnen de CA niet gebruiken voor doeleinden buiten het domein van de "Citizen CA".

6.1.1 Genereren van Sleutelparen

De CA en de RA gebruiken een betrouwbaar proces voor het genereren van de CA-privésleutel, overeenkomstig een gedocumenteerde procedure. De CA verdeelt de geheime gedeelten van de eigen privésleutel(s). De CA mag deze geheime gedeelten overmaken aan geautoriseerde houders van geheime gedeelten, overeenkomstig een gedocumenteerde procedure.

De sleutelparen voor de afhankelijke uitgevende CA's van de "Citizen CA" (die CA-sleutels uitgeeft) werden gegenereerd in een offline HSM die op zijn minst voldoet aan de FIPS 140-2 Niveau 3-vereisten. Vervolgens werden de sleutels van de Uitgevende CA gekloond in een online HSM die op zijn minst voldoet aan de FIPS 140-2 Niveau 3-vereisten.

6.1.2 Aflevering Privésleutel aan Abonnee

De privésleutel van de abonnee wordt gegenereerd door de kaartproducent op en door de QSCD. De privésleutel wordt niet van de QSCD gehaald.

6.1.3 Aflevering van de Openbare Sleutel aan de Uitgever van het Certificaat

Nadat het sleutelpaar op de QSCD is gegenereerd, wordt de publieke sleutel van de abonnee overgeheveld van de Kaartproducent naar de RA door middel van een versleuteld bericht via een beveiligde verbinding. De RA neemt de publieke sleutel op in een aanvraag en verstuurt hem naar de CA via een private, beveiligde verbinding.

Om het certificaat opnieuw aan de Kaartproducent af te leveren, wordt dezelfde methode gebruikt.

6.1.4 Aflevering Publieke Sleutel van CA aan Vertrouwende Partijen

De publieke sleutel van de CA wordt beschikbaar gesteld op de eID Repository-website.

6.1.5 Sleutelgroottes

Meer details zijn terug te vinden in het volgende document:

EID-DEL-004 eID PKI Hiërarchie certificaatprofiel (cf. Appendix C) Genereren Parameters Openbare Sleutel en Kwaliteitscontrole

Zie hoofdstuk **6.1.1 Genereren van Sleutelparen**

6.1.6 Doeleinden Gebruik Sleutel (volgens X.509 v3 domein sleutelgebruik)

Meer details zijn terug te vinden in het volgende document: **EID-DEL-004 eID PKI Hiërarchie certificaatprofiel (cf. Appendix C).**.

6.2 De bescherming van Privésleutels en de Controle van Cryptografische Modules

6.2.1 Beveiligde Cryptografische Module

De hardware van de "Beveiligde Cryptografische Device" is de NXP chip P5CC081, die EAL5+-gecertificeerd is.

De “Belpic” applet V1.7 die draait op het MultiAppID v2.1 80K CC-platform op de chip, is EAL4+-gecertificeerd.

6.2.2 Genereren van een privésleutel

Het sleutelpaar (privésleutel-openbare sleutel) wordt gegenereerd op de chip.

Enkel de openbare sleutel kan vanaf de chip worden geëxporteerd. De privésleutels blijven beveiligd in de chip.

6.2.3 Controle meerdere personen privésleutel

Niet van toepassing. Het "Secure Cryptographic Device" mag enkel worden gebruikt door de aangeduide Abonnee.

6.2.4 Deponeren van een privésleutel

Privésleutels kunnen niet en worden nooit afgehaald van het "Secure Cryptographic Device" waarop ze gegenereerd zijn. Privésleutels mogen nooit gedeponeerd worden.

6.2.5 Veiligheidskopie privésleutel

Privésleutels op een "Secure Cryptographic Device" worden op de smartcard aangemaakt; er kan geen veiligheidskopie van worden gemaakt.

6.2.6 Archivering privésleutel

Privésleutels op een "Secure Cryptographic Device" worden op de smartcard aangemaakt en kunnen er niet van worden afgehaald voor back-up, deponering of archivering.

6.2.7 Overdracht van een privésleutel op of vanaf een cryptografische module

Privésleutels op een "Secure Cryptographic Device" kunnen niet worden overgedragen.

6.2.8 Opslag van privésleutels op een cryptografische module

Privésleutels op een "Secure Cryptographic Device" worden opgeslagen in een beveiligd geheugen. De ingebouwde microchip beschermt privésleutels en andere veiligheidsgerelateerde informatie tegen hacks.

6.2.9 Methode voor het activeren van privésleutels

De Activeringsgegevens voor het "Secure Cryptographic Device" bestaan uit pin- en pukcodes. De pin- en pukcodes worden aan de Abonnee bezorgd in een beschermend verzegeld omhulsel zoals een pinbrief of een verzegelde omslag.

6.2.10 Methode om de privésleutel te vernietigen

De privésleutel kan worden geblokkeerd of zelfs uit bedrijf worden genomen (onomkeerbaar geblokkeerd) als er herhaaldelijk een verkeerde pin- of pukcode wordt opgegeven.

6.2.11 Cryptographic Module Rating

Minimumstandaarden voor cryptografische modules werden gespecificeerd in paragraaf:

> **BIJLAGE B: VEREISTEN VOOR CERTIFICATIEAUTORITEITEN**

6.3 Andere Aspecten van het Beheer van Sleutelparen

De TSP maakt gebruik van cryptografische inrichtingen om de sleutels van de CA te beheren. Deze cryptografische inrichtingen worden Hardware Security Modules (HSM's) genoemd.

Deze inrichtingen zijn conform de formele vereisten (FIPS 140-2 Niveau 3 of hoger), waarbij onder meer gegarandeerd wordt dat misbruik onmiddellijk gedetecteerd wordt en dat privésleutels de HSM niet ongecodeerd kunnen verlaten.

Hardware- en softwaremechanismen die de privésleutels van de CA beschermen zijn gedocumenteerd. Het document toont aan dat mechanismen die de sleutels van de CA beschermen minstens even sterk zijn als de CA-sleutels die ze beschermen.

6.3.1 Archivering Openbare Sleutel

6.3.2 Operationele Periodes Certificaat en Gebruiksperiodes Sleutelpaar

Meer details zijn terug te vinden in het volgende document: **EID-DEL-004 eID PKI HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

6.4 Activeringsgegevens

6.4.1 Genereren en Installeren van Activeringsgegevens

De activering van de Root-CA wordt tot stand gebracht door middel van sleutelbewaarders.

De operationele CA's worden geactiveerd door middel van een operationeel token.

De activering van de sleutel van de abonnee gebeurt:

- eerst bij ontvangst van de eID (QSCD)-kaart door de gemeente:
  - de kaart en de sleutel kunnen enkel door de gemeente geactiveerd worden;
  - in samenwerking met de ambtenaar.
- Voor de operationele activering wordt de Persoonlijke Identificatiecode van de abonnee gebruikt.

6.4.2 Bescherming activeringsgegevens

Voor de Root CA hebben de sleutelbewaarders elk een deel van de activeringssleutel. Die tokens zijn beschermd met een wachtzin. Het beschermingsschema is M VAN N. De tokens worden bewaard in een kluis.

De operationele CA's worden beschermd door een gesplitst operationeel token. Die (M van N) tokens zijn beschermd met een wachtzin. De tokens worden bewaard in een kluis.

De sleutel van de abonnee wordt beschermd door een pin, de pin wordt via de post rechtstreeks aan de abonnee bezorgd in een beveiligde omslag. De Activeringsgegevens moeten van buiten worden geleerd, ze mogen nergens genoteerd worden. De Activeringsgegevens mogen met niemand gedeeld worden. De Activeringsgegevens mogen niet enkel bestaan uit informatie die makkelijk kan worden geraden, zoals persoonlijke gegevens van een Certificaathouder.

6.4.3 Andere Aspecten van Activeringsgegevens

De CA bewaart en archiveert op veilige wijze activeringsgegevens die verband houden met de eigen privésleutel en handelingen.

6.5 Veiligheidscontroles Computermateriaal

De CA voert een aantal passende veiligheidscontroles voor het computermateriaal in. Dat houdt onder meer in: fysieke en logische toegangscontroles, scheiding van rollen, meerdere lagen van controles, opsporen van intrusies en "multifactor"-authenticatieprocessen voor alle personeelsleden die aanleiding kunnen geven tot de uitgifte van een certificaat of die ervoor kunnen zorgen dat een persoon een certificaat kan uitgeven.

6.5.1 Technische Vereisten Specifieke Computerveiligheid

De "Citizen CA" voorziet in de volgende functionaliteit via het besturingssysteem en een combinatie van het besturingssysteem, de PKI-software en fysieke controles:

- toegangscontroles voor CA-diensten en PKI-rollen;
- gedwongen scheiding van taken voor PKI-rollen;
- identificatie en authenticatie van PKI-rollen en bijbehorende identiteiten;
- gebruik van versleuteling voor sessiecommunicatie en databasebeveiliging;

- archivering van CA en "end entity"-geschiedenis en auditgegevens;
- audit van veiligheidsgerelateerde gebeurtenissen;
- herstelmechanismes voor sleutels en het CA-systeem.

Informatie over deze functionaliteit is terug te vinden in de respectieve hoofdstukken van deze CPS.

6.5.2 Veiligheidscontroles Computermateriaal

Niet van toepassing

6.6 Levenscyclus Technische Controles

Bij de aanschaf van hardware en software die dient om een Uitgevende CA te laten werken binnen de "Citizen CA", moet erop worden gelet dat het risico wordt beperkt dat er met bepaalde componenten kan worden geknoeid, zoals het willekeurig selecteren van bepaalde componenten. Uitrusting voor gebruik binnen de eID PKI dient te worden ontwikkeld in een gecontroleerde omgeving en volgens strikte veranderingscontroleprocedures.

Een continue verantwoordelijkheidsketen, vanaf de locatie waar alle hardware en software die werd geïdentificeerd als ondersteuning van een Uitgevende CA binnen de eID PKI, moet worden aangehouden door ze te laten verzenden of leveren via gecontroleerde methodes. De uitrusting van de Uitgevende CA mag geen applicatie of componentsoftware hebben geïnstalleerd die geen onderdeel is van de configuratie van de Uitgevende CA. Alle latere updates van de uitrusting van de Uitgevende CA moeten op dezelfde manier als de oorspronkelijke uitrusting worden aangekocht of ontwikkeld en moeten op een welbepaalde manier door betrouwbaar en goed opgeleid personeel worden geïnstalleerd.

De "CA factory" heeft een goedgekeurd Systeemveiligheidsbeleid opgesteld waarin controles van de computerveiligheid zijn opgenomen die specifiek zijn voor de eID PKI en het volgende aanpakken:

6.6.1 Controles Ontwikkeling Systemen

Voor de ontwikkeling en implementering van nieuwe systemen moeten er formele procedures worden gevolgd. Tijdens de fase van het design en van het specificeren van de vereisten wordt er een analyse van de veiligheidsvereisten uitgevoerd. Uitbestede projecten m.b.t. softwareontwikkeling worden van nabij opgevolgd en gemonitord.

6.6.2 Veiligheidsbeheercontroles

De "Citizen Certificate Authority" volgt de "Certificate Issuing and Management Components (CIMC)"- beveiligingsprofielen die de vereisten definieert voor componenten die Publiekesleutelcertificaten, zoals X.509-Certificaten, uitgeven, intrekken en beheren. De CIMC is gebaseerd op de gebruikelijke Criteria/ISO IS15408-standaarden.

6.6.3 Levenscyclus Veiligheidscontroles

De CA gebruikt een methodologie voor configuratiebeheer voor de installatie en het lopende onderhoud van de CA-systemen. Als de CA-software voor het eerst wordt geladen, dan voorziet ze een methode om na te gaan of de software op het systeem:

- afkomstig is van de softwareontwikkelaar;
- niet werd gewijzigd vóór de installatie;
- de versie is die bedoeld is voor het gebruik.

De “CA Chief Security Officer” controleert periodiek de integriteit van de CA-software en monitort de configuratie van de CA-systemen.

6.7 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 Burgercertificaat, wordt beveiligd met PKI-gebaseerde technieken voor de codering en ondertekening, met het oog op de vertrouwelijkheid van de informatie en de wederzijdse authenticatie. Ook communicatie in verband met aanvragen, de uitgifte, de schorsing, de opheffing van een schorsing en de herroeping van certificaten valt hieronder.
- 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.

6.8 Aanbrengen van Tijdstempels

Niet van Toepassing

7 Certificaat, CRL en OCSP-Profielen

7.1 Profiel van een Certificaat

De profielen en kenmerken van een certificaat staan beschreven in het volgende document: **EID-DEL-004 eID PKI-HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

7.1.1 Versienummer(s)

Zie hoofdstuk 7.1

7.1.2 Certificaatextensies

Zie hoofdstuk 7.1

7.1.3 Algoritme Object Identifiers

Zie hoofdstuk 7.1

7.1.4 Naamvormen

Zie hoofdstuk 7.1

7.1.5 Vereisten m.b.t. Namen

Zie hoofdstuk 7.1

7.1.6 Certificaatpolicy Object Identifier

Zie hoofdstuk 7.1

7.1.7 Gebruik van beleidsbeperkend attribuut

Zie hoofdstuk 7.1

7.1.8 Beleidsqualifiers Syntax en Semantiek

Zie hoofdstuk 7.1

7.1.9 Verwerking semantiek voor kritische certificaatbeleidsattributen

Hoofdstuk is niet van toepassing.

7.1.10 Certificaatgeldigheid

De geldigheid van een Citizen End-Entity-certificaat is onderworpen aan twee vereisten:

- de geldigheidsperiode mag niet langer duren dan 10 jaar en 8 maanden (*zie hoofdstuk 7.1*);

- de geldigheidsperiode van het certificaat mag niet langer zijn dan de geldigheidsperiode van de eID-kaart waarop de chip met het certificaat is geplaatst.

Bij het genereren van de aanvraag tot uitgifte van een certificaat zal de RA steeds de kortste geldigheidsperiode van deze twee vereisten kiezen.

7.2 CRL-Profiel

De CRL-profielen en -kenmerken staan beschreven in het volgende document: **EID-DEL-004 eID PKI-HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

7.2.1 Versienummer(s)

Zie hoofdstuk 7.2

7.2.2 CRL en CRL-Extensies

Zie hoofdstuk 7.2

7.3 OCSP-Profiel

De OCSP-profielen en -kenmerken staan beschreven in het volgende document: **EID-DEL-004 eID PKI-HIËRARCHIE CERTIFICAATPROFIEL (CF. APPENDIX C)**.

7.3.1 Versienummer(s)

Zie hoofdstuk 7.3

7.3.2 OCSP-Extensies

Zie hoofdstuk 7.3

8 Audit van de Overeenkomstigheid en Andere Beoordelingen

Wat het Gekwalificeerd Handtekeningcertificaat betreft, gaat de TSP te werk volgens de voorwaarden van De Europese Richtlijn 910/2014 die het wettelijk kader voor elektronische handtekeningen in België vastlegt.

De TSP komt tegemoet aan de vereisten opgesomd in de ETSI-beleidsdocumenten die verwijzen naar gekwalificeerde certificaten, waaronder:

- EN 319 411-2: Vereisten voor Trust Service Providers die EU- gekwalificeerde certificaten uitgeven
- EN 319 412-5: Profielen voor Trust Service Providers die Certificaten uitgeven, Gekwalificeerd Certificaat-profiel. Deel 5: Extensie voor Gekwalificeerd Certificaatprofiel.

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

- de autoriteit die toezicht houdt op de Trust Service Providers 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 TSP evalueert de resultaten van deze audits, vooraleer ze verder in te voeren.

8.1 Frequentie of Omstandigheden van Evaluatie

De "PKI factory" wordt jaarlijks aan een audit onderworpen.

8.2 Identiteit/Kwalificaties van de Evaluator

De auditdiensten dienen te worden uitgevoerd door onafhankelijke, erkende, geloofwaardige en betrouwbare auditfirma's of IT-consultingbedrijven, mits ze gekwalificeerd zijn om informatieveiligheidsaudits uit te voeren en er ervaring mee hebben, en meer specifiek als ze veel ervaring hebben met PKI en cryptografische technologieën.

8.3 Relatie van de Evaluator met de Geëvalueerde Entiteit

De auditeur en de geauditeerde Uitgevende CA mogen geen andere relatie hebben die afbreuk zou doen aan de onafhankelijkheid en de objectiviteit van de auditeur krachtens de Algemeen Aanvaarde Auditingstandaarden. Deze relaties omvatten financiële, wettelijke, sociale of andere relaties die aanleiding zouden kunnen geven tot een belangenconflict.

8.4 Aspecten die worden Geëvalueerd

Bij de audit wordt op de volgende elementen gelet:

- overeenkomstigheid van de bedrijfsprocedures en -principes van de TSP met de procedures en dienstniveaus bepaald in de CPS;
- beheer van de infrastructuur die de TSP-diensten invoert;
- beheer van de fysieke infrastructuur van de site;
- aanhankelijkheid aan de CPS;
- naleving van de relevante Belgische wetten;
- bevestiging van de overeengekomen dienstniveaus;
- inspectie van audittrails, logs, relevante documenten enz.;
- de reden waarom de hierboven vermelde voorwaarden niet nageleefd werden.

8.5 Acties die worden Ondernomen naar aanleiding van Tekortkomingen

Indien afwijkingen vastgesteld worden, overhandigt de TSP een verslag aan de auditor. In dit verslag worden de maatregelen opgesomd die genomen zullen worden om de situatie recht te zetten en om wel overeenkomstig de voorwaarden te handelen. Indien de voorgestelde maatregelen als ontoereikend worden beschouwd, wordt overgegaan tot een tweede audit om de overeenkomstigheid te garanderen.

8.6 Meedelen van Resultaten

De mening van de auditor, die gestoeld is op de resultaten van de audits, zal over het algemeen beschikbaar zijn op aanvraag.

9 Andere Zakelijke en Wettelijke Kwesties

Zoals in dit hoofdstuk beschreven, zullen bepaalde wettelijke voorwaarden van toepassing zijn op de uitgifte van Burgercertificaten krachtens deze CPS.

9.1 Vergoedingen

9.1.1 Vergoedingen voor de Uitgifte of de Vernieuwing van Certificaten

Artikel 6 van de Wet van 19 juli 1991, vermeld onder punt 1.3 van hoofdstuk 1, regelt enerzijds de vergoeding voor het opnemen van de certificaten op de kaarten (art. 6, §5) en anderzijds de invordering van de kosten voor de aanmaak van de kaarten door de minister van Binnenlandse Zaken (art. 6, §8).

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

De CA biedt de burger gratis de volgende diensten:

- de Publicatie van CRL's en Delta-CRL's;
- toegang tot de wegpagina's van het archief;
- Webservice statusverificatie via archiefpagina's.

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

- certificaatvalidatie door middel van OCSP-status;
- downloaden van CRL's en Delta-CRL's;
- dienst voor verificatie van de certificaatstatus;
- certificaatdirectory
- de publicatie van certificaten;
- de intrekking van certificaten;
- de schorsing van certificaten.

De CA voert mechanismen in die voorkomen dat deze diensten misbruikt worden.

9.1.2 Bijdragen voor Toegang tot Certificaat

Zie sectie 9.1.1

9.1.3 Bijdrage voor Toegang tot Informatie over Herroeping of Statusinformatie

Zie sectie 9.1.1

9.1.4 Bijdragen voor Andere Diensten

Zie sectie 9.1.1

9.1.5 Terugbetalingsbeleid

Hoofdstuk is niet van toepassing.

9.2 Financiële Verantwoordelijkheid

De TSP is verantwoordelijk voor het houden van zijn financiële boeken en records in overeenstemming met de BGAAP en zal een beroep doen op de diensten van een internationaal boekhoudkantoor om financiële diensten te verlenen, met inbegrip van periodieke audits.

9.2.1 Verzekeringsdekking

De TSP verstrekt het Toezichthoudend Orgaan van de Belgische Federale Overheid elk jaar een bewijs van de verzekeringsdekkingen.

9.2.2 Andere Activa

De PKI factory en de Registratieautoriteiten zullen voldoende activa en financiële middelen aanhouden om hun taken te verrichten binnen de eID PKI en om redelijkerwijze in staat te zijn om hun aansprakelijkheid ten overstaan van Certificaathouders en Vertrouwende Partijen te dragen.

9.2.3 Verzekerings- of Garantiedekking voor "End-Entity's"

Hoofdstuk is niet van toepassing.

9.3 Vertrouwelijk Karakter van Zakelijke Informatie

In het kader van de geleverde diensten treedt de CA- en RA-operator (RRN) op als "verwerker" van persoonsgegevens, krachtens artikel 16 van de Wet van 8 December 1992, terwijl de gemeentebesturen optreden als “verwerker” voor de verwerking van persoonsgegevens.

9.3.1 Scope van Vertrouwelijke Informatie

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

- alle persoonlijke en identificeerbare informatie over burgers, verschillend van de informatie opgenomen in een certificaat;
- de precieze reden voor de intrekking of schorsing van een certificaat;
- audittrails;
- loginformatie met het oog op het opstellen van verslagen, zoals de logs van aanvragen door de RA;
- briefwisseling met betrekking tot de diensten van de CA;
- privésleutels van de CA.

9.3.2 Informatie Buiten de Scope van Vertrouwelijke Informatie

De volgende elementen zijn geen vertrouwelijke informatie:

- certificaten en hun inhoud;
- de status van een certificaat.

9.3.3 Verantwoordelijkheid om Vertrouwelijke Informatie te Beschermen

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 worden beveiligd tegen risico's en dat ze niet aan derden overgemaakt of bekendgemaakt worden.

Deze partijen zijn eveneens verplicht persoonlijke gegevens geheim te houden, overeenkomstig de wetgeving ter zake.

9.4 Privacy van Persoonlijke Informatie

9.4.1 Privacyplan

De TSP maakt geen vertrouwelijke informatie bekend of wordt niet gevraagd die bekend te maken zonder een geauthenticeerde 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 TSP en de Belgische Federale Overheid mag de TSP een administratieve vergoeding aanrekenen voor de verwerking van dergelijke openbaarmakingen.

9.4.2 Als Privé Behandelde Informatie

Alle informatie, d.w.z. over de Certificaathouders, wordt door de CA niet openbaar gemaakt aan burgers of vertrouwende partijen, met uitzondering van informatie over:

- henzelf;
- personen onder hun voogdij.

Alleen de RA heeft inzage in de vertrouwelijke informatie.

9.4.3 Informatie die niet als Privé wordt Beschouwd

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

- de status van een enkel certificaat wordt geleverd op aanvraag van een burger of vertrouwende partij;

- de burgers hebben inzage in de niet-vertrouwelijke informatie die de TSP over hen bewaart.
- De inhoud van uitgegeven Digitale Certificaten is openbare informatie en wordt niet als privé beschouwd.

9.4.4 Verantwoordelijkheid om Privé-Informatie te Beschermen

De CA beheert de openbaarmaking van informatie aan het personeel van de CA op een passende manier.

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 TSP 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 TSP, beschikt de RA ook over informatie met betrekking tot de Burgercertificaten, meer bepaald in het Register van de Identiteitskaarten. De Wet van 19 juni 1991 *regelt de toegang tot het Register van de Identiteitskaarten en andere gegevens over de burgers waarover het Rijksregister beschikt.*

9.4.5 Melding en Toestemming om Privé-Informatie te gebruiken

De TSP 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*. Dit is conform de wet van 13 juni 2005 *betreffende de behandeling van persoonsgegevens en de bescherming van de privacy in de sector van de elektronische communicatie.* En in het kader van de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming.

De TSP bewaart geen andere gegevens over certificaten van burgers 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 door de TSP verwerkte persoonsgegevens niet voor andere doeleinden gebruikt.

9.4.6 Bekendmaking Ingevolge een Gerechtelijke of Administratieve Procedure

Zie hoofdstuk 9.4.5

9.4.7 Andere Omstandigheden voor Bekendmaking van Informatie

Certipost heeft geen enkele verplichting om informatie bekend te maken buiten de verplichting ingevolge een legitiem en wettig gerechtelijk bevel dat voldoet aan de vereisten van deze CP/CPS.

9.5 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 CA, inclusief deze CPS, en behoudt zich die rechten voor.

De TSP is eigenaar van alle intellectuele eigendomsrechten die verband houden met de eigen infrastructuur, databases, website enz. en behoudt zich die rechten voor.

Alle software en documentatie ontwikkeld door de TSP in het kader van het project voor de Belgische Elektronische Identiteitskaart, is de exclusieve eigendom van de Belgische Federale Overheid.

9.6 Vertegenwoordigingen en Garanties

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

9.6.1 Vertegenwoordigingen en Garanties CA

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

- deze CPS en de amendementen ervan naleven, zoals gepubliceerd op https://repository.eid.belgium.be;
- een infrastructuur en certificatiediensten voorzien, inclusief de opstelling en werking van het opvraagcentrum en de website van de CA 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 privésleutel(s);
- elektronische certificaten uitgeven overeenkomstig deze CPS en de hierin vermelde plichten vervullen;
- de RA informeren indien de CA niet in staat is de toepassing te valideren overeenkomstig deze CPS;
- na ontvangst van een geauthenticeerde aanvraag van de RA, snel handelen om een certificaat uit te geven overeenkomstig deze CPS;
- na ontvangst van een geauthenticeerde aanvraag vanwege de RA tot intrekking van een certificaat, onmiddellijk handelen om het certificaat in te trekken overeenkomstig deze CPS;

- na ontvangst van een geauthenticeerde aanvraag vanwege de RA tot schorsing van een certificaat, snel handelen om het certificaat overeenkomstig deze CPS te schorsen;
- na ontvangst van een geauthenticeerde aanvraag vanwege de RA tot opheffing van schorsing van een certificaat, onmiddellijk handelen om de schorsing van het certificaat overeenkomstig deze CPS op te heffen;
- 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 CA met de Belgische Federale Overheid;
- een kopie maken van deze CPS en de van toepassing zijnde policy's die beschikbaar zijn op de website;
- handelen overeenkomstig de Belgische wetgeving. De TSP moet in het bijzonder tegemoetkomen aan alle wettelijke vereisten die verbonden zijn met het profiel van gekwalificeerde certificaten voortvloeiend uit de Europese Richtlijn 910/2014 met betrekking tot elektronische handtekeningen.

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

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

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

- het uitgeven van digitale certificaten die geen gegevens bevatten zoals voorgelegd door de RA;
- wanneer met een privésleutel van de CA geknoeid werd;
- het verzuim een 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 de hoofdstukken 9.3 en 9.4
- berantwoordelijk zoals gedefinieerd in 9.8.1

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

9.6.1.1 Vertrouwen op Eigen Risico

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

9.6.1.2 Juistheid van de Informatie

De TSP 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 TSP kan evenwel niet aansprakelijk gesteld worden buiten de limieten bepaald in artikel 9.8.1

9.6.2 Vertegenwoordigingen en Garanties RA

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

- correcte en precieze informatie leveren in de communicatie met de CA;
- ervoor zorgen dat de openbare sleutel afgeleverd aan de CA overeenkomt met de gebruikte privésleutel;
- certificaataanvragen creëren overeenkomstig deze CPS;
- alle controle- en authenticiteithandelingen uitvoeren die zijn voorgeschreven door de procedures van de CA en deze CPS;
- ce aanvraag van de kandidaat in een ondertekend bericht overmaken aan de CA;
- alle aanvragen tot intrekking, schorsing en opheffing van de schorsing van een certificaat ontvangen, controleren en overmaken aan de CA, overeenkomstig de CA-procedures en de CPS;
- de juistheid en authenticiteit controleren van de informatie die door de burger werd geleverd op het moment dat het certificaat wordt vernieuwd, overeenkomstig deze CPS.

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

Het RRN treedt op als enige RA in het domein van de CA en is als enige verantwoordelijk voor de directory's in zijn bezit, inclusief certificaatdirectory's. De RA is verantwoordelijk voor alle controles die ze uitvoert, de resultaten van deze controles en hieruit voortvloeiende aanbevelingen.

De RA is, via de LRA, als enige verantwoordelijk voor de juistheid van de burgergegevens 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 en is aansprakelijk voor de eigen daden en het eigen verzuim, overeenkomstig de Belgische wetgeving.

9.6.3 Vertegenwoordigingen en Garanties van de Abonnee

Tenzij anders vermeld in deze CPS, hebben de burgers onder meer de volgende plichten:

- een certificaat niet te vervalsen;
- certificaten alleen gebruiken voor wettelijke en toegestane doeleinden, overeenkomstig de CPS;

een nieuwe Elektronische Identiteitskaart (en dus Burgercertificaten) aanvragen in geval van wijzigingen aan de informatie die in het certificaat opgenomen is;

de openbare sleutel van de burger niet gebruiken om in het kader van een gepubliceerd Burgercertificaat andere certificaten te verkrijgen;

risico's, verlies, onthulling, wijziging of enig ander onbevoegd gebruik van de privésleutels te vermijden;

de politie, het gemeentebestuur of Docstop contacteren voor een aanvraag tot intrekking van een certificaat ingeval van een gebeurtenis die het vermoeden doet rijzen dat de materiële integriteit van het certificaat in het gedrang gekomen is. Met dergelijke gebeurtenissen wordt onder meer bedoeld: verlies, diefstal, wijziging, niet-geautoriseerde openbaarmaking of een andere aantasting van de privésleutel van een Burgercertificaat (of van beide);

de politie, het gemeentebestuur of Docstop contacteren voor een aanvraag tot intrekking van een certificaat, in geval van een gebeurtenis die de materiële integriteit van het certificaat in het gedrang brengt. Met dergelijke gebeurtenissen wordt onder meer bedoeld: het verlies, de diefstal, de wijziging, de niet-geautoriseerde openbaarmaking of een andere aantasting van de privésleutel van een Burgercertificaat (of van beide), of ingeval de controle van de privésleutels niet meer verzekerd is wegens het in gevaar brengen van de activeringsgegevens (bv. pincode);

verplichting er redelijk zorg voor te dragen dat er geen niet-geautoriseerd gebruik wordt gemaakt van de privésleutel van de abonnee;

na compromittering, de verplichting om onmiddellijk en definitief elk gebruik van de privésleutel te staken;

de verplichting om zo snel mogelijk te verwittigen indien de controle over de privésleutel verloren ging wegens het in gevaar brengen van de activeringsgegevens (bv. pincode);

9.6.4 Vertegenwoordigingen en Garanties Vertrouwende Partij

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 bijhorende voorwaarden voor vertrouwende partijen naleven;

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;

alleen vertrouwen stellen in certificaten tijdens de geldigheidsperiode als die niet geschorst of ingetrokken werden;

op een certificaat vertrouwen in de mate dat dat mogelijk is in de gegeven omstandigheden.

De vertrouwende partijen die toegang hebben tot de informatie die beschikbaar gesteld wordt in de CA-Archieven en op de website, hebben als enige 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 ze de RA-Helpdesk hiervan onmiddellijk op de hoogte brengen.

9.6.5 Vertegenwoordigingen en Garanties van andere Deelnemers

Verplichtingen van de Kaartproducent (CM): de Kaartproducent (CM) is verantwoordelijk voor de initialisatie, de personalisatie en de distributie van de elektronische identiteitskaart die de 0, 1 of 2 burgercertificaten bevat.

De initialisatie omvat de volgende verrichtingen in de smartcard:

- genereren van de sleutelparen voor de identificatie en handtekeningcertificaat;
- het opslaan van de identificatiegegevens, de identificatie en handtekeningcertificaten op de smartcard;
- de authenticatie van de gegevens, alsook de initialisatie van de verschillende bestanden die op de digitale identiteitskaart zijn opgeslagen.

De Kaartproducent zal op een veilige manier de basisdocumenten verzamelen en de oproepingsbrieven, de nieuwe gepersonaliseerde en de geïnitialiseerde digitale identiteitskaarten verdelen, alsmede de beveiligde brieven die bestemd zijn voor de burgers die de pin- en pukcode bevatten.

De Kaartproducent zal een beveiligd systeem invoeren voor de inzameling bij de gemeentebesturen van de vervallen of geannuleerde identiteitskaart en voor de vernietiging ervan.

9.7 Afwijzing van de Garanties

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

winstderving;

verlies van gegevens;

indirecte schade, gevolgschade 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.

9.8 Beperkingen van de Aansprakelijkheid

9.8.1 De aansprakelijkheid van de TSP

De aansprakelijkheid van de TSP ten opzichte van de burger of een vertrouwende partij beperkt zich tot het betalen van een schadevergoeding tot € 2 500 per transactie, beïnvloed door de evenementen opgesomd in het hoofdstuk hieronder.

9.8.2 Gekwalificeerde certificaten

Wat de uitgifte van de Gekwalificeerde Certificaten betreft, regelt artikel 14 van de Wet op de Elektronische Handtekeningen de aansprakelijkheid van de TSP.

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

a. de juistheid op het ogenblik van uitgifte van het gekwalificeerd certificaat van alle gegevens die erin opgenomen zijn en het feit dat het certificaat alle voorgeschreven gegevens voor een gekwalificeerd certificaat bevat;

b. de garantie dat de in het gekwalificeerd certificaat geïdentificeerde ondertekenaar op het tijdstip van de uitgifte van het certificaat houder was van de privésleutel die overeenstemt met de in het certificaat vermelde of geïdentificeerde publieke sleutel;

c. de garantie dat de privésleutel en de openbare sleutel complementair gebruikt kunnen worden.

De TSP is aansprakelijk voor schade toegebracht aan een entiteit of natuurlijke persoon of rechtspersoon die redelijkerwijs vertrouwen stelt in het certificaat, ingeval de intrekking van het certificaat niet geregistreerd werd, tenzij de TSP kan bewijzen dat hij niet nalatig geweest is.

9.8.3 Certificaten die niet als gekwalificeerd beschouwd kunnen 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 TSP.

De TSP wijst uitdrukkelijk elke aansprakelijkheid af ten opzichte van vertrouwende partijen, in alle gevallen waarin het Identiteitscertificaat gebruikt wordt in de context van toepassingen die het mogelijk maken om het Identificatiecertificaat te gebruiken voor het aanmaken van elektronische handtekeningen.

9.8.4 Uitgesloten Aansprakelijkheid

De TSP zal geenszins aansprakelijk kunnen worden gesteld voor verlies dat betrekking heeft op of voortkomt uit een (of meerdere) van de volgende omstandigheden of oorzaken:

- als het Digitaal Certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim in het gedrang is gekomen door de ongeoorloofde bekendmaking of het ongeoorloofde gebruik van het Digitaal Certificaat of een wachtwoord of activatiegegevens die worden gebruikt om de toegang hiertoe te controleren;

- als het Digitaal Certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim, werd uitgegeven als gevolg van enige misinterpretatie, feitelijke vergissing of nalatigheid van een persoon, entiteit of Organisatie;
- als het Digitaal Certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim, is vervallen of werd ingetrokken vóór de datum van de omstandigheden die aanleiding gaven tot de claim;
- als het Digitaal Certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim, werd gewijzigd of veranderd op welke manier dan ook, of op een andere manier werd gebruikt dan is toegestaan volgens de voorwaarden van deze Citizen CA CP/CPS en/of de relevante "Certificate Holder Agreement" of een toepasbare wet of reglementering;
- indien de privésleutel geassocieerd met het Digitaal Certificaat in het bezit van de eisende partij, of anders het voorwerp van een aanspraak, in het gedrang is gekomen;
- als het Digitaal Certificaat in het bezit van de eisende partij werd uitgegeven op een manier die een inbreuk betekent op een toepasbare wet of reglementering;
- computerhardware of -software, of wiskundige algoritmes, zijn ontwikkeld zodat ze openbaresleutelcryptografie of asymmetrische cryptosystemen onveilig maken, op voorwaarde dat Certipost commercieel redelijke praktijken hanteert ter bescherming tegen inbreuken op de beveiliging die voortkomen van dergelijke hardware, software of algoritmen;
- stroompanne, stroomonderbreking of andere stroomstoringen, op voorwaarde dat Certipost commercieel redelijke methodes gebruikt ter bescherming tegen dergelijke storingen;
- panne van een of meerdere computersystemen, communicatie-infrastructuur, verwerking, of opslagmedia of -mechanismen, of een subcomponent van de voorgaande, die niet onder de exclusieve controle van Certipost en/of zijn onderaannemers of dienstverleners vallen;
- een of meerdere van de volgende gebeurtenissen: een natuurramp of overmacht (met inbegrip van en zonder beperkt te zijn tot: overstroming, aardbeving, of enige andere natuurlijke of aan het weer gerelateerde omstandigheden); arbeidsverstoringen; oorlog, oproer of openlijke militaire vijandelijkheden; strijdige wetgeving of overheidsactie, verbod, embargo of boycot; onlusten of verstoring van het openbare leven; brand of ontploffing; catastrofale epidemie; handelsembargo; beperking of belemmering (met inbegrip van, maar niet beperkt tot exportcontroles); onbeschikbaarheid of niet-integriteit van telecommunicatie; met inbegrip van wettelijke verplichting, alle vonnissen van bevoegde rechterlijke instanties waaraan Certipost onderworpen is of kan zijn; en elke gebeurtenis of omstandigheid of reeks van omstandigheden die buiten de controle van Certipost vallen.

9.9 Schadevergoedingen

Zie hoofdstuk 9.8

9.10 Duur en Beëindiging van de CP/CPS

9.10.1 Duur

Deze CP/CPS wordt van kracht na publicatie in de eID Repository. Wijzigingen aan deze CP/CPS worden van kracht na publicatie in de eID Repository.

9.10.2 Beëindiging

Deze CPS blijft van kracht totdat de CA het tegendeel communiceert in haar repertorium op http://repository.eid.belgium.be.

9.10.3 Gevolgen van de Beëindiging en Overleving

De bepalingen van deze Citizen CA CP/CPS zullen de beëindiging of terugtrekking van een Certificaathouder of Vertrouwende Partij uit de eID PKI overleven wat betreft alle acties die zijn gebaseerd op het gebruik van of het vertrouwen op een Digitaal Certificaat of andere deelname binnen de eID PKI. Een dergelijke beëindiging of terugtrekking zal niet van dien aard zijn dat ze een recht of een rechtsmiddel zou benadelen of aantasten dat op een persoon zou rusten tot en met de datum van intrekking of beëindiging.

9.11 Individuele Mededelingen en Communicatie met Deelnemers

Mededelingen met betrekking tot deze CPS kunnen worden gericht aan:

Zie hoofdstuk 1.5.1

9.12 Wijzigingen

9.12.1 Procedure voor Wijzigingen

Aanpassingen aan deze CPS worden beheerd door het administratief beheer dat verantwoordelijk is voor de TSP. Alle voorgestelde wijzigingen aan de CPS moeten goedgekeurd worden door de “PKI management board”.

9.12.2 Kennisgevingsmechanisme en -Periode

Na goedkeuring wordt een nieuwe versie van de CPS aangemaakt en gepubliceerd naast de vorige versie op de repository-website (http://repository.eid.belgium.be).

9.12.3 Omstandigheden die Aanleiding Geven tot Wijziging OID

Minder belangrijke aanpassingen aan deze CPS die geen materiële invloed hebben op het zekerheidsniveau van deze CPS, worden aangeduid met een andere decimaal (bv. versie 1.0 verandert in versie 1.1), terwijl belangrijke aanpassingen aan deze CPS worden aangeduid met een ander geheel getal (bv. versie 1.0 verandert in versie 2.0).

Minder belangrijke aanpassingen aan deze CPS hoeven niet veranderd te worden in de CPS OID of de CPS-index (URL) die aan de CA 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 dienovereenkomstig aangepast worden.

9.13 Bepalingen voor het Oplossen van Geschillen

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

Klachten die verband houden met deze CPS en de certificaten moeten gericht worden aan:

Zie hoofdstuk 1.5.1

Een ontvangstbevestiging wordt binnen de 2 werkdagen na aankomst van de klacht verstuurd. Een antwoord wordt verschaft binnen 10 werkdagen na aankomst van de klacht.

In overeenstemming met de Belgische wet op de Digitale Handtekeningen, zal elke arbitrage, behoudens anders overeengekomen tussen de partijen, plaatshebben in België.

9.14 Toepasselijk Recht

De TSP levert zijn diensten overeenkomstig de bepalingen van de Belgische Wetgeving en de Europese Richtlijn 910/2014.

9.15 Naleving van de Toepasselijke Wetgeving

Deze CP/CPS is onderworpen aan de toepasselijke wetgeving.

9.16 Diverse bepalingen

De TSP 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 Burgercertificaat;
- 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.

9.16.1 Volledige Overeenkomst

Hoofdstuk is niet van toepassing

9.16.2 Overdracht

Hoofdstuk is niet van toepassing

9.16.3 Deelbaarheid

Elke bepaling van deze Citizen CA CP/CPS waarvan wordt bepaald dat ze ongeldig of onafdwingbaar is, zal ineffectief zijn in de mate van die bepaling, zonder dat dit de overige bepalingen van deze Citizen CA CP/CPS ongeldig maakt of zonder dat dit de geldigheid of de afdwingbaarheid van die overige bepalingen aantast.

9.16.4 Handhaving (Vergoedingen Advocaten en Afstand van Rechten)

Als de TSP enig recht, enige bevoegdheid, enig voorrecht of enig rechtsmiddel dat door deze Citizen CA CP/CPS op welke manier dan ook aan haar wordt verleend, niet of met vertraging uitoefent of afdwingt, dan wordt dat niet beschouwd als een afstand van enig zulk recht of dan zal hierdoor de uitoefening of handhaving ervan op geen enkel ogenblik worden verhinderd, noch zal de eenmalige of gedeeltelijke uitoefening van zulk recht, bevoegdheid, voorrecht of rechtsmiddel een andere of de verdere uitoefening ervan of de uitoefening van een ander recht of rechtsmiddel uitsluiten. Afstand doen moet schriftelijk gebeuren, op straffe van ongeldigheid. Geen enkel recht of rechtsmiddel dat wordt verleend krachtens een van de bepalingen van deze Citizen CA CP/CPS is bedoeld om andere rechten of rechtsmiddelen uit te sluiten, behalve indien uitdrukkelijk bepaald in deze Citizen CA CP/CPS, en elk recht en rechtsmiddel zal cumulatief zijn en komt bovenop elk ander recht of rechtsmiddel dat nu of hierna wordt gegeven en dat bestaat in recht en billijkheid of bij verordening of anderszins.

9.16.5 Overmacht

De TSP aanvaardt geen aansprakelijkheid voor het niet-naleven van de garantie of het niet of niet tijdig nakomen van de verplichtingen als gevolg van gebeurtenissen die niet onder haar controle vallen, zoals overmacht, oorlogsdaden, terreurdaden, epidemieën, stroomuitval of uitvallen van de telecommunicatiediensten, brand en andere natuurrampen. Zie ook Hoofdstuk 9.8.2 (Uitgesloten Aansprakelijkheid) hiervoor.

9.17 Andere bepalingen

Hoofdstuk is niet van toepassing.

Bijlagen

This page is intentionally left blank

Bijlage A

Definities en Acroniemen

CA	Certificatieautoriteit (Certification Authority)
CC	Common Criteria
CM	Kaartproducent (Card Manufacturer)
CP	Certificaatpolicy (Certificate Policy)
CPS	Verklaring Certificatiepraktijk (Certification Practice Statement)
CRL	Lijst met Ingetrokken Certificaten (Certificate Revocation List)
EAL	Evaluatie Zekerheidsniveau (Evaluation Assurance Level)
eIDAS	Europese Richtlijn 910/2014, ook Richtlijn inzake Identificatie en Handtekening genoemd (eIDentification And Signature)
OID	Objectidentificator (Object Identifier)
(L)RA	(Lokale) Registratieautoriteit (Registration Authority)

Bijlage B

VEREISTEN VOOR CERTIFICATIEAUTORITEITEN

De door de CA's gebruikte cryptomodules DIENEN TE worden geëvalueerd en gecertificeerd in overeenstemming met een van de volgende standaarden:

- FIPS PUB 140-2 Niveau 3 of hoger
- PP-SSCD 4,5,6
- BSI Cryptographic Modules Security Level “Enhanced”

Appendix C

ISSUING CAs EID-HIËRARCHIE CERTIFICAATPROFIEL GEËXTRAHEERD UIT EID-DEL-004

Vanaf volgende pagina

Table of contents

1. Certificate profiles

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

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

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

1.1. Version

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

Version	
All certificates	Version 3 – Value = "2"

1.2. Certificates Serial Number

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

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

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

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

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

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

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

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

1.3. Signature

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

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

1.4. Issuer

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

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

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

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

1.5. Validity

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

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

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

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

[5] Certificate validity periods defined during key ceremony.

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

	>=2014	10y 3m
Foreigner	>=2006 >=2015	5y 3m 10y 3m

1.6. Subject

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

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

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

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

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

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

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

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

1.7. Subject Public Key Info

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

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

1.8. Key usage

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

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

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

1.9. Extended Key usage

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

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

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

1.10. Authority and Subject Key Identifiers

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

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

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

1.11. NetscapeCertType

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

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

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

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

1.12. Policy mapping

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

1.13. Policy constraint

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

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

1.14. Certificate policies

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

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

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

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

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

Certificate Policies				
	Policy Identifier	Policy Qualifiers	Policy Qualifier Id	Qualifier
eID hierarchy				
Operational CA certificates				
Citizen CA	2.16.56.1.1.1.2 2.16.56.9.1.1.2 2.16.56.10.1.1.2 2.16.56.12.1.1.2	NA	CPS	https://repository.eid.belgium.be
Foreigner CA	2.16.56.1.1.1.7 2.16.56.9.1.1.7 2.16.56.10.1.1.7 2.16.56.12.1.1.7	NA	CPS	https://repository.eid.belgium.be
End user certificates				
Citizen Authentication certificate	2.16.56.1.1.1.2.2 2.16.56.9.1.1.2.2 2.16.56.10.1.1.2.2 2.16.56.12.1.1.2.2	NA	CPS	https://repository.eid.belgium.be
Citizen Signature certificate	2.16.56.1.1.1.2.1 2.16.56.9.1.1.2.1 2.16.56.10.1.1.2.1 2.16.56.12.1.1.2.1	NA	CPS	https://repository.eid.belgium.be

Foreigner Authentication certificate	2.16.56.1.1.1.7.2 2.16.56.9.1.1.7.2 2.16.56.10.1.1.7.2 2.16.56.12.1.1.7.2	NA	CPS	https://repository.eid.belgium.be
Foreigner Signature certificate	2.16.56.1.1.1.7.1 2.16.56.9.1.1.7.1 2.16.56.10.1.1.7.1 2.16.56.12.1.1.7.1	NA	CPS	http://repository.eid.belgium.be

1.15. Basic constraint

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

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

1.16. CRL Distribution Point

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

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

1.17. Freshest CRL - Delta CRL Distribution Point

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

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

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

1.18. Authority Information Access

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

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

[10] See paragraph 4.2 CRL and delta CRL names

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

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

1.19. Subject Directory attributes

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

No subject directory attributes will be present in the eID certificates

1.20. Qualified Certificate Statement

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

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

2. CRL profiles

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

2.1. CRL Profile

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

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

2.2. Δ CRL Profile

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

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

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

2.3. CRL Issuance Frequency

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

3. CA configuration settings

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

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

3.1. Auto-revocation

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

3.2. Unique DN check

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

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

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

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

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

3.3. Variable validity

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

The variable validity feature is only available through XKMS interface.

3.4. Delta CRL

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

4. Naming conventions

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

4.1. Serial number to reference a CA

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

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

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

4.2. CRL and delta CRL names

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

4.3. CA certificate file names

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