



Isabel Policy van de Certificatie-Activiteiten

versie 1.1

Publicatiedatum: 30 juni 2003

Ingangsdatum: 1 juli 2003

© Auteursrechten Isabel 2003. Alle rechten voorbehouden.

Niets van deze uitgave mag worden gereproduceerd, opgeslagen in een database of een storage- en retrievalsysteem, uitgegeven of aan anderen worden doorgegeven in welke vorm ook, elektronisch of mechanisch, met inbegrip van afdrukken, fotokopieën of microfilms, zonder voorafgaande schriftelijke goedkeuring van Isabel NV./S.A.

INHOUD

INHOUD	2
1. INLEIDING	6
1.1. Overzicht	6
1.2. Identificatie	6
1.2.1. Naam	6
1.2.2. Object Identifier	6
1.2.3. Uniform Resource Identifier	7
1.2.4. Historiek van de documentversies	7
1.3. Gemeenschap en toepasbaarheid	7
1.3.1. Certificatieautoriteiten	7
1.3.2. Registratieautoriteiten	7
1.3.3. Eindgebruikers	7
1.3.4. Validatieautoriteiten	8
1.3.5. Policy-autoriteiten	8
1.3.6. Toepasbaarheid	8
1.3.7. Contactgegevens	9
2. ALGEMENE BEPALINGEN	10
2.1. Verplichtingen	10
2.1.1. Verplichtingen van Isabel Certificatieautoriteiten	10
2.1.2. Verplichtingen van Isabel-RA's	14
2.1.3. Verplichtingen van de Abonnee en Houder van een Isabel-certificaat	16
2.1.4. Verplichtingen van de Vertrouwende Partij	19
2.1.5. Verplichtingen inzake Repository	20
2.1.6. Verplichtingen van de Validatieautoriteit	20
2.1.7. Verplichtingen van de Policy-autoriteit	20
2.1.8. De juridische entiteit Isabel	20
2.1.9. Isabel Revocatie Service	21
2.2. Aansprakelijkheid	22
2.3. Financiële verantwoordelijkheid	23
2.3.1. Schadevergoeding door Isabel-Certificaatabonnees, Vertrouwende Partijen en Houders	23
2.3.2. Vertrouwelijke Relaties	23
2.3.3. Administratief proces	23
2.4. Interpretatie en uitvoering	23
2.4.1. Toepasselijke wetten	23
2.4.2. Verwijdering, voortbestaan, fusie, berichtgeving	24
2.4.3. Procedures voor het oplossen van geschillen	24
2.5. Vergoedingen	24
2.6. Publicatie en repository	24
2.6.1. Publicatie van informatie van een Isabel-CA	24
2.6.2. Frequentie van de publicaties	25
2.6.3. Toegangscontrole	25
2.6.4. Repository's	25
2.7. Conformiteitsaudits	25

2.7.1.	Frequentie van de conformiteitsaudits voor een entiteit	26
2.7.2.	Identiteit/kwalificatie van de auditors	26
2.7.3.	De relatie van de auditors met de partij die aan een audit onderworpen wordt	26
2.7.4.	Voorwerp van de audit	26
2.7.5.	Te nemen acties bij gebreken	26
2.7.6.	Mededeling van de resultaten	26
2.8.	Vertrouwelijk karakter	27
2.8.1.	Categorieën informatie die vertrouwelijk moeten blijven	27
2.8.2.	Categorieën informatie die als niet-vertrouwelijk worden aanzien	27
2.8.3.	Bekendmaking van informatie over de Herroeping van Certificaten	27
2.8.4.	Bekendmaking aan Gerechtelijke ambtenaren	27
2.8.5.	Bekendmaking als onderdeel van een burgerrechtelijk onderzoek	27
2.8.6.	Bekendmaking op verzoek van de Abonnee/Houder	28
2.9.	Andere omstandigheden waarin informatie bekend wordt gemaakt	28
2.10.	Intellectuele eigendomsrechten	28
3.	IDENTIFICATIE EN AUTHENTIFICATIE	29
3.1.	Eerste registratie	29
3.1.1.	Soorten namen	29
3.1.2.	Verplicht gebruik van betekenisvolle namen	29
3.1.3.	Regels voor het interpreteren van verschillende naamformaten	29
3.1.4.	Uniek karakter van de namen	30
3.1.5.	Procedure voor het oplossen van geschillen in verband met namen	30
3.1.6.	Herkenning, authenticatie en rol van handelsmerken	30
3.1.7.	Methode om het bezit van een Private Sleutel te bewijzen	30
3.1.8.	Authenticatie van de identiteit van een organisatie	31
3.1.9.	Authenticatie van de individuele identiteit	31
3.2.	Herstarten van de certificatieprocedure	32
3.2.1.	Automatische hernieuwing van het Isabel-certificaat	32
3.2.2.	Hernieuwing van het sleutelpaar	33
3.2.3.	Hernieuwing van de Isabel Secure Signing Card	33
3.3.	Herstarten certificatieprocedure na herroeping	33
3.4.	Aanvraag voor herroeping	33
3.4.1.	Authenticatie door de Isabel-RA	33
3.4.2.	Authenticatie door een Isabel Revocatie Service	34
3.4.3.	Authenticatie door de Isabel-CA	34
4.	OPERATIONELE BEPALINGEN	36
4.1.	Aanvraag certificaat	36
4.1.1.	Aanvraag van een Isabel-certificaat voor een nieuwe Houder	36
4.1.2.	Aanvraag van een Isabel-certificaat voor een bestaande Houder	37
4.2.	Uitgifte certificaat	37
4.2.1.	Gecentraliseerde Certificatieprocedure	37
4.2.2.	Gedecentraliseerde Certificatieprocedure	37
4.2.3.	Manuele Certificatieprocedure	38
4.3.	Aanvaarding certificaat	38
4.3.1.	Gecentraliseerde Certificatieprocedure	38
4.3.2.	Gedecentraliseerde Certificatieprocedure	39
4.3.3.	Manuele Certificatieprocedure	39
4.4.	Herroeping Certificaat	39

4.4.1.	Omstandigheden voor Herroeping	39
4.4.2.	Wie kan Herroeping aanvragen	39
4.4.3.	Procedure voor Herroepingsaanvraag	40
4.4.4.	Uitstel Herroepingsaanvraag	40
4.4.5.	Omstandigheden voor opschorting	40
4.4.6.	Uitgiftefrequentie CRL	40
4.5.	Security audit procedures	40
4.5.1.	Soorten gebeurtenissen die worden geregistreerd	40
4.5.2.	Frequentie van het verwerken van de logs	41
4.5.3.	Bewaarperiode voor de audit log	41
4.5.4.	Bescherming van audit logs	41
4.5.5.	Back-upprocedures audit log	41
4.5.6.	Collection Systeem audit (intern versus extern)	41
4.5.7.	Kennisgeving aan de houder die een gebeurtenis veroorzaakt	41
4.5.8.	Beoordeling zwakke punten	41
4.6.	Archiveren van gegevens	42
4.6.1.	Soorten gebeurtenissen die worden geregistreerd	42
4.6.2.	Bewaarperiode archieven	42
4.6.3.	Beveiliging van de archieven	42
4.6.4.	Back-upprocedures archieven	42
4.6.5.	Vereisten voor het dateren van gegevens	42
4.6.6.	Collection systeem (intern versus extern)	42
4.6.7.	Procedures om gearchiveerde informatie te verkrijgen en te controleren	42
4.7.	Sleutel changeover	43
4.8.	Compromittering en disaster recovery	43
4.9.	Stopzetting CA	43
5.	FYSIEKE, PROCEDURE- EN PERSONEELSMATREGELEN I.V.M. DE VEILIGHEID	44
5.1.	Fysieke maatregelen	44
5.2.	Procedurele maatregelen	44
5.2.1.	Vertrouwelijke functies en verantwoordelijkheden	44
5.2.2.	Identificatie en authenticatie voor elke functie	44
5.3.	Personeelscontroles	44
6.	TECHNISCHE VEILIGHEIDSMATREGELEN	45
6.1.	Aanmaken en installeren van het sleutelpaar	45
6.1.1.	Aanmaken en afleveren van de sleutel	45
6.1.2.	Lengte van de sleutels	45
6.1.3.	Aanmaken van de sleutels	45
6.2.	Bescherming van de Private Sleutel	45
6.2.1.	Standaarden voor versleutelingsmodules	45
6.2.2.	Private Sleutel (n van m) multipersonencontrole	45
6.2.3.	Escrow Private Sleutel	46
6.2.4.	Back-up Private Sleutel	46
6.2.5.	Archiveren Private Sleutel	46
6.2.6.	Invoeren Private Sleutel in een versleutelingsmodule	46
6.2.7.	Methode om een Private Sleutel te activeren	46
6.2.8.	Methode om een Private Sleutel te desactiveren	46
6.2.9.	Methode om een Private Sleutel te vernietigen	46
6.3.	Andere aspecten van het beheer van sleutelparen	47

6.4. Activeringsgegevens	47
6.5. Beveiligingscontroles computer	47
6.6. Levenscyclus technische maatregelen	47
6.7. Netwerkbeveiligingsmaatregelen	47
6.8. Maatregelen engineering versleutelingsmodule	47
7. CERTIFICATEN- EN CRL-PROFIELEN	48
7.1. Certificatenprofiel	48
7.1.1. Versienummer	49
7.1.2. Certificaatextensies	49
7.1.3. Algoritme object identifiers	50
7.1.4. Naamvormen	51
7.1.5. Naambeperkingen	51
7.1.6. Object Identifier Certificaatpolicy	51
7.1.7. Gebruik van de extensie Policy constraints	51
7.1.8. Syntax en semantiek voor de Policy qualifiers	51
7.1.9. Semantiek voor de verwerking van de kritieke extensie certificaatpolicy	51
7.2. CRL/ARL-profiel	52
7.2.1. Versienummer	52
7.2.2. CRL/ARL en CRL/ARL extensies	52
8. SPECIFICATIE ADMINISTRATIE	53
8.1. Specificatie wijzigingsprocedures	53
8.2. Publicatie en mededeling policies	53
8.3. Goedkeuringsprocedures voor CPS	53
9. BIJLAGEN	54
9.1. Bijlage A – Definities	54
9.1.1. Letterwoorden	54
9.1.2. Woordenlijst	55
9.2. Bijlage B – Referenties	58

1. INLEIDING

Het vertrouwen dat wordt gesteld in een digitaal certificaat steunt op de regels die worden gevolgd om dit certificaat uit te geven en te beheren. Deze regels worden geformaliseerd in policy-documenten: de Certificaatpolicy (CP) en de Policy van de Certificatie-Activiteiten (CPS – Certification Practice Statement).

De ITU-T X.509-standaard definieert een CP als “Een reeks regels die aangeven wanneer een certificaat van toepassing is op een bepaalde gemeenschap en/of categorie met gemeenschappelijke veiligheidsvereisten”.

De term CPS wordt door de American Bar Association Guidelines gedefinieerd als: "Een policy van de activiteiten die een CA verricht voor de uitgifte van certificaten."

1.1. OVERZICHT

De onderhavige Isabel-CPS bevat de verplichtingen, praktijken en procedures die de Isabel Certificatieautoriteit (CA), de Registratieautoriteiten (RA's), de Isabel Klanten, de Isabel-certificaat Houders en de Vertrouwende Partijen ondernemen in het raam van de toepassing, de uitgifte, de acceptatie, het gebruik en de herroeping van Isabel-certificaten.

Een Isabel-certificaat is een certificaat dat werd uitgegeven door een Isabel-CA.

Deze Isabel-CPS is gebaseerd op de Internet Engineering Task Force (IETF) RFC 2527: 'Internet X.509 Public Key Infrastructure – CP and CPS Framework – March 1999' die een standaard en een internationaal erkend kader biedt voor Certificaatpolicy's en Policy's van de Certificatie-Activiteiten.

De onderhavige CPS is zodanig gestructureerd dat vanuit dit document kan worden verwezen naar meer dan één CP.

Elke CP kan meer specifieke vereisten bevatten met betrekking tot het specifieke certificaat dat eraan is onderworpen. Als meer specifiek document zal de toepasselijke CP voorrang hebben op de onderhavige CPS.

De toepasselijke CP zal, in combinatie met de onderhavige CPS, worden gebruikt door de Vertrouwende Partij om het niveau van de veiligheid en de betrouwbaarheid te bepalen dat kan worden toegekend aan een Isabel-certificaat.

Deze CPS en de bijhorende CP's zullen eveneens onderworpen zijn aan overeenkomsten die werden gesloten tussen een Isabel-CA en klanten van Isabel. De CP en de CPS zullen voorrang hebben op de overeenkomsten die werden gesloten tussen een Isabel-CA en een klant van Isabel, tenzij anders overeengekomen.

Naar deze CPS zal worden verwezen als volgt : Isabel-CPS v. [versienummer], sectie [nummer].

1.2. IDENTIFICATIE

1.2.1. NAAM

Deze CPS wordt “Policy van de Certificatie-Activiteiten van Isabel” genoemd.

1.2.2. OBJECT IDENTIFIER

De Object Identifier van de “Policy van de Certificatie-Activiteiten van Isabel” is 2.16.56.1.9.3.

1.2.3. UNIFORM RESOURCE IDENTIFIER

De Isabel-CPS is toegankelijk voor het publiek op de website van Isabel op de volgende URL: <http://www.isabel.be/PKI/Policies/Standard.htm>

1.2.4. HISTORIEK VAN DE DOCUMENTVERSIES

Historiek van de documentversies bevindt zich in het document [15] dat toegankelijk is voor het publiek op de volgende URL: <http://www.isabel.be/PKI/Policies/Standard.htm>

1.3. GEMEENSCHAP EN TOEPASBAARHEID

1.3.1. CERTIFICATIEAUTORITEITEN

Deze CPS heeft tot doel een policy te geven van de activiteiten die de Isabel Certificatieautoriteit binnen de Isabel Infrastructuur voor Publieke Sleutels ("Isabel PKI") verricht bij de uitgifte en het beheer van Isabel-certificaten. De toepasbaarheid wordt beschreven in de betreffende CP.

Volgens ITU-T X.509 is een CA "een autoriteit waarin een of meerdere gebruikers hun vertrouwen stellen voor het aanmaken en toekennen van certificaten; eventueel kan de CA ook de sleutel van de gebruiker aanmaken". Een Isabel-CA die certificaten uitgeeft in overeenstemming met deze CPS, moet deze CPS en de toepasselijke CP's respecteren.

In de Isabel Infrastructuur voor Publieke Sleutels kan een Isabel-CA Aanvragen voor Isabel-certificaten accepteren voor Houders van Isabel-certificaten wiens identiteit werd geauthenticeerd door een Isabel-RA.

Na controle van de certificaataanvraag geeft de Isabel-CA een Isabel-certificaat uit dat de identiteit van de Houder van het Isabel-certificaat verbindt met zijn/haar Publieke Sleutel.

Alleen door Isabel erkende Certificatieautoriteiten mogen Isabel-certificaten uitgeven. Isabel publiceert een lijst van erkende Certificatieautoriteiten op haar website <http://www.isabel.be>.

1.3.2. REGISTRATIEAUTORITEITEN

Volgens RFC 2527 is een RA "een entiteit die verantwoordelijk is voor de identificatie en authenticatie van Houders van certificaten, die echter geen certificaten ondertekent of uitgeeft".

In de Isabel Infrastructuur voor Publieke Sleutels accepteren RA's die werken onder toezicht en gezag van een Isabel-CA, Aanvragen voor Isabel-certificaten van Isabel-certificaatabonnees.

De RA's moeten de identiteit van de Houder van een Isabel-certificaat authenticeren en moeten de informatie in de Aanvraag voor een Isabel-certificaat controleren aan de hand van deze CPS en de toepasselijke CP's, en van hun interne procedures. Als de gecontroleerde informatie correct is, stuurt de Isabel-RA een Aanvraag voor een Isabel-certificaat naar de aangewezen Isabel-CA, die het Isabel-certificaat uitreikt aan de Houder van het Isabel-certificaat.

Alleen door Isabel erkende Registratieautoriteiten mogen certificaataanvragen indienen bij een Isabel-CA voor het uitgeven van Isabel-certificaten. Isabel publiceert een lijst van erkende Registratieautoriteiten op haar website <http://www.isabel.be>.

1.3.3. EINDGEBRUIKERS

In het kader van onderhavige Isabel-CPS en conform de toepasselijke CP, bestaan de eindgebruikers in de Infrastructuur van Isabel voor Publieke Sleutels uit:

1. Isabel-Certificaatabonnee
2. Houder van het Isabel-certificaat
3. Vertrouwende Partij bij het Isabel-certificaat

Het 'Subject' attribuut in het Isabel-certificaat wordt aangewend om de Houder van het Isabel-certificaat te benoemen of op een andere wijze te identificeren met:

1. Een naam en voornaam voor een Houder 'Natuurlijke persoon'.
2. Een functiebenaming voor een Houder 'Functie'.
3. Een naam van een applicatie voor een Houder 'Applicatie'.

Binnen het raam van onderhavige Isabel-CPS :

1. mag een eindgebruiker geen CA of RA zijn binnen de Infrastructuur van Isabel voor Publieke Sleutels,
2. is een handtekening van een Houder 'Functie' een technische handtekening, m.a.w. deze mag enkel gebruikt worden voor integriteitdoeleinden, en niet voor transactie autorisatie.

1.3.4. VALIDATIEAUTORITEITEN

In de Isabel Infrastructuur voor Publieke Sleutels geeft een Isabel-Validatieautoriteit elke Vertrouwende Partij de mogelijkheid om informatie te bekomen over de status van de herroeping van Isabel-certificaten.

De Lijsten met Herroepingen van de Certificaten (Certificate Revocation Lists – CRL's) met de serienummers van de herroepen Isabel-certificaten, alsook de herroepen Isabel-certificaten worden gepubliceerd in de Isabel Directory.

Het On-Line Protocol voor de Status van het Certificaat (On-Line Certificate Status Protocol - OCSP) verschaft informatie over de herroeping van Isabel-certificaten.

Via de Isabel website is ondersteuning voorzien voor de verificatie van de revocatie status van individuele certificaten.

1.3.5. POLICY-AUTORITEITEN

Een Policy-autoriteit is de entiteit die verantwoordelijk is voor:

1. De specificatie, validatie en publicatie van de Isabel-CP's en hun herzieningen.
2. De specificatie, validatie en publicatie van onderhavige Isabel-CPS en zijn herzieningen.
3. Het bepalen van de geschiktheid en de correcte implementatie van de Isabel-CPS en de Isabel-CP's.
4. Het definiëren van de herzieningsvereisten en –processen met betrekking tot de implementatie van de CPS en CP's.

De Policy-autoriteit voor onderhavige Isabel-CPS is de Isabel Security Manager.

1.3.6. TOEPASBAARHEID

De Isabel-certificaten die werden uitgegeven in overeenstemming met onderhavige CPS mogen alleen worden gebruikt door Vertrouwende Partijen die behoren tot een klant van Isabel én enkel voor de volgende doeleinden: elektronische handtekening controleren, onmogelijkheid om elektronische handelingen te ontkennen ("non-repudiation"), codeersleutels en codeergegevens.

De Isabel-certificaten mogen niet worden gebruikt door Vertrouwende Partijen die vertrouwen op een Isabel-certificaat en die niet behoren tot een klant van Isabel.

Als een Houder van een Isabel-certificaat beperkingen wenst (financiële of andere) voor transacties die worden geauthenticeerd door het Isabel-certificaat, moet deze Houder beschikken over een ondertekende overeenkomst met elke Partij die vertrouwt op het Isabel-certificaat, waarin zij zich akkoord verklaart met deze beperkingen.

1.3.7. CONTACTGEGEVENS

1.3.7.1. ADMINISTRATIE VAN DE SPECIFICATIES

De Security Manager van Isabel treedt op als Policy-autoriteit voor onderhavige Isabel-CPS. Zij is verantwoordelijk voor alle aspecten van onderhavige Isabel-CPS, inclusief de specificatie, validatie, registratie, publicatie, het onderhoud en de interpretatie.

1.3.7.2. CONTACTPERSOON POLICY-AUTORITEIT

Alle vragen en opmerkingen in verband met onderhavige Isabel-CPS moeten worden gericht aan de vertegenwoordiger van de Policy-autoriteit:

Isabel NV/SA
Isabel Security Manager
Keizerinlaan / Bd de l'Impératrice 13-15
B-1000 Brussels
Belgium
Tel: +32 (0)2/545.17.11
Fax: +32 (0)2/545.17.19
E-mail: policyauthority@isabel.be
Web: www.isabel.be

1.3.7.3. PERSOON DIE BESLIST OVER DE GESCHIKTHEID VAN DE CPS VOOR DE POLICY

De Isabel Security Manager bepaalt of de Isabel-CPS geschikt is voor de Isabel-CP's.

2. ALGEMENE BEPALINGEN

2.1. VERPLICHTINGEN

Deze sectie beschrijft de verplichtingen van de entiteiten binnen de Isabel PKI in verband met de aanvraag, uitgifte, aanvaarding, het gebruik, de publicatie en de herroeping van Isabel-certificaten.

De Vertrouwende Partijen moeten de bepalingen in deze sectie begrijpen vooraleer zij vertrouwen op een Isabel-certificaat.

Deze entiteiten zijn:

1. Isabel-CA
2. Isabel-RA's
3. Abonnees en Houders van Isabel-certificaten
4. Vertrouwende Partijen
5. Isabel Repository
6. Isabel Policy-autoriteit
7. De juridische entiteit Isabel
8. Isabel Revocatie Service

Door een uitgegeven Isabel-certificaat te aanvaarden, aanvaardt een Houder van een Isabel-certificaat de hiernavolgende verplichtingen en bepalingen.

Door gebruik te maken van een Isabel-certificaat aanvaardt de, op een Isabel-certificaat Vertrouwende Partij, de hierna beschreven verplichtingen en bepalingen.

2.1.1. VERPLICHTINGEN VAN ISABEL CERTIFICATIEAUTORITEITEN

Elke CA binnen de Isabel Infrastructuur voor Publieke Sleutels heeft de volgende verplichtingen:

2.1.1.1. NALEVING VAN DE STANDAARDEN

Een Isabel-CA die Isabel-certificaten uitgeeft dient erop toe te zien dat ze alle vereisten die worden vermeld in onderhavige Isabel-CPS en alle vereisten uit de toepasselijke Isabel-CP worden nageleefd. Meer bepaald moeten de uitgegeven Isabel-certificaten beantwoorden aan standaard X.509 versie 3.

2.1.1.2. CORRECTHEID VAN DE VERKLARINGEN

Door een Isabel-certificaat te publiceren in de Repository, garandeert een Isabel-CA aan al wie redelijkerwijze vertrouwt op de informatie in een Isabel-certificaat dat werd uitgegeven onder deze Isabel-CPS, dat het Isabel-certificaat werd verstrekt aan de Houder van het Isabel-certificaat conform de bepalingen in onderhavige Isabel-CPS en in de toepasselijke Isabel-CP. Zij garandeert tevens dat de Houder van het Isabel-certificaat zijn/haar Isabel-certificaat heeft aanvaard onder de beperkingen die worden vermeld in sectie "4.3 – Aanvaarding certificaat".

2.1.1.3. VERWERKING AANVRAGEN I.V.M. CERTIFICATEN

Een Isabel-CA dient Aanvragen in verband met Isabel-certificaten die onder haar toezicht door een Isabel-RA werden uitgegeven tijdig en veilig te verwerken. De Isabel-CA mag enkel Isabel-RA's gebruiken die formeel zijn goedgekeurd door de Isabel-CA.

Voor het verwerken van Aanvragen in verband met Isabel-certificaten, moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie "3.1 – Eerste registratie" en "3.2 – Herstarten van de certificatieprocedure" en in sectie "4.1 – Aanvraag certificaat" van onderhavige Policy van de Certificatie-Activiteit.

2. elke toepasselijke CP.

De CA moet elke aanvraag in verband met certificaten dat niet lijkt te voldoen aan de bepalingen van deze CPS en/of toepasselijke CP, verwerpen.

2.1.1.4. SLEUTELPAAR GENEREREN VOOR DE HOUDER VAN HET ISABEL-CERTIFICAAT

Als de Isabel-CA het sleutelpaar genereert voor de Houder van het Isabel-certificaat, moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie "6.1 – Aanmaken en installeren van het sleutelpaar" van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

2.1.1.5. VERKRIJGEN VAN HET BEWIJS VAN BEZIT VAN DE PRIVATE SLEUTEL

Indien het sleutelpaar werd gegenereerd door de Houder van het Isabel-certificaat, moet de Isabel-CA de combinatie van een Publiek/Privaat sleutelpaar valideren, samen met de identiteit van de Houder; daartoe dient zij van de Houder een bewijs van bezit van de Private sleutel te verkrijgen die aan de te certificeren Publieke sleutel verbonden is.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie "3.1.7 – Methode om het bezit van een Private Sleutel te bewijzen" van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

2.1.1.6. HET UNIEKE KARAKTER VAN EEN SLEUTELPAAR BINNEN DE ISABEL-PKI GARANDEREN

Een Isabel-CA garandeert het unieke karakter van een sleutelpaar binnen de Isabel PKI, ongeacht of het sleutelpaar werd gegenereerd door de Houder van het Isabel-certificaat, of door een Isabel-CA voor de Houder van het Isabel-certificaat.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie "6.1 – Aanmaken en installeren van het sleutelpaar" van onderhavige Isabel-CPS.
2. Elke toepasselijke CP.

2.1.1.7. UITGIFTE VAN EEN ISABEL-CERTIFICAAT

Een Isabel-CA binnen de Isabel PKI is verplicht Isabel-certificaten uit te geven conform de bepalingen in:

1. sectie "4.2 - Uitgifte certificaat" van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

2.1.1.8. KENNISGEVING VAN DE UITGIFTE VAN EEN CERTIFICAAT

Een Isabel-CA zorgt ervoor dat de Houder van het Isabel-certificaat wordt geïnformeerd over de uitgifte van zijn/haar Isabel-certificaat in overeenstemming met:

1. sectie "2.6.1 – Publicatie van informatie van een Isabel-CA" van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

2.1.1.9. ACCEPTATIE VAN DE HOUDER VERKRIJGEN VOOR ZIJN/HAAR ISABEL-CERTIFICAAT

Een Isabel-CA verkrijgt de acceptatie van de Houder van het Isabel-certificaat voor zijn/haar Isabel-Certificaat.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie "4.3 – Aanvaarding certificaat" van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

De acceptatie kan gebeuren (1) door middel van een expliciete kennisgeving, (2) doordat de Houder gebruik maakt van het Certificaat (3) of met ingang van de 10^{de} dag na de publicatie in de Repository zonder dat de Houder enige opmerkingen heeft geformuleerd.

2.1.1.10. PUBLICATIE VAN HET ISABEL-CERTIFICAAT IN EEN ISABEL REPOSITORY

Een Isabel-CA publiceert een Isabel-certificaat dat ze heeft uitgegeven nadat het certificaat werd geaccepteerd (Zie sectie 2.1.1.9 voor de acceptatievoorwaarden) door de Houder van het Isabel-certificaat.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie “2.6 – Publicatie en repository” van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

2.1.1.11. VERWERKING AANVRAGEN TOT HERROEPING CERTIFICAAT

Een Isabel-CA zal een aanvraag voor de herroeping van een certificaat van RA's onder haar toezicht zo snel mogelijk en veilig verwerken.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie “3.4 – Aanvraag voor herroeping” en sectie “4.4 – Herroeping Certificaat” van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

2.1.1.12. INFORMATIE BETREFFENDE DE HERROEPING VAN EEN ISABEL-CERTIFICAAT PUBLICEREN IN EEN ISABEL REPOSITORY

Een Isabel-CA zal de informatie over een Isabel-certificaat dat ze heeft herroepen, publiceren in de Isabel Repository in de vorm van:

1. Het Isabel-certificaat, geactualiseerd met een vlag die aangeeft dat het werd herroepen.
2. Een geactualiseerde Lijst met de Herroepingen van de Certificaten (CRL).

Het herroepen Isabel-certificaat en de geactualiseerde Lijst met de Herroeping van de Certificaten zullen zo vlug mogelijk worden gepubliceerd na de herroeping van het Isabel-certificaat.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in:

1. sectie “2.6 – Publicatie en repository” van onderhavige Isabel-CPS.
2. elke toepasselijke CP.

Dit mechanisme zal de Vertrouwende Partijen toelaten om tijdig en ondubbelzinnig op de hoogte te worden gesteld van de herroeping van een Isabel-certificaat dat werd uitgegeven door een Isabel-CA.

2.1.1.13. KENNISGEVING VAN DE HERROEPING VAN EEN CERTIFICAAT

Een Isabel-CA zorgt ervoor dat de entiteit (de Houder van het Isabel-certificaat of een fysieke persoon, gemachtigd door de klant van Isabel) die de herroeping van een Isabel-certificaat heeft aangevraagd bij een Isabel-RA en om het even welke ander Partij die vertrouwt op dat Isabel-certificaat, op de hoogte worden gesteld van de herroeping van het Isabel-certificaat in overeenstemming met:

1. sectie “4.4.6 - Uitgiftefrequentie CRL” van de Isabel-CPS.
2. elke toepasselijke CP.

2.1.1.14. KENNISGEVING AAN DE HOUDER EN DE VERTROUWENDE PARTIJEN VAN DE VEREISTE INFORMATIE OM CORRECT EN OP EEN VEILIGE MANIER GEBRUIK TE MAKEN VAN DE ISABEL PKI-SERVICES

1. Een Isabel-CA ziet erop toe dat de Houders van Isabel-certificaten, de Abonnees en de Vertrouwende Partijen op de hoogte worden gesteld van hun verplichtingen vermeld in de secties “2.1.3 - Verplichtingen van de Abonnee en Houder van een Isabel-certificaat” en “2.1.4 – Verplichtingen van de Vertrouwende Partij”.
2. Een Isabel-CA informeert de Houders van een Isabel-certificaat over de vereisten met betrekking tot de beveiliging van hun Private Sleutel, vermeld in sectie “6.2 – Bescherming van de Private Sleutel” van de onderhavige Policy van de Certificatie-Activiteit van Isabel.

3. Een Isabel-CA informeert de Houders van een Isabel-certificaat, Abonnees en de Vertrouwende Partijen over de garanties die worden geboden door de Isabel PKI-diensten, en de beperkingen ervan, overeenkomstig sectie “2.2 – Aansprakelijkheid” van de toepasselijke Isabel-CP.

De publicatie van onderhavige Isabel-CPS en de Isabel Certificatiepolities voor de Houders van een Isabel-certificaat en de Vertrouwende Partijen, als kennisgeving worden beschouwd.

2.1.1.15. BEVEILIGING VAN DE PRIVATE SLEUTEL VAN DE ISABEL-CA

Een Isabel-CA beveiligd zijn Private Sleutel overeenkomstig de bepalingen van sectie “6.2 – Bescherming van de Private Sleutel” van onderhavige Isabel-CPS.

2.1.1.16. BEPERKING OP HET GEBRUIK VAN DE PRIVATE SLEUTEL VAN DE UITGIFTE-CA

Een Isabel-CA ziet erop toe dat er geen ongepast gebruik wordt gemaakt van haar Private Sleutel.

Meer bepaald zal de Private Sleutel van de Isabel-CA, gebruikt voor:

1. Het uitgeven van Isabel-certificaten aan Houders
2. Het uitgeven van informatie over de status van herroeping van Isabel-certificaten en
3. andere relevante informatie over de uitgifte van Isabel-certificaten onder de onderhavige Isabel-CPS en de toepasselijke Isabel Certificaatpolities

niet worden gebruikt voor enig ander doel.

Een Isabel-CA mag haar Private Sleutel alleen gebruiken voor doeleinden die overeenstemmen met haar functie als CA.

2.1.1.17. MIDDELEN VOOR ELEKTRONISCHE HANDTEKENING VERSTREKT AAN DE HOUDER VAN HET ISABEL-CERTIFICAAT

Een Isabel-CA verstrekt de Houder van het Isabel-certificaat de volgende middelen voor het aanmaken van een elektronische handtekening:

1. Een Isabel-certificaat dat de Publieke Sleutel certificeert die gekoppeld is aan de Private Sleutel van de Houder.
2. Optioneel de software om een elektronische handtekening aan te maken.
3. Optioneel een Isabel Secure Signing Card of een Isabel Tamper Resistant Device die de Houder toelaten zijn Private Sleutel op te slaan en elektronische handtekeningen te genereren met zijn Private Sleutel.
4. Optioneel een sleutelpaar (Alleen geldig voor de Gecentraliseerde Certificatieprocedure – zie sectie 4.2.1 van onderhavige CPS).
5. Optioneel een PIN code (Alleen geldig voor de Gecentraliseerde Certificatieprocedure – zie sectie 4.2.1 van onderhavige CPS).

2.1.1.18. DE PARTIJEN SCHADELOOS STELLEN VOOR SCHADE EN SANCTIES

Een Isabel-CA vergoedt de partijen voor alle schade die voortvloeit uit het niet naleven van haar verplichtingen zoals vermeld in sectie “2.2 – Aansprakelijkheid” van de betreffende Isabel-CP.

2.1.1.19. GEGEVENS MET BETREKKING TOT DE ACTIVITEITEN ARCHIVEREN

Een Isabel-CA archiveert de gegevens met betrekking tot haar activiteiten.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in sectie “4.6 – Archiveren van gegevens” van deze Isabel-CPS.

2.1.1.20. PUBLICATIE CPS

Een Isabel-CA publiceert de Isabel-CPS.

Voor deze vereiste moet de Isabel-CA voldoen aan de bepalingen vermeld in sectie “2.6 – Publicatie en repository” van deze Isabel-CPS.

2.1.1.21. INFORMATIE BETREFFENDE DE HERROEPING VAN EEN CERTIFICAAT DOOR DE CA PUBLICEREN IN EEN ISABEL REPOSITORY

Een Isabel-CA publiceert de informatie over herroepingen door de CA in een Isabel Repository in de vorm van de Lijsten met Herroepingen van Certificaten van Autoriteiten (Authority Revocation Lists) (Self-signed en Cross-Certificates).

2.1.1.22. BESCHERMING VAN PERSOONLIJKE GEGEVENS

De Isabel-CA verzamelt en verwerkt de persoonlijke gegevens die nodig zijn om de certificatediensten te verlenen, conform de Belgische wet op de bescherming van persoonlijke gegevens (Wet van 8 december 1992).

De verwerking heeft tot doel de certificatediensten te beheren, inclusief het beheer van de klanten. De persoonlijke gegevens van de Houder van het Isabel-certificaat worden opgeslagen op de servers van Isabel N.V./S.A.

De Houder van het Isabel-certificaat heeft het recht zijn gegevens in te zien en indien nodig te corrigeren. Dat recht kan schriftelijk worden opgeëist, per gewone brief, gericht aan:

Isabel NV/SA
Customer Care Operations
Keizerinlaan / Bd de l'Impératrice 13-15
B-1000 Brussels
Belgium

De Houder van het Isabel-certificaat heeft het recht expliciet bezwaar aan te tekenen tegen het gebruik van zijn gegevens voor marketingdoeleinden, door middel van een brief, gericht aan de bovenvermelde afdeling.

2.1.2. VERPLICHTINGEN VAN ISABEL-RA'S

In het algemeen moet een Isabel-RA de rechten en verplichtingen respecteren die zijn opgenomen in deze CPS en elke betrokken CP.

Elke RA binnen de Isabel Infrastructuur voor Publieke Sleutels heeft de volgende specifieke verplichtingen:

2.1.2.1. CERTIFICAATAANVRAGEN VERWERKEN

De Isabel-RA verwerkt de aanvragen voor een Isabel-certificaat van Abonnees van Isabel-certificaten tijdig en veilig.

De Isabel-RA verzekert dat de Abonnee akkoord gaat met de relevante contractuele bepalingen en zal controleren of de Aanvraag van Isabel-certificaten naar behoren is ingevuld, correct en geldig is.

De Isabel-RA voert al haar opgelegde verplichtingen in verband met communicatie en archivering tijdig en correct uit.

De Isabel-RA bereidt de informatie voor die de Isabel-CA nodig heeft en stuurt een Aanvraag om een Isabel-certificaat naar de Isabel-CA.

Voor de verwerking van een Aanvraag voor een Isabel-certificaat is de Isabel-RA tegenover de juridische entiteit van Isabel contractueel verplicht de bepalingen na te leven die zijn vermeld in:

1. sectie "3.1 – Eerste registratie" en sectie "4.1 – Aanvraag certificaat" van onderhavige CPS.
2. elke toepasselijke CP.

2.1.2.2. BETEKENISVOLLE EN UNIEKE DISTINGUISHED NAMES GENEREREN VOOR DE HOUDERS VAN ISABEL-CERTIFICATEN

Een Isabel-RA genereert betekenisvolle en unieke Distinguished Names voor Houders van Isabel-certificaten binnen de Isabel PKI.

De Isabel-RA voldoet aan de bepalingen vermeld in:

1. sectie “3.1.2 – Verplicht gebruik van betekenisvolle namen” en sectie “3.1.4 – Uniek karakter van de namen” van onderhavige Policy van Certificatie-Activiteiten van Isabel.
2. elke toepasselijke CP.

2.1.2.3. ABONNEE/HOUDER IDENTIFICEREN EN AUTHENTIFICEREN EN NAGAAN OF HIJ IS AANGESTELD DOOR EEN ISABEL-KLANT

Een Isabel-RA identificeert en authentificeert op correcte wijze de Abonnees van het Isabel-certificaat, de Houders van het Isabel-certificaat en indien van toepassing, hun gevolmachtigde.

Deze identificatie kan zowel betrekking hebben op persoonlijke als op professionele gegevens.

De Isabel-RA controleert ook of de Abonnee van het Isabel-certificaat, of een Houder van het Isabel-certificaat werden aangesteld door een klant van Isabel.

Voor de identificatie en de authenticatie van de Abonnees van het Isabel-certificaat, de Houders van het Isabel-certificaat en hun gevolmachtigden, voldoet de Isabel-RA aan de bepalingen vermeld in:

1. hoofdstuk “3 – Identificatie en authenticatie” van onderhavige CPS.
2. elke toepasselijke CP.

2.1.2.4. VERZOEKEN IN VERBAND MET DE HERROEPING VAN CERTIFICATEN VERWERKEN

Een Isabel-RA ontvangt verzoeken voor de herroeping van een Isabel-certificaat en verwerkt deze zo snel mogelijk, waarna deze worden doorgestuurd naar een Isabel-CA. Het is de Isabel-CA die de uiteindelijke beslissing neemt om een Isabel-certificaat te herroepen.

Voor de verwerking van een verzoek om de Isabel-certificaten te herroepen, voldoet de RA aan de bepalingen vermeld in de sectie “4.4 – Herroeping Certificaat” van onderhavige CPS.

2.1.2.5. BEVEILIGEN VAN EEN RA PRIVATE SLEUTEL

Een Isabel-RA beveiligt zijn Private Sleutel in overeenstemming met de bepalingen vermeld in sectie “6.2 – Bescherming van de Private Sleutel” van onderhavige CPS.

2.1.2.6. BEPERKING OP HET GEBRUIK VAN DE RA PRIVATE SLEUTEL

Een Isabel-RA gebruikt haar Private Sleutel uitsluitend voor doeleinden die verband houden met haar RA-functie.

2.1.2.7. SCHADEVERGOEDING AAN PARTIJEN

Een Isabel-RA vergoedt de partijen voor elke schade die voortvloeit uit het niet respecteren van haar verplichtingen.

Voor deze vereiste moet de Isabel-RA voldoen aan de bepalingen vermeld in de sectie “2.2 – Aansprakelijkheid” van de toepasselijke Isabel-CP.

2.1.2.8. ARCHIVERING EN BEVEILIGING

De Isabel-RA vervult haar verplichtingen in verband met archivering zo veilig mogelijk om de beschikbaarheid van documenten en/of andere informatie die geldt als bewijs, veilig te stellen en om de vertrouwelijkheid en de integriteit van deze documenten en andere informatie te waarborgen. In het algemeen staat ze in voor de fysieke beveiliging van de informatie, beschermt ze de toegang tot de informatie en geeft ze haar personeel hiervoor de nodige instructies.

2.1.2.9. GOEDKEURING

Elke Isabel-RA die werkt onder het gezag van een Isabel-CA beschikt over een schriftelijke goedkeuring van deze Isabel-CA. De Isabel-CA beschikt over een lijst van goedgekeurde RA's. Door activiteiten uit te voeren als RA voor een Isabel-CA, bevestigt de Isabel-RA dat ze deze verantwoordelijkheid heeft aanvaard en erin toestemt te werken conform de toepasselijke CP's en de Isabel-CPS.

2.1.3. **VERPLICHTINGEN VAN DE ABONNEE EN HOUDER VAN EEN ISABEL-CERTIFICAAT**

De Houders en Abonnees van een Isabel-certificaat zijn in het algemeen verplicht de bepalingen, voorwaarden en procedures van deze CPS en van elke relevante CP te respecteren, welke ze geacht worden te hebben aanvaard door een Isabel-certificaat te gebruiken.

De Houders en Abonnees van een Isabel-certificaat stemmen er mee in om deze verplichtingen na te leven tijdens de volledige operationele periode waarin zij het Isabel-certificaat gebruiken.

De Abonnee zal een overeenkomst tekenen op het ogenblik van de uitgifte van het certificaat, of voordien. Deze overeenkomst is onderworpen aan het Belgisch recht. De RA bewaart een kopie van de overeenkomst. Abonnees zijn in rechten en verplichtingen contractueel gebonden aan Isabel, (1) hetzij rechtstreeks met Isabel, (2) hetzij met de RA.

De Houders en Abonnees van een Isabel-certificaat hebben de volgende verplichtingen:

2.1.3.1. EEN ISABEL-CERTIFICAAT AANVRAGEN

Voor de aanvraag van een certificaat is de Abonnee van het Isabel-certificaat is verplicht om:

1. correcte, accurate en volledige informatie te verstrekken in de Aanvraag voor het Isabel-certificaat.
2. de Aanvraag voor het Isabel-certificaat behoorlijk te laten ondertekenen door de Houder van het Isabel-certificaat.
3. De Aanvraag voor het Isabel-certificaat te ondertekenen.
4. De ondertekende Aanvraag voor het Isabel-certificaat in te dienen bij een Isabel-RA.

Voor deze vereiste moet de Houder van een Isabel-certificaat voldoen aan de bepalingen vermeld in de sectie "3.1 – Eerste registratie" en in de sectie "4.1 – Aanvraag certificaat" van onderhavige CPS.

2.1.3.2. SLEUTELPAAR AANMAKEN

Als de Houder van het Isabel-certificaat zijn/haar sleutelbaar zelf aanmaakt, moet hij/zij voldoen aan de bepalingen in verband met de kwaliteitseisen (onder meer in verband met de lengte en het algoritme van de sleutel), zoals vermeld in sectie "6.1– Aanmaken en installeren van het sleutelbaar" van onderhavige CPS.

2.1.3.3. EEN ISABEL-CERTIFICAAT VERKRIJGEN

Na bericht van de Isabel-RA bij wie de Aanvraag voor een Isabel-certificaat werd ingediend, en na identificatie en authenticatie van de Abonnee en de Houder door deze Isabel-RA, moet de Houder van het Isabel-certificaat het volgende ontvangen van de Isabel-CA:

1. Een Isabel-certificaat dat de Publieke Sleutel certificeert die hoort bij de Private Sleutel van de Houder.
2. Optioneel software om een elektronische handtekening aan te maken.
3. Optioneel een Isabel Secure Signing Card of een Isabel Tamper Resistant Device om de Private Sleutel van de Houder te implementeren.
4. Optioneel een sleutelbaar (Alleen geldig voor de Gecentraliseerde Certificatieprocedure – zie sectie 4.2.1 van onderhavige CPS).
5. Optioneel een PIN code (Alleen geldig voor de Gecentraliseerde Certificatieprocedure – zie sectie 4.2.1 van onderhavige CPS).

2.1.3.4. EEN ISABEL-CERTIFICAAT AANVAARDEN

Na ontvangst van zijn Isabel-certificaat moet de Houder van het Isabel-certificaat zijn Isabel-certificaat en alle daarin vervatte informatie controleren en de Isabel-CA die het certificaat heeft uitgegeven ervan op de hoogte brengen of hij het Isabel-certificaat al dan niet aanvaardt.

Door het certificaat te aanvaarden, bevestigt de Houder dat de informatie in het Isabel-certificaat correct, accuraat en volledig is.

De aanvaarding van het Isabel-certificaat impliceert de aanvaarding van de CPS en de toepasselijke CP, evenals de aanvaarding van alle andere betekenissen aan de Houder.

De aanvaarding kan gebeuren (1) door middel van een expliciete kennisgeving, (2) doordat de Houder gebruik maakt van het Certificaat, (3) of ook nog met ingang van de 10^{de} dag na de publicatie in de Repository zonder dat de Houder enige opmerkingen heeft doorgegeven.

Voor deze vereiste moet de Houder van het Isabel-certificaat voldoen aan de bepalingen vermeld in de sectie “4.3 – Aanvaarding certificaat” van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

2.1.3.5. DE NODIGE INFORMATIE VERKRIJGEN OM OP EEN CORRECTE EN VEILIGE MANIER GEBRUIK TE MAKEN VAN DE ISABEL PKI-DIENSTEN

De Houder van een Isabel-certificaat moet van de Isabel-CA die zijn/haar Isabel-certificaat heeft uitgegeven het volgende ontvangen:

1. Informatie over zijn/haar verplichtingen vermeld in sectie “2.1.3 – Verplichtingen van de Abonnee en Houder van een Isabel-certificaat” van onderhavige CPS.
2. Informatie over de vereisten in verband met de beveiliging van zijn/haar Private Sleutel in overeenstemming met de bepalingen vermeld in sectie “6.2 – Bescherming van de Private Sleutel” van onderhavige CPS.
3. Informatie over de waarborgen die de Isabel PKI-diensten aanbieden in overeenstemming met sectie “2.2 – Aansprakelijkheid” van de toepasselijke Isabel-CP.

De publicatie van onderhavige Isabel-CPS ten aanzien van de Houders van het Isabel-certificaat en de Vertrouwende Partijen, moet als kennisgeving worden beschouwd. Het gebruik van het Isabel-certificaat door de Houder impliceert het aanvaarden van de bepalingen in deze berichtgeving.

2.1.3.6. HET VERTROUWELIJKE KARAKTER VAN DE PRIVATE SLEUTEL GARANDEREN

De Houder van het Isabel-certificaat moet garanderen en er zorg voor dragen dat hij de Private Sleutel als enige in zijn bezit zal hebben en hij moet het vertrouwelijk karakter en de veiligheid ervan garanderen en beschermen, evenals het vertrouwelijk karakter van de PIN-code; deze wordt gebruikt om de Private Sleutel te beschermen tegen ongeoorloofd gebruik.

Over het algemeen neemt de Houder de nodige voorzorgen om het verlies, het bekend maken aan derden, de wijziging of het ongeoorloofd gebruik van sleutelgegevens en de Isabel Secure Signing Card te voorkomen.

Telkens wanneer er gebruik wordt gemaakt van de Private Sleutel van de Houder, wordt ervan uitgegaan dat het de Houder zelf is die hem gebruikt, tenzij onweerlegbaar kan worden aangetoond dat dit niet zo is.

Daartoe dient de Houder van het Isabel-certificaat de bepalingen van sectie “2.8 – Vertrouwelijk karakter” van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

2.1.3.7. BEPERKING VAN HET GEBRUIK VAN DE PRIVATE SLEUTEL EN HET ISABEL-CERTIFICAAT

De Houder van het Isabel-certificaat mag zijn/haar Private Sleutel en Isabel-certificaat alleen gebruiken voor doeleinden die toegelaten zijn, conform de bepalingen van de relevante CP of elke overeenkomst die werd of zal worden opgesteld tussen Isabel en de klant van Isabel.

Als de Houder vermoedt dat zijn Private Sleutel werd gecorrumpeerd, moet hij vragen zijn Isabel-certificaat te herroepen en mag hij geen elektronische handtekeningen meer aanmaken met zijn Private Sleutel.

Als alle certificaten met betrekking tot dezelfde Publieke Sleutel werden herroepen of vervallen zijn, wordt de Publieke Sleutel ongeldig en mag de Houder de bijhorende Private Sleutel niet meer gebruiken, onder meer om een elektronische handtekening te genereren, of om iets te ontsleutelen.

2.1.3.8. KENNISGEVING AAN DE ISABEL REVOCATIE SERVICE VAN MISBRUIK VAN PRIVATE SLEUTEL/PIN – VERLIES VAN ISABEL SECURE SIGNING CARD

Een Abonnee of een Houder van het Isabel-certificaat moet de Isabel Revocation Service onmiddellijk op de hoogte brengen van:

1. De vermoedelijke of vastgestelde corruptie, het verlies of de onthulling van de Private Sleutel van de Houder.
2. Het vermoedelijke of vastgestelde verlies van de Isabel Secure Signing Card van de Houder.
3. Het vermoedelijke of vastgestelde misbruik, het verlies of de onthulling van de PIN-code van de Houder.

Daarom moet de Houder van het Isabel-certificaat voldoen aan de bepalingen vermeld in de sectie “4.4 – Herroeping Certificaat” van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

Houders van een Isabel-certificaat die behoren tot de WISE community kunnen geen gebruik maken van deze dienst en moeten derhalve hun Isabel-RA op de hoogte brengen, zie “2.1.3.9 – Kennisgeving aan de Isabel-RA van misbruik van private sleutel/PIN – verlies van Isabel Secure Signing Card – Statuswijziging”.

2.1.3.9. KENNISGEVING AAN DE ISABEL-RA VAN MISBRUIK VAN PRIVATE SLEUTEL/PIN – VERLIES VAN ISABEL SECURE SIGNING CARD – STATUSWIJZIGING

Een Abonnee of een Houder van het Isabel-certificaat moet zijn Isabel-RA onmiddellijk op de hoogte brengen van:

1. De vermoedelijke of vastgestelde corruptie, het verlies of de onthulling van de Private Sleutel van de Houder.
2. Het vermoedelijke of vastgestelde verlies van de Isabel Secure Signing Card van de Houder.
3. Het vermoedelijke of vastgestelde misbruik, het verlies of de onthulling van de PIN-code van de Houder.
4. Elke wijziging in de informatie die werd verstrekt bij de aanvraag van het Isabel-certificaat voor de Houder.

Voor de vereisten vermeld in punt 1 tot 3 moet de Houder van het Isabel-certificaat voldoen aan de bepalingen vermeld in de sectie “4.4 – Herroeping Certificaat” van onderhavige Policy van de Certificatie-Activiteiten van Isabel. De revocatie wordt gemeld aan de Isabel-RA voor alle gevallen die niet door de Isabel Revocatie Service gedekt worden.

2.1.3.10. SANCTIES EN SCHADEVERGOEDINGEN

De Houder van het Isabel-certificaat en de Vertrouwende Partij moeten voldoen aan de bepalingen vermeld in sectie “2.2 – Aansprakelijkheid” van de toepasselijke CP.

De Isabel-CA heeft het recht het certificaat van een Houder te herroepen als niet wordt voldaan aan de verplichtingen, vermeld in deze CPS, een relevante CP en/of een overeenkomst tussen Isabel en de Houder. In voorkomend geval sluit de herroeping geen andere sancties of schadevergoedingen uit, toegepast bij wet, op grond van overeenkomsten of toepasselijke policies zoals onderhavige CPS of elke andere toepasselijke CP.

2.1.3.11. GEBRUIK VAN HARDWARE, MET NAME DE SECURE SIGNATURE CREATION DEVICE

De Houder van het Isabel-certificaat moet een Secure Signature Creation Device (veilig middel voor het aanmaken van een handtekening) gebruiken om haar/zijn Private Sleutel te bewaren en te gebruiken:

1. Hetzij een Isabel Secure Signing Card (voor Houders 'Natuurlijke persoon' of 'Functie')
2. Hetzij Isabel Tamper Resistant Device (voor Houders 'Natuurlijke persoon', 'Functie', of 'Applicatie')
3. Hetzij hardwarematige veiligheidsmodule van derden (voor Houders 'Natuurlijke persoon', 'Functie', of 'Applicatie')

2.1.3.12. BEPERKINGEN OP HET GEBRUIK VAN DE PUBLIEKE SLEUTEL

De Houder van het Isabel-certificaat of Abonnee mag geen verzoek om een certificaat indienen bij een derde CA dat de Publieke Sleutel uit zijn/haar Isabel-certificaat bevat, ook al is dat Isabel-certificaat verstreken of herroepen.

De Houder van het Isabel-certificaat of Abonnee mag geen verzoek om een certificaat indienen bij een Isabel CA dat de Publieke Sleutel uit zijn/haar certificaat bij een derde CA bevat, ook al is dat certificaat verstreken of herroepen.

2.1.4. VERPLICHTINGEN VAN DE VERTROUWENDE PARTIJ

Bij het beoordelen van de zekerheid van een Isabel-certificaat moet een Vertrouwende Partij rekening houden met de voorwaarden en bepalingen van deze CPS en elke relevante CP, inclusief alle toepasbare aansprakelijkheidsbeperkingen en garanties. Een Vertrouwende Partij moet bovendien alle regels, reglementeringen en statuten die gelden voor alle informatie in het certificaat, kennen en toepassen.

Een Vertrouwende Partij heeft specifiek de volgende verplichtingen:

2.1.4.1. DE NODIGE INFORMATIE VERKRIJGEN OM OP EEN CORRECTE EN VEILIGE MANIER GEBRUIK TE MAKEN VAN DE ISABEL PKI-DIENSTEN

Een Vertrouwende Partij moet van de Isabel-CA die het Isabel-certificaat waarop hij wil vertrouwen, heeft uitgegeven, informatie ontvangen over de waarborgen, aansprakelijkheden en verplichtingen die door de Isabel PKI-services worden voorgesteld in overeenstemming met sectie "2.2 – Aansprakelijkheid" van de toepasselijke Isabel-CP.

2.1.4.2. VERKRIJGEN EN VERIFIËREN VAN HET ISABEL-CA SELF-SIGNED CERTIFICAAT

De Vertrouwende Partij is verplicht het self-signed certificaat van de Isabel-CA te verkrijgen bovenaan de ketting van certificaten die vereist zijn om de geldigheid van een Isabel-certificaat te verifiëren.

Om een self-signed Isabel-CA-certificaat te ontvangen en de geldigheid ervan te controleren, moet de Vertrouwende Partij voldoen aan de bepalingen, vermeld in sectie "4.3 – Aanvaarding certificaat" van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

2.1.4.3. DE INHOUD EN GELDIGHEID VAN HET ISABEL-CERTIFICAAT CONTROLEREN

Een Vertrouwende Partij moet de inhoud en de geldigheid van een Isabel-certificaat controleren en accepteren vooraleer ze op dit certificaat vertrouwt.

Een Vertrouwende Partij moet de volgende attributen van een certificaat controleren:

1. De uitgever (Isabel-CA),
2. De geldigheidsperiode,
3. De herroepingstatus,
4. Het gebruik en de beperkingen van de sleutel en het certificaat,
5. De handtekening van de CA.

De attributen van Isabel-certificaten vindt u in sectie "7.1 – Certificatenprofiel" van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

Een Vertrouwende Partij mag niet vertrouwen op een Isabel-certificaat als:

1. De controle van de elektronische handtekening op het Isabel-certificaat mislukt, of als de controle van het Isabel-certificaat zelf mislukt, of
2. Dit Isabel-certificaat is vervallen, of
3. Dit Isabel-certificaat werd herroepen, of
4. Het Isabel-certificaat wordt gebruikt voor ongeoorloofde doeleinden, of de gebruiksbeperkingen niet worden nageleefd.

2.1.4.4. BEPERKING VAN HET GEBRUIK VAN HET ISABEL-CERTIFICAAT

Een Vertrouwende Partij kan enkel op een Isabel-certificaat vertrouwen voor toegestane gebruiksdoeleinden, en binnen de beperkingen inzake functioneel gebruik en waarde, in overeenstemming met de bepalingen, vermeld in sectie “6.1.9 – Gebruiksdoeleinden van de sleutel” van de toepasselijke CP, indien aanwezig.

2.1.4.5. HANDTEKENINGEN VERIFIËREN

De Vertrouwende Partij is verplicht een digitale handtekening te verifiëren aan de hand van het Isabel-certificaat dat de Publieke Sleutel, die bij de Private Sleutel hoort, certificeert en welke gebruikt werd om de digitale handtekening aan te maken.

2.1.4.6. NIET-NALEVING VAN DE VERPLICHTINGEN VAN DE VERTROUWENDE PARTIJEN

De Vertrouwende Partij moet zich bewust zijn van de bepalingen in sectie “2.3.1 - Schadevergoeding door Isabel-Certificaatabonnees, Vertrouwende Partijen en Houders” en sectie “2.2 – Aansprakelijkheid” van de toepasselijk Isabel-CP.

2.1.5. VERPLICHTINGEN INZAKE REPOSITORY

Zie sectie “2.1.8.2 - Bijhouden van een Elektronische Repository voor Certificaten en informatie betreffende de Herroeping van Certificaten” van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

2.1.6. VERPLICHTINGEN VAN DE VALIDATIEAUTORITEIT

De Validatie Autoriteit is verplicht om tijdsaccurate informatie te verstrekken betreffende de status van de certificaten uitgegeven door de Isabel-CA volgens onderhavige Policy van de Certificatie-Activiteiten van Isabel en de toepasselijke Isabel-CP.

2.1.7. VERPLICHTINGEN VAN DE POLICY-AUTORITEIT

De Policy-autoriteit is verplicht de conformiteit met de onderhavige Isabel-CPS te specificeren, te valideren en te verzekeren en is verplicht te bepalen of onderhavige CPS geschikt is voor de Isabel-CP.

2.1.8. DE JURIDISCHE ENTITEIT ISABEL

2.1.8.1. OVEREENKOMSTEN

Isabel is verantwoordelijk voor het afsluiten van één of meer overeenkomsten met:

1. De Abonnee van het Isabel-certificaat, zodanig dat de rechten en verplichtingen van beide partijen duidelijk en expliciet worden vermeld. Deze overeenkomst verwijst naar de Isabel-CP en de onderhavige CPS, en in het bijzonder naar deze sectie. De overeenkomst zal ten minste de volgende informatie bevatten:

- a. De bevestiging van de Abonnee van het Isabel-certificaat dat de informatie die hij aan de Isabel-RA heeft verstrekt, correct is.
 - b. Dat de Houder van het Isabel-certificaat het sleutelpaar alleen zal gebruiken voor de doeleinden waarvoor het is bestemd en met alle andere beperkingen die aan de Abonnee van het Isabel-certificaat werden meegedeeld in een contract of elk ander wettelijk document (vb. CP, CPS,...).
 - c. De aanvaarding door de Houder van het Isabel-certificaat van de regels en voorwaarden voor het gebruik van de media die worden gebruikt om de Private Sleutel op te slaan, inclusief de aansprakelijkheid voor de beveiliging van de Private Sleutel, de opslagmedia en zijn PIN.
 - d. De bevestiging van de Houder van het Isabel-certificaat dat hij/zij onmiddellijk het verlies van zijn/haar Private Sleutel en/of de bijhorende PIN zal melden, evenals elk vermoeden van misbruik of compromittering van de beveiliging.
 - e. Het systeem van de herroeping van Isabel-certificaten.
 - f. De aansprakelijkheidsbeperkingen van Isabel.
2. De RA's die optreden voor rekening van een Isabel-CA, met duidelijke vermelding van de rechten en verplichtingen van beide partijen.
 3. De Isabel-RA Agent (Lokaal of Centraal), die optreedt voor rekening van een Isabel-RA, met duidelijke vermelding van de rechten en verplichtingen van beide partijen. Deze overeenkomst maakt deel uit van de overeenkomst tussen Isabel en de Isabel-RA.

2.1.8.2. BIJHOUDEN VAN EEN ELEKTRONISCHE REPOSITORY VOOR CERTIFICATEN EN INFORMATIE BETREFFENDE DE HERROEPING VAN CERTIFICATEN

Isabel houdt een Elektronische Repository voor Isabel-certificaten bij en stelt deze ter beschikking, evenals informatie betreffende de herroeping van Isabel-certificaten.

Isabel beveiligt deze Elektronische Repository naar best vermogen tegen ongeoorloofde wijzigingen.

Dit elektronisch repository bevat ten minste:

1. De Isabel-certificaten die werden uitgegeven door Isabel-CA conform de onderhavige Isabel-CPS en de relevante CP.
2. De Lijsten met de Herroepingen van de Isabel-certificaten, die worden gepubliceerd conform de onderhavige Isabel-CPS en de relevante CP.
3. De self-signed certificaten van de Isabel-CA.

Isabel zorgt ervoor dat de certificaten en de bijhorende Lijsten met de Herroepingen van de Certificaten tijdig worden gepubliceerd, zoals vermeld in sectie "2.6 – Publicatie en repository" van onderhavige CPS.

Het Elektronische Repository is permanent (24/24) beschikbaar en kan door de klant te allen tijde worden geconsulteerd.

Het Elektronische Repository kan niet worden geconsulteerd door personen die geen klant zijn van Isabel of door hun vertegenwoordigers.

2.1.9. ISABEL REVOCATIE SERVICE

The Isabel Revocatie Service laat toe om certificaten van Fysische Personen en Functies te revoceren, 24 uur op 24. Deze service is beschikbaar in geval van verlies of diefstal van de smart card van een Houder van een Isabel Certificate of onthulling van de PIN of de Private Sleutel.

Deze service is niet beschikbaar voor Houders van een Isabel-certificaat die tot WISE gemeenschap behoren.

2.1.9.1. VERZOEKEN IN VERBAND MET DE HERROEPING VAN CERTIFICATEN VERWERKEN

Een Isabel Revocatie Service ontvangt verzoeken voor de herroeping van een Isabel-certificaat en verwerkt deze zo snel mogelijk, waarna deze worden doorgestuurd naar een Isabel-CA. Het is de Isabel-CA die de uiteindelijke beslissing neemt om een Isabel-certificaat te herroepen.

Voor de verwerking van een verzoek om de Isabel-certificaten te herroepen, voldoet de Isabel Revocatie Service aan de bepalingen vermeld in de sectie "4.4 – Herroeping Certificaat" van onderhavige CPS.

2.1.9.2. ABONNEE/HOUDER IDENTIFICEREN EN AUTHENTIFICEREN

Een Isabel Revocatie Service identificeert en authenticert op een zo goed mogelijke wijze de Abonnees van het Isabel-certificaat, de Houders van het Isabel-certificaat en indien van toepassing, hun gevolmachtigde, vooraleer over te gaan tot certificaat revocatie.

Deze identificatie kan zowel betrekking hebben op persoonlijke als op professionele gegevens.

2.1.9.3. BEVEILIGING VAN EEN REVOCATIE SERVICE PRIVATE SLEUTEL

Een Isabel Revocatie Service beveiligt zijn Private Sleutel in overeenstemming met de bepalingen vermeld in sectie "6.2 – Bescherming van de Private Sleutel" van onderhavige CPS.

2.1.9.4. BEPERKING OP HET GEBRUIK VAN DE REVOCATIE SERVICE PRIVATE SLEUTEL

Een Isabel Revocatie Service gebruikt haar Private Sleutel uitsluitend voor doeleinden die verband houden met haar Revocatie Service functie.

2.1.9.5. AANSPRAKELIJKHEID

De aansprakelijkheid van de Isabel Revocatie Service voldoet aan de bepalingen vermeld in de sectie "2.2 – Aansprakelijkheid" van de toepasselijke Isabel-CP.

2.1.9.6. ARCHIVERING EN BEVEILIGING

De Isabel Revocatie vervult haar verplichtingen in verband met archivering zo veilig mogelijk om de beschikbaarheid van documenten en/of andere informatie die geldt als bewijs, veilig te stellen en om de vertrouwelijkheid en de integriteit van deze documenten en andere informatie te waarborgen. In het algemeen staat ze in voor de fysieke beveiliging van de informatie, beschermt ze de toegang tot de informatie en geeft ze haar personeel hiervoor de nodige instructies.

2.1.9.7. GOEDKEURING

Elke Isabel Revocatie Service die werkt onder het gezag van een Isabel-CA beschikt over een schriftelijke goedkeuring van deze Isabel-CA. De Isabel Revocatie Service is Card Stop.

2.1.9.8. CONTACT GEGEVENS

De Isabel Revocatie Service is :

Card Stop

Tel : +32 (0)70/344.344

Fax : +32 (0)70/344.355

2.2. AANSPRAKELIJKHEID

De aansprakelijkheid in verband met Isabel-certificaten wordt beschreven in sectie "2.2 – Aansprakelijkheid" van de toepasselijke Isabel-CP.

Isabel zal alles in het werk stellen wat redelijkerwijze mogelijk is om zich voldoende te verzekeren tegen elke aansprakelijkheid tegenover Vertrouwende Partijen of andere partijen, die voortvloeit uit het verstrekken van diensten onder deze CPS, of de toepasselijke Isabel-CP.

2.3. FINANCIËLE VERANTWOORDELIJKHEID

2.3.1. SCHADEVERGOEDING DOOR ISABEL-CERTIFICAATABONNEES, VERTROUWENDE PARTIJEN EN HOUDERS

Isabel-Certificaatabonnees en/of Vertrouwende Partijen die zich verlaten op het Isabel-certificaat en/of Houders van een Isabel-certificaat moeten alle partijen (inclusief de Isabel-CA, de Registratieautoriteiten en de Revocatie Services) en/of Isabel vergoeden voor de schade die voortvloeit uit het niet respecteren van hun verplichtingen.

Een Vertrouwende Partij die heeft gehandeld op een wijze die niet strookt met zijn/haar verplichtingen zoals vermeld in onderhavige CPS, kan geen geldige schadevergoeding eisen van Isabel in geval van schade.

Isabel is niet aansprakelijk voor feiten die het gevolg zijn van de niet-naleving van haar verplichtingen door een Vertrouwende Partij.

2.3.2. VERTROUWELIJKE RELATIES

De relatie tussen Isabel en de Houders van Isabel-certificaten en tussen Isabel en op het Isabel-certificaat Vertrouwende Partijen is geen relatie van agent en principaal. Noch de Abonnees van het Isabel-certificaat, noch de op het Isabel-certificaat Vertrouwende Partijen beschikken over het gezag om Isabel, door middel van een contract of op enige andere manier, aan een verplichting te binden.

2.3.3. ADMINISTRATIEF PROCES

De rekeningen en het jaarverslag van Isabel worden jaarlijks gepubliceerd en gecontroleerd conform de Belgische wet.

2.4. INTERPRETATIE EN UITVOERING

In geval van een conflict of inconsistentie tussen onderhavige Policy van de Certificatie-Activiteiten van Isabel, een Isabel-CP en de contractuele overeenkomsten met de Klant, Houders en Abonnees van een Isabel-certificaat geldt:

1. De bepalingen van een Isabel-CP voorrang op de incompatibele of tegenstrijdige bepalingen van de Policy van de Certificatie-Activiteiten van Isabel.
2. De bepalingen van een Isabel-CP en Isabel-CPS voorrang op de contractuele overeenkomsten en elke specifieke, nieuwe overeenkomst, tenzij anders gestipuleerd.

2.4.1. TOEPASSELIJKE WETTEN

De uitvoering, de constructie, de interpretatie en de geldigheid van onderhavige Policy van de Certificatie-Activiteiten van Isabel zijn onderworpen aan de Belgische wet.

2.4.2. VERWIJDERING, VOORTBESTAAN, FUSIE, BERICHTGEVING

Voor zover een bevoegde rechtbank of soortgelijke instantie oordeelt dat een of meer voorwaarden van dit document ongeldig, onafdwingbaar of onwettelijk zijn, zullen deze voorwaarden uit dit document – dat verder geldig blijft – worden verwijderd. Deze voorwaarden zullen worden vervangen door een clause die de intentie van de ongeldige clause zo dicht mogelijk benadert.

In het uitzonderlijke geval waarin de nationale wetten die gelden voor een buitenlandse Abonnee op een Isabel-certificaat of Houder niet toelaten dat zekere bepalingen uit deze CPS worden opgenomen, zullen deze specifieke bepalingen van de CPS als onbestaande worden beschouwd voor deze Abonnee op/Houder van het Isabel-certificaat, alsof ze er niet in waren opgenomen; in voorkomend geval is de eerste paragraaf van onderhavige artikel van toepassing.

De bepalingen die van nature blijven gelden na het einde van de geldigheidstermijn van deze CPS, zullen ook blijven voortbestaan.

Ingeval van een fusie zal Isabel S.A./N.V. haar beste inspanningen leveren om de continuïteit van de hierin vermelde CA-activiteiten te verzekeren.

Alle officiële berichten die vereist zijn in het raam van deze CPS, zullen schriftelijk worden opgemaakt en verzonden via aangetekende post, fax, of via een e-mailbericht dat is ondertekend met een geavanceerde elektronische handtekening.

2.4.3. PROCEDURES VOOR HET OPLOSSEN VAN GESCHILLEN

Alle partijen die betrokken zijn bij de Isabel-PKI, inclusief de Isabel-CA, RA, Klanten, Abonnees, Houders en Vertrouwende Partijen, zullen te goeder trouw en naar beste vermogen trachten een minnelijke schikking te treffen voor eventuele onderlinge vorderingen, geschillen of discussies.

Als er binnen een redelijke termijn geen minnelijke schikking kan worden getroffen voor een geschil, zullen alle geschillen uitsluitend worden beslecht door de Rechtbanken van Brussel. De Partijen kunnen te allen tijde instemmen met een arbitrageprocedure via Cepina of SGOA (Stichting Geschillen Oplossing Automatisering).

2.5. VERGOEDINGEN

De vergoedingen voor Isabel-certificaten en de bijbehorende diensten, evenals hun modaliteiten, zijn bepaald in de contractuele overeenkomsten tussen Klanten van/Abonnees op/Houders van het Isabel-certificaat en Isabel.

Terugbetalingen zijn enkel mogelijk voor zover dit uitdrukkelijk overeengekomen is.

2.6. PUBLICATIE EN REPOSITORY

2.6.1. PUBLICATIE VAN INFORMATIE VAN EEN ISABEL-CA

Een Isabel-CA moet de volgende informatie publiceren:

1. De Isabel-CP.
2. De Policy van de Certificatie-Activiteiten van Isabel.
3. De Isabel-certificaten die door de Houder werden aanvaard, waarmee hij verklaart dat ze de juiste informatie bevatten.
4. De Lijsten met Herroepingen van Certificaten voor Isabel-certificaten.
5. Het self-signed certificaat en de cross-certificaten van de Isabel-CA.
6. De Lijsten met Herroepingen van Certificaten van Autoriteiten (ARL's).
7. Isabels algemene voorwaarden voor certificatiediensten.

8. De modelcontracten voor certificatediensten.

Deze informatie zal on-line worden gepubliceerd en kan ook in andere vormen worden gepubliceerd.

2.6.2. FREQUENTIE VAN DE PUBLICATIES

Binnen 24 uur na hun aanvaarding door de Houder worden de Isabel-certificaten gegarandeerd gepubliceerd. Doorgaans worden de Isabel-certificaten binnen het half uur na hun aanvaarding gepubliceerd.

De Lijsten met Herroepingen van Certificaten van de Isabel-certificaten (CRL) en de Lijsten met Herroepingen van Certificaten van Autoriteiten (ARL) worden doorgaans geactualiseerd binnen het half uur nadat er een verandering werd in aangebracht; zij worden minstens om de 24 uur opnieuw uitgegeven.

De versiecontrole voor de Isabel-CPS gebeurt zoals bepaald in dit document.

De uitgifte van de CPS wordt behandeld in sectie "8 - Specificatie Administratie" van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

2.6.3. TOEGANGSCONTROLE

De Isabel-CA zorgt voor de nodige toegangscontroles om het ongeoorloofd schrijven, wijzigen of wissen van certificaten, policydocumenten, CRL's en andere items in de Repository te verhinderen.

Tot onderhavige Isabel-CPS hebben toegang in **modus alleen-lezen**:

1. De Isabel-CA
2. De Isabel-RA's
3. De Abonnees en Houders van het Isabel-certificaat
4. De op het Isabel-certificaat Vertrouwende Partijen

Onderhavige Isabel-CPS is toegankelijk in **modus schrijven/updates** voor de Policy-autoriteit, zie sectie "8 - Specificatie Administratie".

De Isabel-certificaten, de Lijsten met Herroepingen van Certificaten (CRL's) voor Isabel-certificaten en de Lijsten met Herroepingen van Certificaten van Autoriteiten (ARL's) zijn toegankelijk in **modus alleen-lezen** voor:

1. De RA's
2. De Abonnees en Houders van het Isabel-certificaat
3. De op het Isabel-certificaat Vertrouwende Partijen
4. De Isabel Repository
5. De Isabel Policy-Autoriteit

De Isabel-certificaten, de Lijsten met Herroepingen van Certificaten van de Isabel-certificaten en de Lijsten met Herroepingen van Certificaten van Autoriteiten zijn toegankelijk in **modus schrijven/updates** voor de Isabel-CA.

2.6.4. REPOSITORY'S

De Isabel-certificaten en de Lijsten met Herroepen Isabel-certificaten worden gepubliceerd in een Isabel X.500 directory.

Isabel S.A./N.V., en niet de Isabel-Certificatieautoriteit, is verantwoordelijk voor het beheer van de Isabel X.500.

2.7. CONFORMITEITSAUDITS

Isabel onderwerpt al zijn procedures aan audits en controleert hun conformiteit met onderhavige Isabel-CPS. Audits kunnen worden uitgevoerd op Isabel-CA's en RA's.

2.7.1. FREQUENTIE VAN DE CONFORMITEITSAUDITS VOOR EEN ENTITEIT

De frequentie van deze audits wordt bepaald door:

1. De interne policies van Isabel.
2. De toepasselijke Belgische wetgeving.
3. Andere partijen die bevoegd zijn om audits uit te voeren op grond van hun relatie met Isabel.

2.7.2. IDENTITEIT/KWALIFICATIE VAN DE AUDITORS

De auditor(s) wordt/worden gekozen als onafhankelijke partijen met ervaring op het gebied van Infrastructuren voor Publieke Sleutels.

De auditor(s) beschikt/beschikken over de nodige kwalificaties die wettelijk zijn opgelegd en gebruikelijk zijn in de handels/beroepswereld. De auditor(s) heeft/hebben als voornaamste taak de CA of de Veiligheid van het Informaticasysteem aan audits te onderwerpen; zij moeten in hoge mate vertrouwd zijn met PKI-policies (CPS en CP's).

De auditor(s) wordt/worden vermeld in de Revisiestatus van de Isabel-CPS.

2.7.3. DE RELATIE VAN DE AUDITORS MET DE PARTIJ DIE AAN EEN AUDIT ONDERWORPEN WORDT

De auditors moeten onafhankelijk zijn van Isabel en de Isabel CA's.

De auditors zullen met Isabel een contractuele overeenkomst hebben voor het uitvoeren van de audit en zullen voldoende onafhankelijk georganiseerd zijn van de Isabel-CA, Isabel-RA of elke andere component van de Isabel-PKI om een onbevooroordeelde, onafhankelijke evaluatie uit te voeren.

2.7.4. VOORWERP VAN DE AUDIT

Er zullen audits worden uitgevoerd in verband met:

1. De infrastructuur van de Isabel-CA.
2. Het management van de Isabel-CA.
3. De belangrijkste management policies en procedures van de Isabel-CA.
4. De operaties van de Isabel-CA.
5. De operaties van de Isabel-RA.
6. De conformiteit met de policies van Isabel, CP en CPS.
7. De naleving van de Belgische wetgeving.

2.7.5. TE NEMEN ACTIES BIJ GEBREKEN

De auditrapporten worden door Isabel geëvalueerd. Afwijkingen ten opzichte van de Isabel-CP, CPS of andere onregelmatigheden zullen voorrang krijgen en correctieve maatregelen zullen worden genomen. Achteraf kan nog een audit worden uitgevoerd om de vereiste rechtzettingen na te gaan.

2.7.6. MEDEDELING VAN DE RESULTATEN

De bevindingen van een audit worden in een rapport gegoten dat uitsluitend wordt gericht aan de Isabel Security Manager.

De informatie van het auditrapport wordt niet publiek bekend gemaakt, tenzij de nationale wetgeving dit vereist. Auditinformatie dient te worden aanzien als strikt vertrouwelijk binnen het kader van onderhavige CPS.

2.8. VERTROUWELIJK KARAKTER

2.8.1. CATEGORIEËN INFORMATIE DIE VERTROUWELIJK MOETEN BLIJVEN

Alle informatie betreffende de toepassing, uitgifte, aanvaarding en herroeping van Isabel-certificaten wordt als vertrouwelijk beschouwd en is slechts beperkt toegankelijk, tenzij zij is opgenomen in sectie “2.8.2 – Categorieën informatie die als niet-vertrouwelijk worden aanzien”.

Deze informatie kan deel uitmaken van een wederzijds akkoord tussen Isabel en een Derde, en zij kan bekend gemaakt zijn in het kader van een geheimhoudingsovereenkomst.

Onderstaande informatie blijft voorbehouden aan Abonnees op het Isabel-certificaat, Houders en Vertrouwende Partijen:

1. Isabel-certificaten en de daarin vervatte informatie.
2. Lijsten met Herroepingen van Certificaten (CRL) die herroepen Isabel-certificaten bevatten.
3. Self-signed certificaten en cross-certificaten van Isabel Certificatieautoriteiten.
4. Lijsten met Herroepingen door Autoriteiten (ARL's).

2.8.2. CATEGORIEËN INFORMATIE DIE ALS NIET-VERTROUWELIJK WORDEN AANZIEN

Onderstaande informatie is openlijk verkrijgbaar en valt dus niet onder de vertrouwelijkheidverplichtingen van deze sectie:

1. De onderhavige Isabel-CPS.
2. De Isabel-CP's.

Aangezien de onderhavige Isabel-CPS niet als een vertrouwelijk document geldt, bevat zij geen vertrouwelijke informatie.

2.8.3. BEKENDMAKING VAN INFORMATIE OVER DE HERROEPING VAN CERTIFICATEN

De redenen voor de herroeping van een certificaat worden geformuleerd in de ITU-T X.509 standaard met het extensieveld ‘Reason code’ in de CRL.

De Houder van het Isabel-certificaat of de persoon die over de volmacht beschikt van de Isabel-Klant die de herroeping van het certificaat van de Houder heeft aangevraagd, wordt op de hoogte gebracht over de herroeping van het Isabel-certificaat.

Aan de Vertrouwende Partijen mag geen andere informatie worden verstrekt dan die welke in het veld ‘Reason code’ is vermeld.

Details over het extensieveld ‘Reason code’ in de CRL zijn terug te vinden in sectie “7.2.2 - CRL/ARL en CRL/ARL extensies” van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

2.8.4. BEKENDMAKING AAN GERECHTELIJKE AMBTENAREN

Isabel-CA en RA's mogen vertrouwelijke informatie bekend maken op grond van een bevelschrift, ondertekend door een rechter of een gerechtelijk ambtenaar in het kader van een strafrechtelijk onderzoek of indien de wet dit vereist.

2.8.5. BEKENDMAKING ALS ONDERDEEL VAN EEN BURGERRECHTELIJK ONDERZOEK

Geen bepalingen.

2.8.6. BEKENDMAKING OP VERZOEK VAN DE ABONNEE/HOUDER

Isabel-CA's en RA's mogen vertrouwelijke informatie over een Abonnee/Houder van een Isabel-certificaat bekendmaken op verzoek van, of met de toestemming van deze Abonnee /Houder van een Isabel-certificaat.

2.9. ANDERE OMSTANDIGHEDEN WAARIN INFORMATIE BEKEND WORDT GEMAAKT

Geen bepalingen.

2.10. INTELLECTUELE EIGENDOMSRECHTEN

Alle informatie in dit document maakt deel uit van het intellectueel eigendomsrecht van Isabel. Dat geldt voor alle informatie die wordt gepubliceerd door Isabel, in openbaar of privaat verband.

Deze rechten reiken verder dan enige contractuele relatie die mogelijk bestaat met Isabel.

De Certificaten en toegangs- en ondertekeningsmiddelen, met inbegrip van de Publieke Sleutel, zijn het exclusieve eigendom van Isabel. Elk gebruik van de Certificaten en toegangs- en ondertekeningsmiddelen buiten de overeengekomen functionaliteiten van het Isabel-systeem moet worden opgenomen in een contract met Isabel. Wanneer alle Certificaten met betrekking tot dezelfde Publieke Sleutel vervallen of herroepen zijn, mogen de Houder, Abonnee of Klant de gegevens met betrekking tot het creëren van een handtekening na de vervaldatum of na de herroeping niet langer gebruiken om een handtekening te plaatsen, of om deze gegevens te laten certificeren door een andere certificatedienstverlener.

3. IDENTIFICATIE EN AUTHENTIFICATIE

3.1. EERSTE REGISTRATIE

Deze sectie beschrijft de voorzieningen voor identificatie en de authenticatie in het raam van de initiële registratie van een Abonnee van het Isabel-certificaat.

In het raam van deze CPS zijn er drie types Houders van Isabel-certificaten

1. Houders 'Natuurlijke personen'
2. Houders 'Functie'
3. Houder 'Applicatie'

Een natuurlijke persoon vertegenwoordigt een Houder van een Isabel-certificaat

1. In het geval de Houder een 'Natuurlijke persoon' is, wordt hij vertegenwoordigd door de natuurlijke persoon die is geïdentificeerd in het certificaat.
2. In het geval de houder een 'Functie' is, wordt hij vertegenwoordigd door de natuurlijke persoon die de functie vertegenwoordigt die is geïdentificeerd in het certificaat (vertegenwoordiger functie).
3. In het geval de Houder een 'Applicatie' is, wordt hij vertegenwoordigd door één of meer natuurlijke personen die gemachtigd zijn de applicatie te vertegenwoordigen die is geïdentificeerd in het certificaat.

3.1.1. SOORTEN NAMEN

Een Isabel-CA moet het X.500 Distinguished Name formaat gebruiken voor de velden met de namen van Subjects (Houders) en de Issuers (Uitgevers) in een Isabel-certificaat.

3.1.2. VERPLICHT GEBRUIK VAN BETEKENISVOLLE NAMEN

Een Isabel-RA moet garanderen dat de informatie betreffende de Distinguished Name die wordt ingevoerd in het veld Subject (Houder) van een Isabel-certificaat in de X.500 name space waarvoor Isabel bevoegd is, betekenisvol is.

Het Common Name veld, dat wordt gebruikt als onderdeel van de X.500 Distinguished Name voor de Houder van het Isabel-certificaat, bevat:

1. De achternaam en de voornaam voor Houders 'Natuurlijke persoon'
2. De naam van de functie voor Houders 'Functie'
3. De naam van de applicaties voor Houders 'Applicatie'

Als er een organisatie wordt vermeld, moet de informatie over de naam overeenstemmen met de "wettelijke benaming" van de organisatie, zoals die is geregistreerd conform de geldende wetten en reglementeringen.

3.1.3. REGELS VOOR HET INTERPRETEREN VAN VERSCHILLENDE NAAMFORMATEN

Zoals beschreven in sectie 3.1.1 van onderhavige Policy van de Certificatie-Activiteiten van Isabel, worden er alleen namen gebruikt in het formaat X.500 Distinguished Names.

De Distinguished Name van een Subject (Houder) van een Isabel-certificaat heeft de volgende attributen:

CN=

1. Subject's Last Name and First Name (Houder 'Fysieke persoon') of
2. Function's Name (Houder 'Functie') of
3. Application's Name (Houder 'Applicatie')

O= *Subject's Organisation name*

L=ISABEL

C=BE

Optioneel kan er ook een attribuut OU en GN aanwezig zijn.

3.1.4. UNIEK KARAKTER VAN DE NAMEN

Een Isabel-RA moet garanderen dat de Distinguished Name in het veld Subject (Houder) van een Isabel-certificaat in het X.500 namenveld waarvoor Isabel bevoegd is, uniek is.

Aan de Houders van Isabel-certificaten kunnen unieke namen worden toegekend dankzij de tools die RA agenten gebruiken en die beletten dat aan Houders van Isabel-certificaten uit dezelfde organisatie dezelfde Voornaam/Achternaam of naam van de Functie wordt toegekend.

Als een Houder van een Isabel-certificaat dezelfde Voornaam/Achternaam of Functienaam heeft als een andere Houder van een Isabel-certificaat in dezelfde organisatie, dan moet de Isabel-RA agent bij het invoeren van de informatie over de Houder van het Isabel-certificaat letters of cijfers toevoegen aan het einde van de Voornaam/Achternaam of Functienaam van de Houder van een Isabel-certificaat.

3.1.5. PROCEDURE VOOR HET OPLOSSEN VAN GESCHILLEN IN VERBAND MET NAMEN

De Isabel-CA is gemachtigd om alle geschillen in verband met Distinguished Names die worden gebruikt in het veld Subject (Houder) van Isabel-certificaten in de X.500 name space waarvoor Isabel bevoegd is, te beslechten.

3.1.6. HERKENNING, AUTHENTIFICATIE EN ROL VAN HANDELSMERKEN

RA's kunnen noch controleren, noch garanderen dat handelsmerken, dienstmerken of andere beschermde tekens in de Isabel-certificaten rechtsgeldig kunnen worden gebruikt zonder inbreuk te plegen op een intellectueel eigendomsrecht. Noch de RA, noch een CA binnen de Isabel PKI zullen verplicht zijn een dergelijk onderzoek in te stellen naar mogelijke inbreuken. Niettemin, als een Isabel-RA vermoedt dat er inbreuk wordt gepleegd op een intellectueel eigendomsrecht, heeft ze het recht de registratieprocedure op te schorten en/of te beëindigen, en te controleren of er op het eerste gezicht een intellectueel eigendomsrecht werd geschonden. De Isabel-RA heeft het recht alle wettelijke documenten op te vragen die het eigendomsrecht of het rechtsgeldige gebruik van het onderzochte recht bewijzen.

3.1.7. METHODE OM HET BEZIT VAN EEN PRIVATE SLEUTEL TE BEWIJZEN

Als het sleutelpaar werd gegenereerd door de Houder van het Isabel-certificaat, moet de Isabel-CA het bewijs ontvangen dat de Houder van het Isabel-certificaat de Private Sleutel in zijn bezit heeft die hoort bij de te certificeren Publieke Sleutel.

Aan deze vereiste wordt voldaan door de Aanvraag voor het Isabel-Certificaat te ondertekenen met de Private Sleutel die de Houder heeft aangemaakt en door de verificatie van deze handtekening door de Isabel-CA met behulp van de Publieke Sleutel van de houder die moet worden gecertificeerd en die hoort bij de Private Sleutel die werd gebruikt om de Aanvraag voor het Isabel-Certificaat te ondertekenen.

3.1.8. AUTHENTIFICATIE VAN DE IDENTITEIT VAN EEN ORGANISATIE

De Isabel-RA is verplicht de identiteit van een kandidaat-Klant te authenticeren vooraleer de Abonnees van deze Isabel-Klant Isabel-Certificaten mogen aanvragen.

De authenticatie van de identiteit van een kandidaat-Klant gebeurt in het raam van het registratieproces waaraan de ondertekening van een Isabel Service/Product contract tussen de Isabel-Klant en Isabel is onderworpen.

In het raam van dit registratieproces moet de kandidaat-Klant de volgende authenticatiestukken voorleggen aan de Isabel-RA:

1. Een naar behoren ingevuld Isabel Service/Product contract, dat de rechten en verplichtingen bevat met betrekking tot de certificatiediensten, ondertekend door de wettelijke vertegenwoordiger (of eventueel een gevolmachtigde afgevaardigde) van de kandidaat-Klant en door een vertegenwoordiger van Isabel.
2. Een ondertekende kopie van de identiteitskaart, het paspoort of een gelijkwaardig officieel document van de wettelijke vertegenwoordiger van de kandidaat-Klant (en de gevolmachtigde afgevaardigde indien van toepassing).
3. Een kopie van de toepasselijke oprichtingsakten van de kandidaat-Klant.
4. Officiële documenten die bewijzen dat de wettelijke vertegenwoordiger en, indien van toepassing, de gevolmachtigde afgevaardigde, het recht heeft te tekenen (bijvoorbeeld een uittreksel van de bijlagen bij het Belgisch Staatsblad of de notulen van een vergadering van de Raad van Bestuur).

Indien het registratieproces wordt ingezet door een gevolmachtigde afgevaardigde, moeten, naast de bovenvermelde stukken, ook de volgende documenten worden voorgelegd:

1. Een volmacht, ondertekend door een wettelijke afgevaardigde, of toegekend via een beslissing van een bedrijfsorgaan van de kandidaat-Klant, die de gevolmachtigde in staat stelt de kandidaat-Klant in dit stadium te vertegenwoordigen.
2. Een ondertekende kopie van de identiteitskaart, het paspoort of een gelijkwaardig officieel document van de gevolmachtigde.
3. Een ondertekende kopie van de identiteitskaart, het paspoort of een gelijkwaardig officieel document van de kandidaat-Klant

Zodra dit Isabel Service/Product contract is ondertekend door de kandidaat-Klant en door Isabel, wordt deze kandidaat-Klant een Isabel-Klant, ook Isabel-Abonnee genoemd.

3.1.9. AUTHENTIFICATIE VAN DE INDIVIDUELE IDENTITEIT

De identiteit van een individu wordt geauthentificeerd in het raam van het Isabel-Certificatieproces.

De Isabel-Certificatie telt 2 stadia waarin een identificatie en een authenticatie plaatsvindt van de Abonnee/Houder van het Isabel-certificaat of hun gevolmachtigde.

U vindt een overzicht van de Isabel-Certificatieprocessen in de secties, "4.1 – Aanvraag certificaat", "4.2 – Uitgifte certificaat" en "4.3 – Aanvaarding certificaat" van dit document.

3.1.9.1. HET EERSTE STADIUM VAN AUTHENTIFICATIE

Dit is de fase waarin de Aanvrager van het Isabel-certificaat een aanvraag indient voor een Isabel-certificaat bij een Isabel-RA.

In dit stadium wordt de Abonnee van het Isabel-certificaat door de Isabel-RA geauthentificeerd op basis van een persoonlijke authenticatie of elk ander geldig identificatiemiddel.

De Abonnee van het Isabel-certificaat moet de volgende authenticatiedocumenten voorleggen aan de Isabel-RA:

1. Een volledig ingevulde Aanvraag voor een Isabel-certificaat, ondertekend door de Abonnee van het Isabel-certificaat en ondertekend door de natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt:

- a. In het geval de Houder een 'Natuurlijke persoon' is, wordt hij vertegenwoordigd door de natuurlijke persoon die is geïdentificeerd in het certificaat.
- b. In het geval de houder een 'Functie' is, wordt hij vertegenwoordigd door de natuurlijke persoon die de functie vertegenwoordigt zoals deze is geïdentificeerd in het certificaat (vertegenwoordiger functie).
- c. In het geval de Houder een 'Applicatie' is, wordt hij vertegenwoordigd door één of meer natuurlijke personen die gemachtigd zijn de applicatie te vertegenwoordigen zoals deze is geïdentificeerd in het certificaat.

Waarbij beiden zich houden aan alle procedures, bepalingen en policies in verband met Isabel-certificaten.

2. Een ondertekende kopie en voorlegging van het origineel van de identiteitskaart, het paspoort of een gelijkwaardig officieel document van de Aanvrager van het Isabel-certificaat of de natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt.
3. Een officieel document dat bewijst dat de Houder die een Isabel-certificaat aanvraagt, een professionele status heeft of deel uitmaakt van een bepaalde klant van Isabel (bijvoorbeeld een uittreksel uit het Handelsregister of elk ander gelijkwaardig officieel document).

Voor buitenlandse Houders/Aanvragers van Isabel-certificaten kan bijkomend een voorafgaande authenticatie van deze documenten vereist zijn door een notaris, of een andere functionaris met gelijkwaardige bevoegdheid binnen het rechtsgebied van de Houder/Aanvrager. Ook een officiële (Nederlandse) vertaling kan vereist zijn voor documenten die werden opgesteld in de lokale taal.

Als het certificatieproces wordt ingezet door een afgevaardigde met volmacht, zijn, naast de bovenvermelde stukken, de volgende documenten vereist:

1. Een volmacht, ondertekend door een wettelijke vertegenwoordiger van de Isabel-Klant die de gevolmachtigde in staat stelt de Isabel-Klant in dit stadium te vertegenwoordigen.
2. Een ondertekende kopie en voorlegging van de originele identiteitskaart, het paspoort of een gelijkwaardig officieel document van de gevolmachtigde.

3.1.9.2. HET TWEDE STADIUM VAN AUTHENTICATIE

In het tweede stadium van de authenticatie wordt de natuurlijke persoon die de Houder van het Isabel-certificaat, of zijn gevolmachtigde vertegenwoordigt, door de Isabel-RA geauthenticeerd op basis van een persoonlijke authenticatie of een ander geldig identificatiemiddel.

De natuurlijke persoon die de Houder van het Isabel-certificaat, of zijn gevolmachtigde vertegenwoordigt, moet de volgende authenticatiedocumenten voorleggen aan de Isabel-RA: ondertekende kopie en voorlegging van de originele identiteitskaart, het paspoort of een gelijkwaardig officieel document van de natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt.

In het geval de natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt, op zijn beurt wordt vertegenwoordigd door een gevolmachtigde, moeten tevens de volgende documenten worden voorgelegd:

1. Een volmacht, ondertekend door de natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt en die de gevolmachtigde in staat stelt deze persoon te vertegenwoordigen.
2. Een ondertekende kopie en voorlegging van de originele identiteitskaart, het paspoort of een gelijkwaardig officieel document van de gevolmachtigde.

3.2. HERSTARTEN VAN DE CERTIFICATIEPROCEDURE

Deze sectie beschrijft de bepalingen inzake identificatie en authenticatie in het raam van de hernieuwing van een Isabel-certificaat voor een Houder die reeds werd geregistreerd.

3.2.1. AUTOMATISCHE HERNIEUWING VAN HET ISABEL-CERTIFICAAT

Een Isabel-certificaat dat niet werd herroepen, wordt door de Isabel-CA die het certificaat uit geeft, automatisch hernieuwd aan het einde van de geldigheidsperiode van het certificaat. In het raam van dit Hernieuwingsproces van Isabel-certificaten wordt dezelfde Publieke Sleutel opnieuw gecertificeerd.

De Isabel-CA authenticereert haar eigen hernieuwingsaanvragen voor certificaten.

3.2.2. HERNIEUWING VAN HET SLEUTELPAAR

Een Houder van een Isabel-certificaat wiens sleutelbaar lokaal werd gegenereerd door een Isabel tool op zijn/haar werkpost, of centraal door een Isabel CA, kan zijn/haar sleutelbaar lokaal hernieuwen met behulp van een Isabel tool op zijn/haar werkpost, op voorwaarde dat hij/zij beschikt over een geactiveerde Isabel Secure Signing Card.

3.2.3. HERNIEUWING VAN DE ISABEL SECURE SIGNING CARD

Als de Houder van een Isabel-certificaat zich in een situatie bevindt waarin hij niet langer in een positie is om gebruik te maken van zijn/haar Isabel Secure Signing Card en een nieuwe kaart nodig heeft, moet de Abonnee van een Isabel-certificaat een volledig ingevuld en getekend bestelformulier naar de Isabel-RA sturen per fax of per post.

De Isabel-RA authenticereert het bestelformulier, herroept het Isabel-certificaat dat bij de te hernieuwen Isabel Secure Signing Card hoort en herstart de certificatieprocedure voor de Houder.

3.3. HERSTARTEN CERTIFICATIEPROCEDURE NA HERROEPING

De Houder van een Isabel-certificaat wiens Isabel-certificaat werd herroepen en die een nieuw Isabel-certificaat wil aanvragen, moet opnieuw het volledige Isabel-Certificatieproces doorlopen en moet opnieuw worden geauthentificeerd conform de bepalingen vermeld in sectie "3.1.9 - Authenticatie van de individuele identiteit".

3.4. AANVRAAG VOOR HERROEPING

Deze sectie beschrijft de bepalingen inzake identificatie en authenticatie in het raam van de herroeping van een Isabel-certificaat.

Isabel biedt aan zijn klanten twee wijzen voor het herroepen van een Isabel Certificaat aan :

1. een herroepings service aangeboden door de Isabel-RA,
2. een herroepings service aangeboden door een Isabel Revocatie Service.

3.4.1. AUTHENTICATIE DOOR DE ISABEL-RA

De Houder of de bevoegde vertegenwoordiger van de Isabel-Klant waaraan de Houder verbonden is moet de volgende authenticatiedocumenten verstrekken aan de Isabel-RA voor de herroeping van het Isabel-certificaat van de Houder: volledig ingevuld formulier voor de herroeping van het Isabel-certificaat, op papier, verstuurd via fax of via de post, met de handgeschreven handtekening van de Houder van het Isabel-certificaat of de bevoegde vertegenwoordiger van de Isabel-Klant van de Houder.

De Isabel-RA authenticereert de aanvraag voor herroeping die werd verstuurd door de Houder of de bevoegde vertegenwoordiger op basis van de handgeschreven handtekening op de aanvraag voor herroeping.

Als de aanvraag voor herroeping is geauthentificeerd door een Isabel-RA agent, gebruikt de Isabel-RA agent een Isabel tool om een elektronische aanvraag voor herroeping te genereren, te tekenen met zijn/haar Private Sleutel en te versturen naar de geëigende Isabel-CA.

3.4.2. AUTHENTIFICATIE DOOR EEN ISABEL REVOCATIE SERVICE

Isabel heeft een Revocatie Service die 24 uur op 24 ter beschikking staat van haar klanten. Deze service wordt uitgevoerd door Card Stop. Deze service garandeert dat de revocatie wordt geïnitieerd binnen het uur na de aanvraag van de Klant.

De Isabel Revocatie Service is niet beschikbaar voor Isabel Klanten die tot de WISE communiteit behoren.

De Revocatie Service bestaat uit twee fasen :

1. Een herroepingfase
2. Een bevestigingsfase

3.4.2.1. DE HERROEPINGSFASE : AUTHENTIFICATIE EN IDENTIFICATIE

Tijdens deze fase voert de Revocatie Service de volgende acties uit:

1. de authenticatie van de beller,
2. de identificatie van de certificaten die moeten herroepen worden, en
3. het herroepen van de certificaten in geval van correcte identificatie en authenticatie, of
4. het niet herroepen in geval van onvoldoende identificatie en/of authenticatie.

De Revocatie Service identificeert de certificaten die moeten herroepen worden, gebaseerd op een aantal identificatie vragen die gesteld worden aan de beller. De volgende informatie wordt gevraagd:

1. CardID van de Secure Signing Card waarop de Private Sleutel staat waarvoor het Public Sleutel certificaat moet herroepen worden, en
2. UserID van de Certificaat Houder wiens certificaten moeten herroepen worden, en
3. SubscriptionID van het abonnement waartoe de gebruiker behoort, en de naam van de Certificaat Houder, en
4. Naam van het Abonnement tot hetwelk de Certificaat Houder behoort.

De revocatie wordt uitgevoerd naar best vermogen, indien de beller voldoende informatie heeft doorgegeven om geauthenticeerd te worden en om eenduidig de certificaten die moeten herroepen worden te identificeren.

3.4.2.2. DE BEVESTIGINGSFASE

De werkdag volgend op de dag van de herroeping, wordt een bevestigingsprocedure opgestart. De certificaatverantwoordelijke wordt gecontacteerd om de herroeping te confirmeren via fax.

De fax die teruggestuurd wordt door de certificaatverantwoordelijke wordt geverifieerd; succesvolle verificatie leidt tot de finalisatie van de herroeping, en indien noodzakelijk, het verzenden van een nieuwe Isabel Secure Signing Card.

In geval de herroeping niet bevestigd wordt door de certificaatverantwoordelijke, BV. Indien het herroepen certificaat onterecht herroepen werd, kan de reactivatie van het certificaat aangevraagd worden.

3.4.2.3. NIET UITGEVOERDE HERROEPINGEN

In geval de herroeping om eender welke reden niet kan uitgevoerd worden, wordt een onderzoek opgestart vanaf de volgende werkdag.

3.4.3. AUTHENTIFICATIE DOOR DE ISABEL-CA

De Isabel-CA authentificeert een aanvraag voor herroeping op basis van een elektronische handtekening die werd gegenereerd met de Private Sleutel van de Isabel-RA agent of de Revocatie Service en gecontroleerd met het certificaat van de Isabel-RA agent of de Revocatie Service.

Wanneer de aanvraag voor herroeping is geauthentificeerd door een Isabel-CA, herroept de Isabel-CA het Isabel-certificaat en publiceert het herroepen Isabel-certificaat en de geactualiseerde Lijst met Herroepingen van de Isabel-certificaten in de Isabel directory. De Lijst met Herroepingen (Certificate Revocation List - CRL) wordt door de Isabel-CA ondertekend om de integriteit van de CRL te garanderen.

4. OPERATIONELE BEPALINGEN

In het raam van de onderhavige Policy van de Certificatie-Activiteiten van Isabel worden 3 certificatieprocedures ondersteund die de toepassing, de uitgifte en de aanvaarding van Isabel-certificaten dekken:

1. De 'Gecentraliseerde' Certificatieprocedure waarbij het sleutelbaar van de Houder 'Natuurlijke Persoon' of 'Functie' centraal wordt gegenereerd door een Isabel-CA.
2. De 'Gedecentraliseerde' Certificatieprocedure waarbij het sleutelbaar van de Houder 'Natuurlijke Persoon' of 'Functie' wordt gegenereerd door de natuurlijke persoon die de Houder vertegenwoordigt op zijn/haar werkpost.
3. De 'Manuele' Certificatieprocedure waarbij het sleutelbaar van de Houder 'Natuurlijke Persoon', 'Functie' of 'Applicatie' wordt gegenereerd door de natuurlijke persoon die de Houder vertegenwoordigt en wordt opgeslagen in een Isabel Tamper Resistant Device of in een hardwarematige veiligheidsmodule van derden.

De 3 eerste secties van dit hoofdstuk beschrijven de Toepassing, Uitgifte en Aanvaarding van Isabel-certificaten in het raam van de bovenvermelde certificatieprocedures.

De vierde sectie beschrijft het Herroepingsproces voor Isabel-certificaten.

De 4 volgende secties van dit hoofdstuk geven een overzicht van de activiteiten in verband met:

1. Procedures security audit
2. Archiveren van gegevens
3. Wijziging sleutel
4. Compromittering en Disaster Recovery

Meer details over deze controles zijn vervat in de documenten [6] tot [9]. Deze documenten zijn niet publiek toegankelijk, maar kunnen worden geconsulteerd op grond van een gemotiveerd verzoek, dat werd goedgekeurd door de Isabel Security Manager.

De gedetailleerde informatie of activiteiten bevinden zich niet in de onderhavige Policy van de Certificatie-Activiteiten van Isabel, die niet is onderworpen aan vertrouwelijkheidsbeperkingen.

4.1. AANVRAAG CERTIFICAAT

Met betrekking tot het proces van de Aanvraag voor een Isabel-certificaat, zal de Abonnee van een Isabel-certificaat de voorwaarden en verplichtingen respecteren van de toepasselijke CP en elke contractuele overeenkomst.

Tijdens de Aanvraag zal het identificatie- en authenticatieproces plaatsvinden dat wordt beschreven in hoofdstuk 3.

De Aanvraag van een Isabel-certificaat kan het aanmaken van een sleutelbaar door de Isabel-CA of Isabel Agent of de uitgifte van een Isabel Secure Signing Card door de Isabel-CA al of niet omvatten.

De Aanvraag van een Isabel-certificaat zal leiden tot de uitgifte van een Isabel-certificaat en tot de publicatie van het Isabel-certificaat in de Isabel Repository.

Het aanvraagproces voor een Isabel-certificaat hangt niet af van de gekozen certificatieprocedure.

De aanvraag voor een Isabel-certificaat kan plaatsvinden in 2 verschillende contexten:

4.1.1. AANVRAAG VAN EEN ISABEL-CERTIFICAAT VOOR EEN NIEUWE HOUDER

Een Abonnee van een Isabel-certificaat vraagt een Isabel-certificaat aan voor een **nieuwe** Isabel Houder 'Natuurlijke Persoon', 'Functie' of 'Applicatie'.

Indien de Isabel-Abonnee behoort tot een kandidaat Isabel-Klant, moet een bevoegde vertegenwoordiger van de kandidaat Isabel-Klant de authenticatiedocumenten, gespecificeerd in sectie “3.1.8 – Authenticatie van de identiteit van een organisatie” van onderhavige Isabel-CPS, voorleggen aan de Isabel-RA na identificatie en authenticatie van de bevoegde vertegenwoordiger.

De Abonnee van een Isabel-certificaat die een Isabel-certificaat aanvraagt voor een **nieuwe** Isabel Houder ‘Natuurlijke Persoon’, ‘Functie’ of ‘Applicatie’, moet de authenticatiedocumenten, gespecificeerd in sectie “3.1.9.1 – Het eerste stadium van authenticatie” van onderhavige Isabel-CPS, voorleggen aan de Isabel-RA na persoonlijke identificatie, authenticatie of elk ander geldig identificatiemiddel.

4.1.2. AANVRAAG VAN EEN ISABEL-CERTIFICAAT VOOR EEN BESTAANDE HOUDER

De Abonnee van een Isabel-certificaat vraagt een Isabel-certificaat aan voor een **bestaande** Isabel Houder ‘Natuurlijke Persoon’, ‘Functie’ of ‘Applicatie’.

De Abonnee van een Isabel-certificaat moet de authenticatiedocumenten, beschreven in sectie “3.2.3 – Hernieuwing van de Isabel Secure Signing Card” van onderhavige Isabel-CPS, voorleggen aan de Isabel-RA.

4.2. UITGIFTE CERTIFICAAT

De uitgifte van een Isabel-certificaat hangt af van de gekozen certificatieprocedure.

4.2.1. GECENTRALISEERDE CERTIFICATIEPROCEDURE

De Gecentraliseerde Certificatieprocedure geldt voor Houders ‘Natuurlijke Persoon’ en ‘Functie’.

1. Na controle van de aanvraagdocumenten, zoals beschreven in sectie “4.1 – Aanvraag certificaat”, start een Isabel-RA agent de gecentraliseerde certificatieprocedure voor de Houder.
2. Het Isabel-CA-systeem genereert het sleutelpaar, het Isabel-certificaat en de PIN-code van de Houder centraal en personaliseert de Isabel Secure Signing Card: laadt het sleutelpaar, de PIN-code en de Isabel-CA Publieke Sleutel op de chip van de Isabel Secure Signing Card.
3. De Isabel-CA stuurt de envelop met de Isabel Secure Signing Card naar de Isabel-RA, de RA die zorgt voor de distributie naar de Titularis.
4. De Isabel-CA stuurt de initiële PIN-code van de Houder in een beveiligde envelop naar het kantooradres van de natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt. Deze envelop bevat ook een uitnodiging voor de natuurlijke persoon die de Houder vertegenwoordigt, om zijn/haar Isabel Secure Signing Card af te halen bij een Isabel-RA.
5. De natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt moet zijn/haar Isabel Secure Signing Card verplicht afhalen bij de Isabel-RA. De Houder van het Isabel-certificaat, of zijn/haar gevolmachtigde, moet de authenticatiedocumenten, beschreven in sectie “3.1.9.2 – Het tweede stadium van authenticatie” van onderhavige Policy van de Certificatie-Activiteiten van Isabel, bezorgen aan de Isabel-RA agent.

4.2.2. GEDECENTRALISEERDE CERTIFICATIEPROCEDURE

De Gedecentraliseerde Certificatieprocedure geldt voor Houders ‘Natuurlijke Persoon’ en ‘Functie’.

Vooraleer de Gedecentraliseerde Certificatieprocedure kan worden gestart, moet een blanco Isabel Secure Signing Card, geleverd zijn aan de Houder van het Isabel-certificaat Subject.

1. Na controle van de aanvraagdocumenten, zoals beschreven in sectie “4.1 – Aanvraag certificaat”, start de Isabel-RA agent de gedecentraliseerde certificatieprocedure voor de Houder.

2. De natuurlijke persoon die de Houder vertegenwoordigt, gebruikt een Isabel tool om zijn/haar sleutelbaar aan te maken op zijn/haar werkpost. De Isabel tool slaat het sleutelbaar van de Houder op de Isabel Secure Signing Card van de Houder.
3. De Houder van het Isabel-certificaat gebruikt een Isabel tool om de Publieke Sleutel van de Houder veilig door te sturen naar het systeem van de Isabel-CA en de Publieke Sleutel van de Isabel-CA veilig op te halen uit het systeem van de Isabel-CA-systeem. De Isabel tool slaat de Publieke Sleutel van de Isabel-CA op de Isabel Secure Signing Card van de Houder.
4. De Isabel-RA nodigt de natuurlijke persoon die de Houder vertegenwoordigt uit om het document, dat 2 geheime activeringscodes bevat, op te halen.
De natuurlijke persoon die de Houder van het Isabel-certificaat, of zijn/haar gevolmachtigde vertegenwoordigt, moet de Isabel-RA de authenticatiedocumenten bezorgen die worden beschreven in sectie "3.1.9.2 – Het tweede stadium van authenticatie" van onderhavige Policy van de Certificatie-Activiteiten van Isabel.
5. De Houder van het Isabel-certificaat gebruikt een Isabel tool om de 2 geheime activeringscodes te authenticeren en bevestigt zijn/haar aanvraag voor een certificaat aan het systeem van de Isabel-CA.

Na controle genereert het systeem van de Isabel-CA het Isabel-certificaat van de Houder en publiceert het in de Isabel directory.

4.2.3. MANUELE CERTIFICATIEPROCEDURE

De Manuele Certificatieprocedure geldt voor Houders 'Natuurlijke Persoon', 'Functie' en 'Applicatie'.

1. Na controle van de aanvraagdocumenten, zoals beschreven in sectie "4.1 – Aanvraag certificaat", start de Isabel-RA agent de manuele certificatieprocedure voor de Houder.
2. De natuurlijke persoon die de Houder vertegenwoordigt, gebruikt een tool van Isabel of van een derde om het sleutelbaar van de Houder te genereren, ontvangt op een veilige manier de Isabel-CA Publieke Sleutel, slaat het sleutelbaar van de Houder en de Isabel-CA Publieke Sleutel op in een Isabel Tamper Resistant Device of een hardware veiligheidsmodule van derden en maakt een diskette aan met een certificaataanvraag voor de Publieke Sleutel van de Houder.
3. De natuurlijke persoon die de Houder vertegenwoordigt, brengt de diskette met de certificaataanvraag naar de kantoren van de Isabel-CA.

Na een persoonlijke authenticatie van de natuurlijke persoon die de Houder vertegenwoordigt door de RA agent, die eveneens aanwezig is in de kantoren van de Isabel-CA, genereert de Isabel-CA het Isabel-certificaat van de Houder en publiceert het in de Isabel directory.

De natuurlijke persoon die de Houder van het Isabel-certificaat of zijn/haar gevolmachtigde vertegenwoordigt, moet de Isabel-CA de authenticatiedocumenten bezorgen die worden beschreven in sectie "3.1.9.2 – Het tweede stadium van authenticatie" van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

4.3. AANVAARDING CERTIFICAAT

De aanvaarding van zijn/haar Isabel-certificaat door de Houder hangt af van de gekozen certificatieprocedure: zie verder. Elke certificatieprocedure bevat een garantie dat de Houder de Publieke Sleutel en het certificaat van de Isabel-CA zal ontvangen.

4.3.1. GECENTRALISEERDE CERTIFICATIEPROCEDURE

In de Gecentraliseerde Certificatieprocedure wordt de aanvaarding van het Isabel-certificaat door de Houder van het Isabel-certificaat gerealiseerd via expliciete kennisgeving van aanvaarding door de Houder van het Isabel-certificaat:

De natuurlijke persoon die de Houder van het Isabel-certificaat vertegenwoordigt, gaat naar het systeem van de Isabel-CA en authenticereert zich met behulp van een elektronische handtekening op basis van zijn/haar Private Sleutel, die is opgeslagen op zijn/haar Isabel Secure Signing Card.

Het systeem van de Isabel-CA toont het Isabel-certificaat aan zijn/haar Houder en vraagt hem/haar zijn/haar Isabel-certificaat te aanvaarden.

Zodra de Houder van het Isabel-certificaat zijn/haar Isabel-certificaat heeft aanvaard, wordt het certificaat van de Houder naar zijn/haar werkpost gestuurd en door de Isabel-CA gepubliceerd in de Isabel Directory.

4.3.2. GEDECENTRALISEERDE CERTIFICATIEPROCEDURE

Zodra de Isabel-CA de bevestiging heeft ontvangen van de certificaataanvraag van de Houder, geauthentificeerd met de 2 geheime activeringscodes, publiceert ze het Isabel-certificaat van de Houder in de Isabel directory. De Houder van het Isabel-certificaat download zijn/haar Isabel-certificaat van de Isabel directory met behulp van een Isabel tool.

In de Gedecentraliseerde Certificatieprocedure wordt de aanvaarding van het Isabel-certificaat door de Houder gerealiseerd, hetzij door het gebruik van het Certificaat door de Houder, hetzij na de 10^{de} dag te rekenen vanaf de publicatie in de Isabel Directory zonder tegenbericht of opmerkingen van de Houder.

4.3.3. MANUELE CERTIFICATIEPROCEDURE

In de Manuele Certificatieprocedure wordt de aanvaarding van het Isabel-certificaat door de Houder gerealiseerd, op het ogenblik van de manuele certificatie, waar de vertegenwoordiger van de Houder van het Certificaat een document moet ondertekenen dat de inhoud van het Certificaat van de Houder bevat. Na het ondertekenen wordt het Certificaat in de Isabel Directory gepubliceerd.

4.4. HERROEPING CERTIFICAAT

De herroeping van een Isabel-certificaat is definitief en onomkeerbaar.

4.4.1. OMSTANDIGHEDEN VOOR HERROEPING

De herroeping van een Certificaat van een Isabel-houder 'Natuurlijke Persoon', 'Functie', of 'Applicatie' zal altijd plaatsvinden na een definitieve beslissing van een Isabel-RA of een Revocatie Service.

Een Certificaat van een Isabel-houder moet worden herroepen als:

1. De Private Sleutel van de houder werd gecorrumpeerd of als de vertrouwelijkheid ervan niet langer is gewaarborgd.
2. De gecertificeerde informatie niet langer toepasselijk of geldig is.
3. De Private Sleutel van de houder werd vervangen.
4. De Houder geen deel meer uitmaakt van een Klant van Isabel of als de Klant van Isabel zijn activiteiten heeft stopgezet.
5. Het Isabel-certificaat werd afgeleverd op basis van onjuiste of valse informatie.
6. Andere mogelijke redenen zijn: BV. de Houder heeft zijn/haar Isabel Secure Signing Card onbruikbaar gemaakt, namelijk hij heeft meer dan 5 opeenvolgende ongeldige Pincodes ingevoerd.

4.4.2. WIE KAN HERROEPING AANVRAGEN

De herroeping van het Certificaat van een Isabel-houder 'Natuurlijke Persoon', 'Functie' en 'Applicatie' kan worden aangevraagd door :

1. De natuurlijke persoon die is geïdentificeerd in een Certificaat met Houder 'Natuurlijke Persoon'.
2. De natuurlijke persoon die een Functie- of Applicatiecertificaat vertegenwoordigt.

3. Elke fysieke persoon die door een Isabel-Klant is gemachtigd om de herroeping van zijn Houder-certificaten aan te vragen.
4. Elke Isabel-RA.
5. De Isabel-CA die het certificaat heeft uitgegeven.

4.4.3. PROCEDURE VOOR HERROEPINGSAANVRAAG

De procedure voor herroepingaanvraag wordt beschreven in de secties “3.4.1 - Authenticatie door de Isabel-RA”, “3.4.2 –Authenticatie door een Isabel Revocatie Service” en “3.4.3 - Authenticatie door de Isabel-CA” van onderhavig document.

4.4.4. UITSTEL HERROEPINGSAANVRAAG

Er is geen uitstel toegestaan.

4.4.5. OMSTANDIGHEDEN VOOR OPSCHORTING

De opschorting van het certificaat wordt niet ondersteund in de Isabel-PKI.

4.4.6. UITGIFTEFREQUENTIE CRL

De uitgiftefrequentie van de CRL vindt u in sectie “2.1.1.12 – Informatie betreffende de herroeping van een Isabel-certificaat publiceren in een Isabel Repository”.

4.5. SECURITY AUDIT PROCEDURES

4.5.1. SOORTEN GEBEURTENISSEN DIE WORDEN GEREGISTREERD

De Isabel-CA en de Registratieautoriteiten registreren alle gebeurtenissen betreffende een Isabel-certificaat in audit logs. Deze gebeurtenissen worden geregistreerd voor een bepaalde periode, met name om het bewijs te kunnen leveren van certificering of herroeping in verband met gerechtelijke acties. Zie ook [2] voor de vereisten die de Belgische nationale wetgeving stelt in verband met het registreren van gebeurtenissen.

Ook belangrijke gebeurtenissen in verband met de omgeving van de Isabel-CA, het beheer van de sleutel en de certificaten worden geregistreerd, en met name:

1. Alle gebeurtenissen in verband met de levenscyclus van CA-sleutels.
2. Alle gebeurtenissen in verband met de levenscyclus van Isabel-certificaten.
3. Alle gebeurtenissen in verband met de voorbereiding van Isabel Secure Signature Creation Devices.
4. Alle verzoeken en verslagen in verband met herroepingaanvragen, evenals de daaruit voortvloeiende actie.

De Isabel-CA zorgt ervoor dat alle gebeurtenissen aangaande de registratie, inclusief certificaataanvragen, automatische hernieuwing of hernieuwing van certificaten worden geregistreerd, en meer bepaald dat:

1. Document(en) die door de Abonnee van een Isabel-certificaat worden voorgelegd aan de Isabel-RA of de Isabel-CA in verband met de registratie.
2. De plaats waar kopies van identificatiedocumenten worden bewaard, inclusief de ondertekende Aanvraag van een Isabel-certificaat.
3. Alle specifieke keuzes in de aanvraag van de Abonnee.
4. De identiteit van de Isabel-Klant die de Aanvraag van een Isabel-certificaat heeft aanvaard.

5. De methode die wordt gebruikt om eventuele identificatiedocumenten te valideren.
6. De naam van de CA die de documenten ontvangt en/of de RA die de documenten verstuurt, indien van toepassing.

De details van de gebeurtenissen en gegevens die worden geregistreerd worden beschreven in [6].

4.5.2. FREQUENTIE VAN HET VERWERKEN VAN DE LOGS

Het bevoegde personeel van de Isabel-CA controleert geregeld de audit logs, ten minste één keer per week. De details in verband met de frequentie van de controle van de event logs worden beschreven in [6].

4.5.3. BEWAARPERIODE VOOR DE AUDIT LOG

De bewaarperiode van de audit logs is vermeld in sectie “4.6.2 – Bewaarperiode archieven”.

4.5.4. BESCHERMING VAN AUDIT LOGS

De vertrouwelijkheid en de integriteit van actuele en gearchiveerde gebeurtenissen betreffende Isabel-certificaten wordt gewaarborgd door de mechanismen voor toegangscontrole die de verwerking en de toegang tot de audit logs uitsluitend beperken tot het bevoegde personeel van Isabel.

De audit logs worden elektronisch gedateerd en ondertekend. Om te beletten dat ze worden gewijzigd, worden er van de audit logs verschillende back ups gemaakt.

4.5.5. BACK-UPPROCEDURES AUDIT LOG

Isabel zorgt ervoor dat er geregeld een back-up wordt gemaakt van de audit log. Er worden dagelijks, wekelijks, maandelijks en jaarlijks back-ups gemaakt van de audit logs en de dragers worden binnen en buiten de back-up site bewaard.

4.5.6. COLLECTION SYSTEEM AUDIT (INTERN VERSUS EXTERN)

Het collection systeem voor de audit logs is geïntegreerd in het Isabel-CA-systeem.

4.5.7. KENNISGEVING AAN DE HOUDER DIE EEN GEBEURTENIS VEROORZAAKT

Isabel is niet verplicht de persoon, het systeem of de applicatie op de hoogte te brengen als hij/zij/het een gebeurtenis zou hebben veroorzaakt die werd geregistreerd door het auditsysteem van Isabel.

4.5.8. BEOORDELING ZWAKKE PUNTEN

Er worden geregeld veiligheidscontroles uitgevoerd op de Isabel-RA/CA-systemen en procedures, conform de Isabel security policies beschreven in [10] en [11]. Zie ook sectie “2.7 – Conformiteitsaudits” van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

4.6. ARCHIVEREN VAN GEGEVENS

4.6.1. SOORTEN GEBEURTENISSEN DIE WORDEN GEREGISTREERD

De volgende elementen worden gearhiveerd:

1. Isabel-certificaten
2. Lijst met Herroepingen van de Isabel-certificaten
3. Isabel Certificaat-Policies
4. Policy van de Certificatie-Activiteiten van Isabel
5. Alle gebeurtenissen en verzoeken die leiden tot wijzigingen in Isabel-certificaten en Lijsten met Herroepingen van de Isabel-certificaten

4.6.2. BEWAARPERIODE ARCHIEVEN

Alle informatie in verband met Isabel-certificaten wordt minstens voor een periode van 10 jaar gearhiveerd.

4.6.3. BEVEILIGING VAN DE ARCHIEVEN

De elektronische en papieren archieven worden beveiligd met fysieke en logische mechanismen voor toegangscontrole om ongeoorloofde toegang te beletten. De archieven zijn beveiligd tegen omgevingsbedreigingen, zoals temperatuur, brand, overstroming, vocht en magnetische straling.

4.6.4. BACK-UPPROCEDURES ARCHIEVEN

Er bestaan verschillende kopieën van de archieven om de beschikbaarheid te garanderen.

De archieven worden geregeld herschreven op hedendaagse media om de bewaarperiode te garanderen en om te beletten dat de media-infrastructuur veroudert.

4.6.5. VEREISTEN VOOR HET DATEREN VAN GEGEVENS

De gearhiveerde informatie wordt elektronisch gedateerd en ondertekend.

4.6.6. COLLECTION SYSTEEM (INTERN VERSUS EXTERN)

Het collection systeem van de archieven is geïntegreerd in het Isabel-CA-systeem.

4.6.7. PROCEDURES OM GEARCHIVEERDE INFORMATIE TE VERKRIJGEN EN TE CONTROLEREN

De Houder van het Isabel-certificaat zal toegang krijgen tot de informatie die over hem werd gearhiveerd, zonder de algemene vertrouwelijkheidsverplichtingen van de Isabel-CA's en RA's in het gedrang te brengen. Alle verzoeken om gearhiveerde informatie te verkrijgen, moeten schriftelijk worden gericht aan de Isabel Security Manager.

De gearhiveerde informatie moet geregeld worden gecontroleerd om de beschikbaarheid van de gearhiveerde informatie te waarborgen tijdens de retentieperiode, zoals vermeld in sectie 4.6.2 van onderhavig document.

4.7. SLEUTEL CHANGEOVER

De Isabel-CA zorgt ervoor dat zijn private sleutels voor ondertekening niet worden gebruikt nadat hun levenscyclus is geëindigd. Als een private sleutel van een Isabel-CA het einde van zijn levenscyclus heeft bereikt, wordt het certificaat herroepen.

Het genereren en vervangen van een sleutelpaar van een Isabel-CA wordt beschouwd als bedrijfsgeheim.

4.8. COMPROMITTERING EN DISASTER RECOVERY

In geval van een disaster, inclusief de compromittering van de private sleutel van de CA, beschikt de Isabel-CA over policies en procedures om de operaties zo vlug mogelijk te restaureren, zoals beschreven in [10], [11], [12] en [13].

4.9. STOPZETTING CA

Als een Isabel-CA zijn activiteiten stopzet, zal Isabel handelen zoals bepaald door de Belgische nationale wetgeving, zie [2].

5. FYSIEKE, PROCEDURE- EN PERSONEELSMATREGELEN I.V.M. DE VEILIGHEID

5.1. FYSIEKE MATREGELEN

De Isabel-CA beschikt over policies en procedures om te verzekeren dat de fysieke toegang tot kritische diensten wordt gecontroleerd en de fysieke risico's met betrekking tot zijn bezittingen maximaal worden beperkt, zoals beschreven in [10] en [12].

5.2. PROCEDURELE MATREGELEN

5.2.1. VERTROUWELIJKE FUNCTIES EN VERANTWOORDELIJKHEDEN

De functies van de Isabel-CA die in de volgende secties worden beschreven moeten worden vervuld door betrouwbaar personeel.

5.2.1.1. CA OPERATOR

Deze personen treden op als operators van het Isabel-CA-systeem en gebruiken de CA-werkpost onder tweevoudige controle. Er zullen twee groepen van CA Operators zijn.

5.2.1.2. CA SYSTEM ADMINISTRATOR

Deze personen beheren het Isabel-CA-systeem met behulp van de console.

5.2.1.3. CA SECURITY OFFICER

Deze personen implementeren de CA-policies, staan in voor de conformiteit met de Isabel-CP en CPS, en controleren de audit logs.

5.2.2. IDENTIFICATIE EN AUTHENTIFICATIE VOOR ELKE FUNCTIE

Vertegenwoordigers van elke functie worden geauthenticeerd met een elektronische handtekening die wordt gegenereerd met hun Private Sleutel, die is opgeslagen op een Isabel Secure Signing Card.

5.3. PERSONEELSCONTROLES

Isabel zorgt ervoor dat het personeel en de aanwervingprocedures de betrouwbaarheid van haar activiteiten verbeteren en ondersteunen, door het personeel richtlijnen op te leggen die worden beschreven in [13].

Deze richtlijnen voor het personeel bevatten een specifieke vertrouwelijkheidsovereenkomst.

6. TECHNISCHE VEILIGHEIDSMATREGELEN

6.1. AANMAKEN EN INSTALLEREN VAN HET SLEUTELPAAR

6.1.1. AANMAKEN EN AFLEVEREN VAN DE SLEUTEL

Het sleutelbaar van de Houder wordt hetzij centraal gegenereerd door de Isabel-CA, hetzij lokaal door de Houder zelf. De Isabel-certificatieprocedures (zie hoofdstuk 4 - Operationele bepalingen) garanderen dat de Private Sleutel van de Houder en de Publieke Sleutel van de Isabel CA in beide gevallen op een veilige manier worden overgemaakt aan de Houder en dat de Publieke Sleutel van de Houder op een veilige manier wordt overgemaakt aan de Isabel-CA.

6.1.2. LENGTE VAN DE SLEUTELS

De RSA Publieke Sleutel (modulus n), gecertificeerd door een Isabel-certificaat heeft een lengte van minimum 512 bits.

De RSA Publieke Sleutel (modulus n), gecertificeerd door een Isabel-certificaat voor een Isabel Secure Signing Card heeft een lengte van minimum 1024 bits.

De Isabel-CA-sleutels hebben een lengte van 2048 bits.

6.1.3. AANMAKEN VAN DE SLEUTELS

De informatie over het proces voor het aanmaken van sleutels van Isabel is eigendom van Isabel.

De kwaliteit van dit proces werd gecontroleerd.

De kwaliteit van de parameters van dit proces wordt permanent bewaakt.

6.2. BESCHERMING VAN DE PRIVATE SLEUTEL

6.2.1. STANDAARDEN VOOR VERSLEUTELINGSMODULES

Conform onderhavige Policy van de Certificatie-Activiteiten van Isabel, moet de Private Sleutel van de Houder van het Isabel-certificaat hetzij op een Isabel Secure Signing Card worden opgeslagen, hetzij in een Isabel Tamper Resistant Device of bij een hardware veiligheidsmodule van derden die is goedgekeurd door Isabel.

De hardwarematige veiligheidsmodules van derden moeten beantwoorden aan de FIPS PUB 140-1 Level 3 of hoger.

6.2.2. PRIVATE SLEUTEL (N VAN M) MULTIPERSONENCONTROLE

Deze sectie geldt voor Isabel-CA private sleutels en mogelijke Houders 'Applicatie'.

De CA-Private Sleutels staan onder drievoudige controle.

De Private Sleutels van Houders 'Applicatie' staan onder enkel- of meervoudige controle, afhankelijk van de security policies van de Klant.

6.2.3. ESCROW PRIVATE SLEUTEL

De Private Sleutels van Isabel worden niet in escrow gegeven.

6.2.4. BACK-UP PRIVATE SLEUTEL

Van de Private Sleutel van de Houder van het Isabel-certificaat wordt geen back-up genomen, tenzij voor Houders die hun Private Sleutel bewaren in een Isabel Tamper Resistant (TRD). Van Private Sleutels die werden opgeslagen in een TRD wordt een back-up gemaakt op verschillende sets TRD-chipkaarten.

6.2.5. ARCHIVEREN PRIVATE SLEUTEL

De Private Sleutels van Isabel worden niet gearhiveerd.

6.2.6. INVOEREN PRIVATE SLEUTEL IN EEN VERSLEUTELINGSMODULE

De Private Sleutel wordt op een veilige manier ingevoerd in de versleutelingsmodule. De details worden beschouwd als bedrijfsgeheim.

6.2.7. METHODE OM EEN PRIVATE SLEUTEL TE ACTIVEREN

De Private Sleutel wordt beveiligd door middel van een PIN of een wachtwoord. De details over de Private Sleutel worden beschouwd als vertrouwelijke informatie van het bedrijf.

6.2.8. METHODE OM EEN PRIVATE SLEUTEL TE DESACTIVEREN

De Private Sleutel wordt gedeactiveerd als de Isabel Secure Signing Card uit de kaartlezer wordt genomen of als de Isabel TRD wordt uitgeschakeld.

Voor hardwarematige veiligheidsmodules van derden dient men de specificaties van de fabrikant te raadplegen.

6.2.9. METHODE OM EEN PRIVATE SLEUTEL TE Vernietigen

De Private Sleutel wordt vernietigd als de Isabel Secure Signing Card wordt vernietigd.

Voor een Private Sleutel die is opgeslagen in een Isabel TRD, wordt de Private Sleutel vernietigd als de Isabel TRD wordt uitgeschakeld EN als alle TRD chipkaarten die de Private Sleutel bevatten, worden vernietigd.

Voor hardwarematige veiligheidsmodules van derden dient men de specificaties van de fabrikant te raadplegen.

6.3. ANDERE ASPECTEN VAN HET BEHEER VAN SLEUTELPAREN

De Isabel-certificaten en bijgevolg de Publieke Sleutel die ze certificeren, worden gedurende ten minste 10 jaar gearchiveerd.

6.4. ACTIVERINGSGEGEVENS

De activeringsgegevens van de Houder worden hetzij centraal gegenereerd door de Isabel-CA, of lokaal door de Houder zelf. In beide gevallen garanderen de Isabel-certificatieprocedures (Zie hoofdstuk 4 - Operationele bepalingen) dat de activeringsgegevens van de Houder op een veilige manier aan de Houder wordt overgemaakt.

Daarna dient de Houder de vertrouwelijkheid van zijn/haar activeringsgegevens te waarborgen.

Isabel neemt geen back-up van de activeringsgegevens van de Houder, geeft ze niet in escrow en archiveert ze niet.

6.5. BEVEILIGINGSCONTROLES COMPUTER

De Isabel-CA heeft logische mechanismen voor toegangscontroles geïmplementeerd op het niveau van het besturingssysteem, de middleware en op applicatieniveau op de CA-systemen en heeft policies en procedures ingevoerd die ervoor zorgen dat de toegang tot de CA-systemen wordt beperkt tot bevoegde personen, zoals beschreven in [10], [11] en [13].

6.6. LEVENSCYCLUS TECHNISCHE MAATREGELEN

De levenscyclus van de technische maatregelen zijn geïmplementeerd overeenkomstig de Isabel security policies beschreven in [10] en [11].

6.7. NETWERKBEVEILIGINGSMATREGELEN

De netwerkbeveiligingsmaatregelen worden geïmplementeerd overeenkomstig de Isabel security policies beschreven in [10] en [11].

6.8. MAATREGELEN ENGINEERING VERSLEUTELINGSMODULE

Zie sectie 6.2.1 van onderhavig document.

7. CERTIFICATEN- EN CRL-PROFIELEN

7.1. CERTIFICATENPROFIEL

Gelieve deze informatie ook te raadplegen in de toepasselijke Isabel-CP.

Het profiel van een **Isabel-certificaat** dat wordt uitgereikt aan een Houder 'Natuurlijke Persoon' is of aan een Houder 'Functie' ziet er als volgt uit:

Veld van het certificaat	Waarde of waardenindeling
Version	INTEGER {V3(2)} (Opmerking: integer waarde 2 stemt overeen met v3 certificaten)
Serial number	INTEGER {0..MAX} Het nummer heeft als vorm yyyyddnnnnn waarbij <ul style="list-style-type: none"> • Yyyy het jaar is waarin het certificaat werd aangemaakt • ddd het nummer van de dag in dat jaar is • nnnnn een volgnummer voor die dag is
Signature algorithm	<i>AlgorithmIdentifier sha-1WithRSAEncryption</i> <i>OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}</i>
Issuer	<i>CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE</i>
Validity	<i>NotBefore=UTCTime</i> <i>NotAfter=UTCTime</i>
Subject (Normale gebruikers – natuurlijke personen)	<i>CN=Lastname Firstname; O=Organisation name; L=ISABEL; C=BE</i> <i>Mogelijk kan ook een OU- en/of een GN-veld aanwezig zijn.</i>
Subject (Normale gebruikers – Functies)	<i>CN=Function Name; O=Organisation name; L=ISABEL; C=BE</i> <i>Mogelijk kan ook een OU- en/of een GN-veld aanwezig zijn.</i>
subjectPublicKeyInfo	<i>AlgorithmIdentifier rsaEncryption</i> <i>OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1}</i>

Het profiel van een **Isabel-certificaat** dat wordt uitgereikt aan een Houder 'Applicatie' ziet er als volgt uit:

Veld van het certificaat	Waarde of waardenindeling
Version	INTEGER {V3(2)} (Opmerking: integer waarde 2 stemt overeen met v3 certificaten)
Serial number	INTEGER {0..MAX} Het nummer heeft als vorm yyyyddnnnnn waarbij <ul style="list-style-type: none"> • Yyyy het jaar is waarin het certificaat werd aangemaakt • ddd het nummer van de dag in dat jaar is • nnnnn een volgnummer voor die dag is

Veld van het certificaat	Waarde of waardenindeling
Signature algorithm	<i>AlgorithmIdentifier sha-1WithRSAEncryption</i> <i>OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}</i>
Issuer	<i>CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE</i>
Validity	<i>notBefore=UTCTime</i> <i>notAfter=UTCTime</i>
Subject (Normale gebruikers – Applicaties)	<i>CN=Application Name; O=Organisation name; L=ISABEL; C=BE</i> <i>Mogelijk kan ook een OU- en/of een GN-veld aanwezig zijn.</i>
subjectPublicKeyInfo	<i>AlgorithmIdentifier rsaEncryption</i> <i>OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1}</i>

7.1.1. VERSIENUMMER

Alle Isabel-certificaten die door Isabel-certificatieautoriteiten worden uitgereikt moeten stroken met ITU-T X.509 v3. zie ref [3] in sectie “9.2 – Bijlage B – Referenties” in onderhavige CPS.

7.1.2. CERTIFICAATEXTENSIES

De extensies die zijn gedefinieerd voor X.509v3-certificaten reiken werkwijzen aan om bijkomende attributen te koppelen aan gebruikers of Publieke Sleutels, alsook voor het beheer van de certificatenhiërarchie. Dit veld mag enkel in versie 3 verschijnen. Het veld is een opeenvolging van een of meerdere certificaatextensies.

Een applicatie MOET het certificaat verwerpen wanneer zij een kritieke extensie tegenkomt die zij niet herkent; een niet-kritieke extensie kan evenwel genegeerd worden bij niet-herkenning.

Hierna volgt een lijst van de standaard certificaatextensies (zoals gedefinieerd in ITU-T X.509) gebruikt in Isabel-certificaten die door een Isabel Certificatieautoriteit worden uitgereikt, evenals een beschrijving van de manier waarop zij worden gebruikt, met inbegrip van het kritische (C) of niet-kritische (NC) karakter.

Voor een vollediger beschrijving van deze certificaatextensies, zie CF ITU-T X.509v3.

Onderstaande tabel geeft een beknopt overzicht van de VERPLICHTE extensies en hun waarde voor een **Isabel-certificaat** dat wordt uitgereikt aan een natuurlijke persoon of aan een functie:

Extensieveld certificaat	AI dan niet kritiek	Waarde of waardenindeling
authorityKeyIdentifier	NC	Dit veld identificeert de te gebruiken publieke sleutel van de CA om de handtekening op de certificaten te controleren. <i>BYTE STRING ::= {4341 3032} (“CA02”)</i>
subjectPublicKeyInfo <i>OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium (56) Isabel(1) 8}</i>	NC/C	Dit veld is een eigen extensie van Isabel <i>Uitsluitend voor intern gebruik</i> Dit veld is kritiek voor herroepen certificaten.

Extensieveld certificaat	AI dan niet kritiek	Waarde of waardenindeling
SerialNumber (OID 2.5.4.5)	NC	Dit veld geeft de Isabel Secure Signing Card's Identifier (CardID) weer. Deze extensie heeft enkel een waarde als de Isabel Secure Signing Card verpersoonlijkt werd via de gecentraliseerde certificatieprocedure.
KeyUsage	NC	Dit veld geeft een lijst van het toegestane gebruik van de sleutel. BIT STRING ::= {digitalSignature(0), nonRepudiation(1), keyEncipherment(2), dataEncipherment(3)}
CertificatePolicies	NC	Dit veld bevat een reeks van een of meerdere policy-informatietermen, die elk bestaan uit een object identifier (OID) en optionele qualifiers. Deze policy-informatietermen duiden aan onder welke policy het certificaat werd uitgegeven en voor welke doeleinden het certificaat kan worden gebruikt. Heeft de waarde {joint-iso-ccitt(2) allocation per country (16) Belgium (56) isabel (1) certification-policies(9) standard(2)} Het veld bevat tevens aan attribuut dat een URI is voor de volledige versie van de CPS: http://www.isabel.be/PKI/Policies/Standard.htm
ExtKeyUsage	NC	Dit veld geeft verdere gebruiksmogelijkheden voor de sleutel. Het is een lijst van OID's. KeyPurposeID ::= {id-kp-clientAuth, id-kp-emailProtection}
AuthorityInfoAccess	NC	Dit veld verstrekt een pointer naar een on-line service voor de status van herroepen certificaten. De waarde is: https://ocsp1.isabel.be/

Onderstaande tabel geeft een beknopt overzicht van de VERPLICHTE extensies en hun waarde voor een **Isabel-certificaat** dat is uitgereikt aan een applicatie:

Extensieveld certificaat	AI dan niet kritiek	Waarde of waardenindeling
authorityKeyIdentifier	NC	Dit veld identificeert de te gebruiken publieke sleutel van de CA om de handtekening op de certificaten te controleren. BYTE STRING ::= {4341 3032} ("CA02")
subjectPublicKeyInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8}	NC/C	Dit veld is een eigen extensie van Isabel <i>Uitsluitend voor intern gebruik</i> Dit veld is kritiek voor herroepen certificaten.

7.1.3. ALGORITME OBJECT IDENTIFIERS

sha-1WithRSAEncryption
OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsdsi(113549) pkcs(1) pkcs-1(1) 5}

rsaEncryption

OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1}

7.1.4. NAAMVORMEN

Entiteit	Naamvorm
Houder van het Isabel-certificaat (natuurlijke persoon)	<i>CN=Lastname Firstname; O=Organisation name; L=ISABEL; C=BE</i> <i>Mogelijk kan ook een OU- en/of een GN-veld aanwezig zijn.</i>
Houder van het Isabel-certificaat (Functie)	<i>CN=Function Name; O=Organisation name; L=ISABEL; C=BE</i> <i>Mogelijk kan ook een OU- en/of een GN-veld aanwezig zijn.</i>
Houder van het Isabel-certificaat (Applicatie)	<i>CN=Application Name; O=Organisation name; L=ISABEL; C=BE</i> <i>Mogelijk kan ook een OU-veld aanwezig zijn.</i>
Isabel-CA	<i>CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE</i>

Elk e-mail adres, noch de namen dat het bevat, in het Certificaat kunnen beschouwd worden als een element van identificatie op basis waarvan het Certificaat is uitgegeven.

7.1.5. NAAMBEPERKINGEN

In een Isabel-certificaat wordt geen extensie naambeperking gebruikt.

7.1.6. OBJECT IDENTIFIER CERTIFICAATPOLICY

Zie sectie "1.2 – Identificatie" van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

7.1.7. GEBRUIK VAN DE EXTENSIE POLICY CONSTRAINTS

In een Isabel-certificaat wordt geen extensie policyconstraints gebruikt.

7.1.8. SYNTAX EN SEMANTIEK VOOR DE POLICY QUALIFIERS

Voor de certificaatpolicy die in de extensie certificaatpolities gedefinieerd is, wordt een policy qualifier gedefinieerd.

Deze qualifier is een URI voor de volledige versie van de CPS: <http://www.isabel.be/PKI/Policies/Standard.htm> voor de Policy van de Certificatie-Activiteiten van Isabel.

7.1.9. SEMANTIEK VOOR DE VERWERKING VAN DE KRITIEKE EXTENSIE CERTIFICAATPOLICY

De extensie certificaatpolities wordt als niet kritisch gemarkeerd, zie 7.1.2.

7.2. CRL/ARL-PROFIEL

Het profiel van een Lijst met de Herroepingen van de Certificaten (CRL) en een Lijst met Herroepingen van Certificaten van Autoriteiten (ARL), aangemaakt door een Isabel-certificatieautoriteit, ziet er als volgt uit:

Certificaatveld	Waarde of waardenindeling
Version	INTEGER {V2(1)} (Opmerking: integer waarde 1 stemt overeen met v2 CRL's)
Signature	AlgorithIdentifier sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
Issuer	CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE
ThisUpdate	UTCTime: Geeft het tijdstip weer waarop de CRL werd aangemaakt.
NextUpdate	UTCTime: Duidt aan wanneer de volgende CRL zal worden aangemaakt (uiterlijk).
RevokedCertificates	De lijst van herroepen certificaten. (Houdercertificaten voor CRL's en CA-certificaten voor ARL's).

7.2.1. VERSIENUMMER

Alle Isabel CRL's en ARL's moeten conform ITU-T X.509 v2 zijn.

7.2.2. CRL/ARL EN CRL/ARL EXTENSIES

Dit zijn de Isabel CRL/ARL-extensies:

CRL-extensieveld	AI dan niet kritiek	Waarde of waardenindeling
authorityKeyIdentifier	NC	Dit veld identificeert de te gebruiken publieke sleutel van de CA om de handtekening op de certificaten te controleren. BYTE STRING ::= {4341 3032} ("CA02")
CrlNumber	NC	INTEGER. Het nummer van de CRL/ARL.

CRL-entries kunnen ook extensies bevatten. Hierna volgt een lijst van degene die in de Isabel CRL/ARL-entries zijn gebruikt:

CRL-ingang extensieveld	AI dan niet kritiek	Waarde of waardenindeling
ReasonCode	NC	Deze extensie specificeert om welke reden de entry herroepen is. Mogelijke waarden zijn: CRLReason ::= ENUMERATED { unspecified (0), keyCompromise (1), caCompromise (2), affiliationChanged (3), superseded (4), cessationOfOperations (5)} Andere waarden zijn toegelaten maar niet gebruikt.

8. SPECIFICATIE ADMINISTRATIE

8.1. SPECIFICATIE WIJZIGINGSPROCEDURES

Opmerkingen, vragen en wijzigingsaanvragen met betrekking tot onderhavige Isabel-CPS moeten worden gericht aan de Policy-autoriteit gespecificeerd onder sectie “1.3.7 – Contactgegevens” van onderhavige Policy van de Certificatie-Activiteiten van Isabel.

Isabel mag te allen tijde wijzigingen aanbrengen in onderhavige Isabel-CPS.

8.2. PUBLICATIE EN MEDEDELING POLICIES

Onderhavige Isabel-CPS staat onder het rechtstreeks toezicht van de Policy-autoriteit en de General Manager van Isabel. Het senior management van Isabel ziet erop toe dat de activiteiten in het kader van onderhavige Isabel-CPS correct worden geïmplementeerd.

Teneinde rekening te houden met veranderende omstandigheden, wetgeving, technologie en veiligheidsrisico's herziert de Policy-autoriteit onderhavige Isabel-CPS regelmatig.

De Policy-autoriteit doet aanbevelingen voor veranderingen in onderhavige Isabel-CPS die onderworpen zullen worden aan een consultatieproces binnen Isabel en goedkeuring door de General Manager vooraleer enige veranderingen worden geïmplementeerd.

Onderhavige Isabel-CPS en de latere versies ervan worden gepubliceerd op de URI: <http://www.isabel.be/PKI/Policies/>. De publicatiedatum en ingangsdatum, evenals het versienummer worden vermeld op de titelpagina van de Isabel-CPS. De gepubliceerde versie die na deze URL volgt, is de enige geldige versie binnen de periode van die publicatie.

Ook mededelingen met betrekking tot onderhavige Isabel-CPS worden op bovenstaande URL gepubliceerd.

Het aanhoudend gebruik van een Isabel-certificaat na de publicatie van een nieuwe versie van de CPS impliceert dat de Houder deze nieuwe versie aanvaardt.

De meest recente versie van onderhavige CPS is on-line verkrijgbaar. Oudere versies worden door Isabel gearchiveerd.

8.3. GOEDKEURINGSPROCEDURES VOOR CPS

De Policy-autoriteit voor onderhavige Isabel-CPS en de General Manager van Isabel moeten wijzigingen aan het onderhavige document goedkeuren.

9. BIJLAGEN

9.1. BIJLAGE A – DEFINITIES

9.1.1. LETTERWOORDEN

Letterwoord	Betekenis
ARL	Lijst met Herroepingen van Certificaten van Autoriteiten (Authority Revocation List)
CA	Certificatieautoriteit
CBF	Commissie voor het Bank- en Financiewezen (Commission Bancaire et Financière)
CP	CertificaatPolicy
CPS	Policy van de Certificatie-Activiteiten (Certification Practice Statement)
CRL	Lijst met de Herroepingen van de Certificaten (Certificate Revocation List)
HSM	Hardwarematige veiligheidsmodule (Hardware Security Module)
OCSP	On Line Protocol voor de Status van het Certificaat (Online Certificate Status Protocol)
OID	Object Identifier
PIN	Persoonlijk IdentificatieNummer
PKI	Infrastructuur voor Publieke Sleutels (Public Key Infrastructure)
RA	RegistratieAutoriteit
SSCD	Secure Signature Creation Device (veilig middel voor het aanmaken van handtekeningen)
TRD	Tamper Resistant Device (HSM Isabel)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WISE	Worldwide Internet Services for Enterprises in corporate e-banking

9.1.2. WOORDENLIJST

Term	Omschrijving
Applicatie	In de onderhavige context is dit een Applicatie welke de Houder kan zijn in een Certificaat. Dergelijke Applicatie is een software applicatie die met behulp van een geautomatiseerd proces (ten allen tijde) getekende informatie publiceert, en aldus niet afhankelijk mag zijn van een menselijke tussenkomst voor het genereren van een elektronische handtekening. Voorbeelden van dergelijke Applicaties zijn websites die elektronisch getekende offertes maakt voor haar klanten, of elektronisch getekende berichten die verstuurd worden voor commerciële of marketing doeleinden.
Abonnee	Zie Isabel-Certificaatabonnee.
Authenticatie	Het proces waarbij de identiteit wordt vastgelegd, gebaseerd op het bezit van een geloofwaardig bewijsstuk.
Certificatieautoriteit	Een autoriteit waarin gebruikers hun vertrouwen stellen voor het aanmaken en beheren van certificaten; eventueel kan de CA ook het sleutelbaar van de gebruiker aanmaken.
Certificatieautoriteit Cross-Certificate	Dit is een Certificaat getekend door de Certificatieautoriteit dat een andere Publieke Sleutel van de Certificatieautoriteit bevat. In de Isabel Certificatieautoriteit worden meerdere sleutels gebruikt door de Certificatieautoriteit.
Certificaatpolicy	Een reeks regels die aangeven wanneer een certificaat van toepassing is op een bepaalde gemeenschap en/of categorie met gemeenschappelijke veiligheidsvereisten.
Digitaal certificaat	De publieke sleutel van een Houder, samen met de identiteit van de Houder en nog andere informatie, onvervalsbaar gemaakt dankzij de versleuteling met de private sleutel van de CA die het Certificaat heeft uitgegeven.
Hardwarematige veiligheidsmodule	Hardwarematige versleutelingsmodule, gebruikt voor het aanmaken en opslaan van Private Sleutels en het aanmaken van elektronische handtekeningen.
Houder	Zie Houder van het Isabel-certificaat.
Houder van het Isabel-certificaat	<p>Een natuurlijke persoon, een applicatie of een functie (bijv. "boekhouder"), in een certificaat geïdentificeerd als de Houder van de Private Sleutel die bij de in het certificaat verstrekte Publieke Sleutel hoort.</p> <p>Aan de Houder van het Isabel-certificaat werd een Isabel-certificaat verstrekt in het kader van zijn beroepsactiviteiten; hij ontsleutelt en/of ondertekent met de Private Sleutel die bij dat Isabel-certificaat hoort voor de Isabel-klant waarvan hij deel uitmaakt.</p> <p>Een of meerdere natuurlijke personen fungeren als Houder van het Isabel-certificaat:</p> <ul style="list-style-type: none"> - In het geval de Houder "Natuurlijke Persoon" is, wordt de Houder vertegenwoordigd door de natuurlijke persoon geïdentificeerd in het certificaat. - In het geval van een Houder "Functie" wordt de Houder vertegenwoordigd door één natuurlijke persoon die bevoegd is om de functie te vertegenwoordigen geïdentificeerd in het certificaat (functievertegenwoordiger). - Indien de Houder "Applicatie" is, wordt de Houder vertegenwoordigd door een of meerdere natuurlijke personen die bevoegd zijn om de applicatie te vertegenwoordigen geïdentificeerd in het certificaat.

Term	Omschrijving
Infrastructuur voor Publieke Sleutels	Een geheel van hardware, software, mensen, processen en policies die gebruik maakt van de technologie voor elektronische handtekeningen om de controleerbare associatie van de publieke component van een asymmetrische Publieke Sleutel aan een specifieke Houder die de bijhorende Private Sleutel bezit, te vereenvoudigen.
Isabel Agent	Een personeelslid van Isabel of van een bedrijf dat met Isabel verbonden is door een servicecontract.
Isabel-certificaat	Een Digitaal certificaat, uitgegeven door een Isabel-CA.
Isabel-Certificatieautoriteit	Een CA uitgebaat door Isabel. Isabel CA wordt eveneens gerefereerd als de technische organisatie rond de Certificatieautoriteit, die beheerd wordt door het bedrijf Isabel NV/SA.
Isabel-Certificaatabonnee	Een natuurlijke persoon die de volmacht heeft van een Isabel-klant om een Isabel-certificaat aan te vragen voor een of meerdere natuurlijke personen, applicaties of functies als Houder. Een natuurlijke persoon als Houder kan een Isabel-Certificaatabonnee zijn die voor eigen rekening optreedt.
Isabel-Gebruiker	Een natuurlijke persoon die producten/diensten van Isabel gebruikt binnen het kader van een contract dat de Isabel-klant waartoe de Gebruiker behoort, bindt aan Isabel.
Isabel-klant	Een entiteit die een contract ondertekend heeft met Isabel teneinde diensten en/of producten van Isabel te verkrijgen.
Isabel-Registratieautoriteit	Een RA die werkt onder de bevoegdheid en onder de controle van een Isabel-CA.
Isabel Secure Signing Card	Een Smart Card waarop de Private Sleutel van een Houder opgeslagen is, door deze Houder gebruikt voor het aanmaken van een elektronische handtekening. De elektronische handtekening wordt binnenin de Isabel Secure Signing Card aangemaakt.
Isabel Tamper Resistant Device	Een hardware beveiligingsmodule waarin de Private Sleutel is opgeslagen van een Houder van een Isabel-certificaat en die door deze Houder wordt gebruikt om een elektronische handtekening aan te maken. De elektronische handtekening wordt aangemaakt in de Isabel Tamper Resistant Device.
Isabel-Validatieautoriteit	Een autoriteit die aan iedere bij het Isabel-certificaat Vertrouwende Partij een manier verschafft om statusinformatie te verkrijgen over de herroeping van Isabel-certificaten.
Lijst met Herroepingen van Certificaten van Autoriteiten	Een lijst met nummers van herroepen certificaten; hierin worden enkel herroepen autoriteitcertificaten geïdentificeerd, en geen Houdercertificaten.
Lijst met Herroepingen van Certificaten	Een lijst met nummers van herroepen certificaten die elektronisch ondertekend is door de uitgevende CA.
Persoonlijk Identificatienummer	Een geheime code (PIN) die wordt gebruikt om ongeoorloofde toegang tot een Private Sleutel te beletten.
Policy-autoriteit	De entiteit die verantwoordelijk is voor de specificatie en validatie van de Isabel-CP's en die moet nagaan of de Policy van de Certificatie-Activiteiten (CPS) past bij deze Certificaatpolicies.
Policy van de Certificatie-Activiteiten	Een policy van de activiteiten die een Certificatieautoriteit (CA) aanwendt voor de uitgifte van certificaten (CPS).
Private Sleutel	Het gedeelte van een publiek/privaat sleutelpaar dat geheim moet gehouden worden en enkel mag gekend zijn door de Houder.

Term	Omschrijving
Publieke Sleutel	Het gedeelte van een publiek/privaat sleutelpaar dat publiek bekend mag worden gemaakt of verspreid mag worden zonder de veiligheid van het versleutelingsysteem in gevaar te brengen.
Registratieautoriteit	Een entiteit die verantwoordelijk is voor de identificatie en authenticatie van Houders van certificaten, maar die geen certificaten ondertekent of uitgeeft. Een RA kan deelnemen aan het proces voor de Aanvraag van een certificaat, de herroeping van een certificaat, of beide, zoals vermeld in de corresponderende CP en de onderhavige CPS.
Self-signed certificaat	Certificaat getekend met de Private Sleutel waarvan de Publieke Sleutel zich in het Certificaat bevindt. Typisch wordt dit gebruikt voor de CA root certificaten, waarbij de root sleutel zich in het Certificaat bevindt getekend met de corresponderende Private Sleutel.
Vertrouwende Partij	Zie Vertrouwende Partij bij het Isabel-certificaat
Vertrouwende Partij bij het Isabel-certificaat	Een Vertrouwende Partij bij het Isabel-certificaat is een natuurlijke persoon of een applicatie die een Isabel-klant is of daartoe behoort, en die vertrouwt op de informatie vervat in een Isabel-certificaat en/of op elektronische handtekeningen die zijn geverifieerd met behulp van dat certificaat en/of op alle overige informatie gepubliceerd door een Isabel-CA die Isabel-certificaten uitgeeft.
Verzoek om een Isabel-certificaat	Indiening van gevalideerde informatie voor de Aanvraag van een Isabel-certificaat door een Isabel-RA bij een Isabel-CA teneinde de uitgifte van een Isabel-certificaat te bekomen.
WISE communauteit	Gebruikers die geregistreerd en gecertificeerd werden door een Isabel-RA voor het gebruik van WISE.

9.2. BIJLAGE B – REFERENTIES

	Titel	Auteur	Datum
[1]	'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic Signatures'	Europees Parlement en Europese Raad	13 december 1999
[2]	'Wet houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatediensten'	Belgisch Parlement	9 juli 2001
[3]	ITU-T Recommendation X.509	ITU-T	juni 1997
[4]	RFC 2527: 'Internet X.509 Public Key Infrastructure – CP and Certification Practices Framework'	Internet Engineering Task Force (IETF)	maart 1999
[5]	Banking – Public Key Infrastructure Policy and Practices framework – ISO/TC68/SC2/WG8 N 001	International Standards Organisation	22 oktober 2002
[6]*	Isabel-CA Technical Manual	Isabel	
[7]*	Isabel-CA Initialisation	Isabel	
[8]*	Isabel Key Management	Isabel	januari 1996
[9]*	Isabel Key Management Banks viewpoint	Isabel	februari 1996
[10]*	Isabel Corporate Security Policy	Isabel	juli 2001
[11]*	Isabel Information Security Manual	Isabel	januari 2002
[12]*	Isabel Physical Security Manual	Isabel	januari 2002
[13]*	Isabel Personnel Security Manual	Isabel	november 2001
[14]	FIPS PUB 140-1	NIST	januari 1994
[15]	Isabel CPS-CP versions	Isabel	

* Dit is een vertrouwelijk document van Isabel