PKI@BNPPF Certificate Policy

versie 1.0

Datum van publicatie: 27 augustus 2012

Datum van inwerkingtreding: 29 augustus 2012

Inhoud

1. Inleiding

Het vertrouwen in een digitaal certificaat hangt af van de regels die worden gevolgd voor de afgifte en het beheer van dergelijke certificaten. Die regels worden officieel vastgesteld in beleidsdocumenten, met name de Certificate Policy (CP) en het Certification Practice Statement (CPS).

Volgens de norm ITU-T X.509 is een CP "een bepaalde reeks voorschriften die de geldigheid aangeven van een certificaat voor een bepaalde gemeenschap en/of categorie toepassingen met gemeenschappelijke veiligheidsvereisten".

De term CPS wordt in de richtsnoeren van de American Bar Association als volgt gedefinieerd: "Een document waarin wordt beschreven volgens welke procedures een Certification Authority (CA) certificaten uitgeeft."

Terwijl de CP vooral de *basisverplichtingen* van de CA en de andere bij de PKI betrokken partijen bepaalt, gaat het CPS dieper in op de *manier waarop* deze verplichtingen worden nagekomen door de Isabel CA en de andere bij de PKI betrokken partijen.

1.1. OVERZICHT

Deze "PKI@BNPPF Certificate Policy" bepaalt het toepassingsgebied van en de regels die van toepassing zijn op de "PKI@BNPPF Certificates". In het document worden de voorwaarden vastgesteld voor de uitgifte, het beheer en het gebruik van certificaten op basis van een openbare sleutel, die worden aangeduid als "PKI@BNPPF Certificates", en de encryptietechnologie die gebruikt wordt voor de authenticatie en de bewaking van het vertrouwelijke karakter, de integriteit en de onweerlegbaarheid van gegevens.

Een PKI@BNPPF Certificate is een certificaat dat een Isabel CA voor specifieke doeleinden van BNP Paribas Fortis uitgeeft.

De onderhavige CP bevat:

- een opsomming van de entiteiten die deel uitmaken of gebruikmaken van de diensten van de Isabel Public Key Infrastructure in het kader van de aanvraag, de uitgifte, de aanvaarding, het gebruik en de intrekking van PKI@BNPPF Certificates;
- een beschrijving van de toepasselijkheid van PKI@BNPPF Certificates op derde partijen;
- een beschrijving van de verplichtingen en de aansprakelijkheden van de entiteiten die betrokken zijn bij de aanvraag, de uitgifte, de aanvaarding, het gebruik en de intrekking van PKI@BNPPF Certificates;
- een beschrijving van het PKI@BNPPF Certificate-profiel;
- een verklarende woordenlijst en een lijst met referentiedocumenten.

Zoals wordt aangegeven in de punten 1.3.6 en 2.1.4, moeten PKI@BNPPF Certificate Subjects en Relying Parties zich ervan vergewissen, door dit document en alle andere door hen noodzakelijk geachte informatie te lezen, dat uitgegeven PKI@BNPPF Certificates of ander diensten die een Isabel CA in het kader van dit beleid verleent geschikt zijn voor het beoogde gebruik.

Door te vertrouwen op informatie in een door een Isabel CA uitgegeven PKI@BNPPF Certificate, stemt de Relying Party in met de voorwaarden en de bepalingen van dit beleid.

1.2. IDENTIFICATIE

1.2.1. NAAM

Deze CP is getiteld "PKI@BNPPF Certificate Policy".

1.2.2. OBJECT IDENTIFIER

De Object Identifier van de "PKI@BNPPF Certificate Policy" is 2.16.56.1.9.48.1.1.

1.2.3. UNIFORM RESOURCE IDENTIFIER

De PKI@BNPPF Certificate Policy zal publiek toegankelijk zijn op de website Easy Banking Business van BNP Paribas Fortis.

1.2.4. HISTORIEK VAN DE VERSIES VAN HET DOCUMENT

Dit document is herzien op de volgende data:

Datum	Wijzigingen	Versie
27 augustus 2012	Initale versie	1.0

1.3. GEMEENSCHAP EN TOEPASSINGSGEBIED

1.3.1. CERTIFICATION AUTHORITIES

Volgens de norm ITU-T X.509 is een CA "een autoriteit die een of meer gebruikers vertrouwen voor het aanmaken en toewijzen van certificaten, waarbij de CA eventueel de sleutel van de gebruikers aanmaakt".

In de Public Key Infrastructure kunnen Isabel Certification Authorities aanvragen voor PKI@BNPPF Certificates aanvaarden van Certificate Subjects van wie de identiteit is geauthenticeerd door een PKI@BNPPF Registration Authority (RA).

Nadat de Isabel CA het door de PKI@BNPPF RA ingediende certificeringsverzoek heeft gecontroleerd, wordt een PKI@BNPPF Certificate uitgegeven dat de identiteit van het Certificate Subject koppelt aan zijn/haar Public Key.

1.3.2. REGISTRATION AUTHORITIES

Volgens RFC 3647 [4] is een RA "een entiteit die belast is met een of meer van de volgende taken: identificatie en authenticatie van aanvragers van certificaten, goedkeuring of afwijzing van certificaataanvragen, intrekking of opschorting van certificaten in bepaalde omstandigheden, verwerking van verzoeken van Subscribers om hun certificaten in te trekken of op te schorten en goedkeuring of weigering van verzoeken van Subscribers om hun certificaten te vernieuwen of een nieuw sleutelpaar toe te wijzen.

In de Isabel Public Key Infrastructure aanvaarden PKI@BNPPF RA die onder het toezicht en het gezag van een Isabel CA werken PKI@BNPPF Certificate-aanvragen voor PKI@BNPPF Certificates van PKI@BNPPF Certificate Subscribers.

PKI@BNPPF RAs moeten de identiteit van het PKI@BNPPF Certificate Subject authenticeren en de in de PKI@BNPPF Certificate-aanvraag opgenomen informatie controleren. Indien de gecontroleerde informatie correct blijkt, stuurt de PKI@BNPPF RA een PKI@BNPPF Certificate -verzoek naar de bevoegde Isabel CA met het oog op de toewijzing van een PKI@BNPPF Certificate aan het PKI@BNPPF Certificate Subject.

Enkel door BNP Paribas Fortis gemachtigde Registration Authorities mogen een Isabel CA verzoeken om PKI@BNPPF Certificates uit te geven. BNP Paribas Fortis publiceert een lijst van gemachtigde Registration Authorities op haar website voor Easy Banking Business.

1.3.3. EINDENTITEITEN

Ten behoeve van deze PKI@BNPPF Certificate Policy omvatten de eindentiteiten in de Public Key Infrastructure:

1. PKI@BNPPF Certificate Certificate Subscribers;
2. PKI@BNPPF Certificate Subjects;
3. PKI@BNPPF Certificate Relying Parties.

Een BNP Paribas Fortis Customer machtigt PKI@BNPPF Certificate Subscribers en PKI@BNPPF Certificate Subjects.

Het Subject-attribuut in het PKI@BNPPF Certificate wordt gebruikt om het PKI@BNPPF Certificate Subject een naam te geven of anderszins te identificeren:

1. naam en voornaam indien het Subject een natuurlijke persoon (Physical Person Subject) betreft;
2. naam van een functie indien het een Subject van een functie (Function Subject) betreft.

In het kader van deze PKI@BNPPF CP:

1. mag een PKI@BNPPF Certificate Subject geen CA of RA van de Isabel Public Key Infrastructure zijn;
2. is de handtekening van een Function Subject een technische handtekening, d.w.z. dat ze uitsluitend mag worden gebruikt om integriteitsredenen en niet om transacties goed te keuren, tenzij anders is bepaald in het tussen de BNP Paribas Fortis Customer en BNP Paribas Fortis gesloten contract.

1.3.4. VALIDATION AUTHORITIES

In de Isabel Public Key Infrastructure geeft een Isabel Validation Authority de Relying Parties toegang tot informatie over de geldigheid van PKI@BNPPF Certificates.

"On-Line Certificate Status Protocol (OCSP)"-responders leveren die informatie over de geldigheid van PKI@BNPPF Certificates.

Later zal de geldigheid van individuele certificaten op de website kunnen worden gecontroleerd.

1.3.5. POLICY AUTHORITIES

Een Policy Authority is de entiteit die verantwoordelijk is voor:

1. het opstellen, valideren en publiceren van de PKI@BNPPF CP en de wijzigingen daarvan;
2. het bepalen van de geschiktheid en de correcte tenuitvoerlegging van de PKI@BNPPF CP;
3. het bepalen van de evaluatievereisten en -processen in verband met de tenuitvoerlegging van de CP.

De Policy Authority voor deze PKI@BNPPF CP is: BNP Paribas Fortis. Zie 1.3.7 Contactgegevens.

1.3.6. TOEPASSINGSGEBIED

PKI@BNPPF Certificate die overeenkomstig deze CP zijn uitgegeven, mogen slechts worden gebruikt door Relying Parties die deel uitmaken van een BNP Paribas Fortis Customer EN voor de volgende doeleinden: controle van digitale handtekeningen, onweerlegbaarheid, encryptiesleutels en encryptiegegevens.

Er moet een contractuele relatie zijn tussen de Relying Parties en BNP Paribas Fortis.

Indien een PKI@BNPPF Certificate Subject (financiële of andere) beperkingen wil opleggen voor transacties die worden geauthenticeerd door het PKI@BNPPF Certificate, moet dat Subject met elke Relying Party een overeenkomst hebben ondertekend waarin dergelijke beperkingen zijn overeengekomen.

1.3.7. CONTACTGEGEVENS

1.3.7.1. ORGANISATIE SPECIFICATIEBEHEER

De Security Manager van BNP Paribas Fortis treedt op als Policy Authority voor deze PKI@BNPPF CP. Hij is verantwoordelijk voor alle aspecten van deze PKI@BNPPF CP, met inbegrip van de opstelling, validatie, registratie, publicatie, actualisering en interpretatie ervan.

1.3.7.2. CONTACTPERSOON BIJ DE POLICY AUTHORITY

Alle vragen en opmerkingen over deze PKI@BNPPF CP dienen te worden gericht aan de vertegenwoordiger van de Policy Authority ervan:

Business Information & Security Officer

FORTIS BANK NV

Warandeberg 3

1000 Brussel

België

mailto: rpb.information.security.incident.management@bnpparibasfortis.com

2. Algemene bepalingen

2.1. VERPLICHTINGEN

In dit punt worden de verplichtingen beschreven van de entiteiten die binnen de PKI betrokken zijn bij de aanvraag, de uitgifte, de aanvaarding, het gebruik, de publicatie en de intrekking van PKI@BNPPF Certificates.

PKI@BNPPF CertificateRelying Parties moeten de bepalingen in dit punt begrijpen alvorens op een PKI@BNPPF Certificate te vertrouwen.

Het betreft de volgende entiteiten:

1. Isabel CA;
2. PKI@BNPPF RA;
3. PKI@BNPPF Certificate Subscribers en Subjects;
4. PKI@BNPPF Certificate Relying Parties;
5. BNP Paribas Fortis Repository;
6. Policy Authority;

BNP Paribas Fortis als rechtspersoon. BNP Paribas Fortis

Om bij een Isabel CA PKI@BNPPF Certificates te kunnen aanvragen voor PKI@BNPPF Certificate Subscribers, moet de PKI@BNPPF RA de hieronder beschreven verplichtingen aanvaarden.

Om een PKI@BNPPF Certificate te kunnen uitgeven, moet de Isabel CA de hieronder beschreven verplichtingen aanvaarden.

Door een uitgegeven PKI@BNPPF Certificate te aanvaarden, aanvaardt het PKI@BNPPF Certificate Subject de hieronder vermelde verplichtingen en bepalingen.

Door gebruik te maken van een PKI@BNPPF Certificate, aanvaarden PKI@BNPPF Certificate Relying Parties hun verplichtingen en de hieronder vermelde bepalingen.

2.1.1. VERPLICHTINGEN VAN DE ISABEL CERTIFICATION AUTHORITIES

Een Isabel CA die PKI@BNPPF Certificates in de Public Key Infrastructure uitgeeft, heeft de in de onderstaande punten beschreven verplichtingen.

2.1.1.1. KENNISGEVING VAN DE UITGIFTE VAN CERTIFICATEN

Isabel CA's zorgen ervoor dat het PKI@BNPPF Certificate Subject in kennis wordt gesteld van de uitgifte van zijn/haar PKI@BNPPF Certificate.

2.1.1.2. PUBLICATIE VAN DE PKI@BNPPF CERTIFICATES IN EEN ISABEL REPOSITORY

Isabel CA's publiceren de door hen uitgegeven PKI@BNPPF Certificates nadat de certificaten door de betrokken PKI@BNPPF Certificate Subjects zijn aanvaard.

2.1.1.3. NAUWKEURIGHEID VAN DE INFORMATIE

Door een PKI@BNPPF Certificate uit te geven in het kader van deze CP, garandeert de Isabel CA aan alle partijen die binnen de grenzen van het redelijke op de informatie in het PKI@BNPPF Certificate vertrouwen, dat zij het PKI@BNPPF Certificate aan het genoemde PKI@BNPPF Certificate Subject heeft toegewezen overeenkomstig de bepalingen van deze PKI@BNPPF CP.

2.1.1.4. VERWERKING VAN VERZOEKEN TOT INTREKKING VAN CERTIFICATEN

Isabel CA's verwerken verzoeken tot intrekking van PKI@BNPPF Certificates die zijn uitgegeven door de PKI@BNPPF RA's die onder hun toezicht vallen. De publicatie van de intrekking wordt geregeld in punt "2.6.2 – Publicatieregelmaat".

2.1.1.5. PUBLICATIE VAN INFORMATIE OVER DE INTREKKING VAN PKI@BNPPF CERTIFICATES IN EEN ISABEL REPOSITORY

Isabel CA's publiceren informatie over de intrekking van door haar ingetrokken PKI@BNPPF Certificates in een Isabel Repository in de vorm van een geactualiseerde Certificate Revocation List (CRL).

De Isabel CA's leven de bepalingen van punt "2.6 – Publicatie en repository" van deze PKI@BNPPF CP na en respecteren de in punt "2.6.2 – Publicatieregelmaat" vastgestelde regelmaat.

Zo kunnen PKI@BNPPF Certificate Relying Parties tijdig en ondubbelzinnig de geldigheidsstatus van door de Isabel CA's uitgegeven PKI@BNPPF Certificates controleren.

2.1.1.6. KENNISGEVING VAN DE INTREKKING VAN EEN CERTIFICAAT

De Isabel Certification Authorities zorgen ervoor dat de entiteit (het PKI@BNPPF Certificate Subject of een PKI@BNPPF Certificate Subscriber) die een verzoek tot intrekking van een PKI@BNPPF Certificate indient bij een PKI@BNPPF Registration Authority, alsook alle andere partijen die redelijkerwijze hun vertrouwen in dat PKI@BNPPF Certificate stellen, in kennis gesteld worden van de intrekking van het PKI@BNPPF Certificate.

De Isabel Certification Authorities zorgen ervoor dat de informatie over de intrekking beschikbaar is voor alle partijen.

2.1.1.7. NORMNALEVING

Uitgegeven PKI@BNPPF Certificates moeten in overeenstemming zijn met versie 3 van de norm X.509.

2.1.1.8. ARCHIVERING EN BEVEILIGING

Isabel Certification Authorities komen hun archiveringsverplichtingen op de veiligst mogelijke manier na, teneinde de beschikbaarheid van documenten en/of andere informatie als bewijsmateriaal te garanderen en het vertrouwelijke karakter en de integriteit van dergelijke documenten en andere informatie te vrijwaren. In het algemeen zien zij toe op de fysieke veiligheid van de informatie, beveiligt zij de toegang ertoe en leidt zij haar personeel op.

2.1.1.9. BESCHERMING VAN PERSOONSGEGEVENS

De Isabel CA's zien erop toe dat vertrouwelijke en persoonsgegevens worden verwerkt overeenkomstig de Belgische wet op de bescherming van de persoonlijke levenssfeer.

2.1.2. VERPLICHTINGEN VAN DE ISABEL RA'S

Elke PKI@BNPPF RA die is goedgekeurd en binnen de Isabel Public Key Infrastructure werkt, heeft de in de onderstaande punten beschreven specifieke verplichtingen.

2.1.2.1. BESCHERMING VAN DE PRIVATE KEY VAN DE RA

PKI@BNPPF RA's moeten ervoor zorgen dat alleen zij in het bezit zijn van hun Private Key en de vertrouwelijkheid en de veiligheid van die Private Key en de vertrouwelijkheid van de daarbij horende activeringsgegevens beschermen en garanderen.

2.1.2.2. BEPERKING OP HET GEBRUIK VAN DE PRIVATE KEY VAN DE RA

PKI@BNPPF RA's mogen hun Private Key slechts gebruiken voor doeleinden die verband houden met hun RA-functie.

2.1.2.3. SCHADELOOSSTELLING VAN PARTIJEN

PKI@BNPPF RA's vergoeden partijen voor schade die zij veroorzaken door hun verplichtingen niet nakomen, binnen de in punt "2.2 – Aansprakelijkheid" van deze PKI@BNPPF Certificate Policy vastgestelde grenzen.

2.1.2.4. ARCHIVERING EN BEVEILIGING

PKI@BNPPF RA's komen hun archiveringsverplichtingen op de veiligste manier na, teneinde de beschikbaarheid van documenten en/of andere informatie als bewijsmateriaal te garanderen en teneinde de vertrouwelijkheid en integriteit van dergelijke documenten en andere informatie te vrijwaren. In het algemeen zien zij toe op de fysieke veiligheid van de informatie, beveiligt zij de toegang ertoe en leidt zij haar personeel op.

2.1.2.5. GOEDKEURING

Elke PKI@BNPPF RA is goedgekeurd door BNP Paribas Fortis. BNP Paribas Fortis heeft een lijst van erkende PKI@BNPPF RA's. Door op te treden als PKI@BNPPF RA voor een Isabel CA, verklaart de PKI@BNPPF RA dat zij deze verantwoordelijkheid aanvaardt en ermee instemt haar activiteiten in overeenstemming met deze CP te verrichten.

2.1.3. PKI@BNPPF CERTIFICATE VERPLICHTINGEN VAN SUBSCRIBERS EN SUBJECTS

PKI@BNPPF Certificate Subscribers en Subjects moeten in de regel de bepalingen, voorwaarden en procedures van deze CP naleven. Zij worden geacht die te hebben aanvaard wanneer zij een PKI@BNPPF Certificate gebruiken.

PKI@BNPPF Certificate Subscribers en Subjects verbinden zich ertoe die verplichtingen na te komen zolang het PKI@BNPPF Certificate geldig is.

Elke Subscriber dient een overeenkomst te onderteken met een PKI@BNPPF RA, op het moment van of vóór de uitgifte van het certificaat. De PKI@BNPPF RA bewaart een kopie van deze overeenkomst. PPKI@BNPPF Certificate Subscribers zijn gebonden door de rechten en plichten ten aanzien van de BNP Paribas Fortis die voortvloeien uit hun contractuele verbintenis met de PKI@BNPPF RA.

PKI@BNPPF Certificate Subscribers en PKI@BNPPF Certificate Subjects hebben de in de onderstaande punten beschreven verplichtingen.

2.1.3.1. VERZAMELING VAN DE NODIGE INFORMATIE VOOR EEN CORRECT EN VEILIG GEBRUIK VAN DE PKI-DIENSTEN

PKI@BNPPF Certificate Subjects dienen de volgende informatie te ontvangen van de PKI@BNPPF RA die hun PKI@BNPPF Certificate heeft uitgegeven:

1. een kennisgeving over hun verplichtingen;
2. een kennisgeving over de voorschriften met betrekking tot de bescherming van hun persoonlijke levenssfeer;
3. een kennisgeving over de exacte garanties die de PKI-diensten bieden.

De publicatie van deze PKI@BNPPF CP voor de PKI@BNPPF Certificate Subjects en PKI@BNPPF Certificate Relying Parties dient als een kennisgeving ervan te worden gezien. Door het PKI@BNPPF Certificate te gebruiken, aanvaardt het Subject de inhoud van de genoemde kennisgevingen.

2.1.3.2. WAARBORGING VAN DE GEHEIMHOUDING VAN DE PRIVATE KEY

PKI@BNPPF Certificate Subjects moeten ervoor zorgen dat alleen zij hun Private Key in hun bezit hebben en het vertrouwelijke karakter en de veiligheid van die Private Key en de vertrouwelijkheid van de activeringsgegevens beschermen en garanderen.

In het algemeen dienen Subjects alle voorzorgsmaatregelen te treffen om te voorkomen dat hun sleutels en de PKI@BNPPF Secure Signing Card met de daarbij horende activeringsgegevens verloren gaan, aan andere partijen worden meegedeeld dan wel gewijzigd worden of ongeoorloofd worden gebruikt.

Telkens de Private Key van een Subject gebruikt wordt, wordt aangenomen dat het het betrokken Subject is die die gebruikt, tot het tegendeel afdoende is bewezen.

2.1.3.3. BEPERKING OP HET GEBRUIK VAN DE PRIVATE KEY EN HET PKI@BNPPF CERTIFICATE

PKI@BNPPF Certificate Subjects mogen hun Private Key en PKI@BNPPF Certificate slechts gebruiken voor de toegelaten gebruiksdoelen, overeenkomstig de bepalingen in:

1. punt "1.3.6 – Toepassingsgebied" van deze PKI@BNPPF CP;
2. tussen BNP Paribas Fortis en de BNP Paribas Fortis Customer gesloten overeenkomsten.

Wanneer een Subject vermoedt dat zijn Private Key gecompromitteerd is, moet hij verzoeken om zijn PKI@BNPPF Certificate in te trekken en mag hij met de desbetreffende Private Key geen digitale handtekeningen meer genereren.

Wanneer alle aan een bepaalde Public Key gekoppelde certificaten ingetrokken of vervallen zijn, wordt de Public Key ongeldig en mag het Subject de overeenkomstige Private Key niet langer gebruiken, ook niet om een digitale handtekening te genereren of te decoderen.

2.1.3.4. MELDING AAN DE PKI@BNPPF REVOCATION SERVICE VAN DE COMPROMITTERING VAN EEN PRIVATE KEY / PIN OF HET VERLIES VAN DE PKI@BNPPF SECURE SIGNING CARD

Een PKI@BNPPF Certificate Subject of PKI@BNPPF Certificate Subscriber moet de PKI@BNPPF Registration Authority meteen op de hoogte brengen van:

1. een vermoede of vastgestelde compromittering of onthulling dan wel een vermoed of vastgesteld verlies van de Private Key van het Subject;
2. een vermoed of vastgesteld verlies van de PKI@BNPPF Secure Signing Card van het Subject;
3. een vermoede of vastgestelde compromittering of onthulling dan wel een vermoed of vastgesteld verlies van de pincode van het Subject.

Indien de PKI@BNPPF Registration Authority niet kan worden bereikt, mag overeenkomstig punt "3.4 – Intrekkingsverzoek" contact worden opgenomen met Card Stop.

2.1.3.5. MELDING VAN STATUSWIJZIGINGEN AAN DE PKI@BNPPF RA

PKI@BNPPF Certificate Subjects en PKI@BNPPF Certificate Subscribers moeten hun PKI@BNPPF RA onmiddellijk in kennis stellen van wijzigingen in de informatie die zij bij de aanvraag voor het PKI@BNPPF Certificate van het desbetreffende Subject hebben verstrekt.

2.1.3.6. GEBRUIK VAN EEN VEILIG APPARAAT VOOR HET GENEREREN VAN HANDTEKENINGEN

PKI@BNPPF Certificate Subjects moeten een Secure Signature Creation Device gebruiken om hun Private Key op te slaan en te gebruiken: de zogenoemde PKI@BNPPF Secure Signing Card.

2.1.3.7. BEPERKING OP HET GEBRUIK VAN DE PUBLIC KEY

PKI@BNPPF Certificate Subjects en Subscribers mogen geen certificeringsverzoek bij een derde CA indienen dat de Public Key in een PKI@BNPPF Certificate bevat, ook niet als het PKI@BNPPF Certificate vervallen of ingetrokken is.

PKI@BNPPF Certificate Subjects en Subscribers mogen bij een Isabel CA geen certificeringsverzoek indienen dat de Public Key bevat in een certificaat dat is uitgegeven door een andere CA dan de Isabel CA's, ook niet indien het certificaat van die derde partij vervallen of ingetrokken is.

2.1.4. VERPLICHTINGEN VAN DE RELYING PARTIES

Een Relying Party heeft de in de onderstaande punten vermelde specifieke verplichtingen.

2.1.4.1. VERZAMELING VAN DE NODIGE INFORMATIE VOOR EEN CORRECT EN VEILIG GEBRUIK VAN DE PKI-DIENSTEN

Relying Parties moeten van de Isabel CA die het PKI@BNPPF Certificate heeft uitgegeven waarin zij hun vertrouwen willen stellen, een kennisgeving ontvangen van de exacte garanties, aansprakelijkheden en verplichtingen die de PKI-diensten inhouden overeenkomstig punt "2.2 – Aansprakelijkheid" van deze PKI@BNPPF CP.

De Relying Parties moeten de inhoud van de kennisgevingen lezen en aanvaarden. In het algemeen dienen de Relying Parties deze CP, met inbegrip van alle toepasselijke aansprakelijkheidsbeperkingen en garanties, te aanvaarden alvorens een door een Isabel CA uitgegeven PKI@BNPPF Certificate te gebruiken. Bovendien moeten Relying Parties zich bewust zijn van alle regels, reglementen en statuten die van toepassing zijn op alle in een PKI@BNPPF Certificate opgenomen informatie en die naleven.

2.1.4.2. HET SELF-SIGNED CERTIFICATE VAN DE ISABEL CA BEKOMEN EN CONTROLEREN

Relying Parties moeten het Self-Signed Certificate van de Isabel CA aan de basis van de certificatenketen bekomen. Zij hebben dat namelijk nodig om de geldigheid van PKI@BNPPF Certificates te kunnen controleren.

Relying Parties moeten verplicht de inhoud en de geldigheid van het Self-Signed Certificate van de Isabel CA controleren en aanvaarden alvorens hun vertrouwen te stellen in dat certificaat.

Relying Parties moeten de volgende attributen van het Self-Signed Certificate van de Isabel CA controleren:

1. de emittent (Isabel CA);
2. de geldigheidsduur;
3. de gebruiksvoorschriften en de beperkingen van de sleutel en het certificaat;
4. de handtekening van de CA.

Relying Parties moeten het Self-Signed Certificate van de Isabel CA aanvaarden, overeenkomstig punt "4.3 – Aanvaarding van certificaten".

2.1.4.3. BEPERKING OP HET GEBRUIK VAN PKI@BNPPF CERTIFICATES

Relying Parties kunnen op PKI@BNPPF Certificates vertrouwen voor de toegelaten gebruiksdoelen en binnen de vastgestelde grenzen met betrekking tot functioneel gebruik en waarde, overeenkomstig punt "1.3.6 – Toepassingsgebied" van deze CP.

Relying Parties moeten verplicht de inhoud en de geldigheid van een PKI@BNPPF Certificate controleren en aanvaarden alvorens erop te vertrouwen.

Relying Parties moeten de volgende attributen van een PKI@BNPPF Certificate controleren:

1. de emittent (Isabel CA);
2. de geldigheidsduur;
3. de intrekkingsstatus (geldigheid);

4. het toegelaten gebruik en de beperkingen van de sleutel en het certificaat, zoals gespecificeerd in het PKI@BNPPF Certificate overeenkomstig punt "7.1.2 – Certificaatextensies",
5. de handtekening van de CA.

De attributen van een PKI@BNPPF Certificate zijn te vinden in punt "7.1 – Certificaatprofielen" van deze PKI@BNPPF CP.

Relying Parties mogen geen vertrouwen stellen in een PKI@BNPPF Certificate wanneer:
1. de digitale handtekening op het PKI@BNPPF Certificate of het PKI@BNPPF Certificate zelf niet kan worden gecontroleerd; of
2. het PKI@BNPPF Certificate is vervallen; of
3. het PKI@BNPPF Certificate werd ingetrokken; of
4. het PKI@BNPPF Certificate wordt gebruikt voor niet-toegelaten doeleinden of de gebruiksbeperkingen niet werden gerespecteerd.

2.1.4.4. HANDTEKENINGCONTROLE

Relying Parties moeten verplicht digitale handtekeningen controleren met het PKI@BNPPF Certificate van de Public Keys die bij de Private Keys horen die werden gebruikt om de digitale handtekeningen te genereren.

2.1.4.5. NIET-NAKOMING VAN DE VERPLICHTINGEN DOOR RELYING PARTIES

Relying Parties dienen zich ter dege bewust te zijn van de bepalingen in de punten "2.3.1 – Schadeloosstelling door BNP Paribas Fortis Customers, Relying Parties en Subjects" en "2.2 – Aansprakelijkheid" van deze PKI@BNPPF CP.

2.1.5. VERPLICHTINGEN INZAKE REPOSITORY

Isabel stelt een elektronisch repository ter beschikking voor PKI@BNPPF Certificates en informatie met betrekking tot de intrekking van PKI@BNPPF Certificates en ziet toe op de instandhouding daarvan.

Isabel doet haar uiterste best om dit elektronische repository tegen ongeoorloofde wijzigingen te beschermen.

Dit elektronische repository bevat op zijn minst:
1. de PKI@BNPPF Certificates die de Isabel Certification Authority overeenkomstig deze PKI@BNPPF CP heeft uitgegeven;
2. de lijst van ingetrokken certificaten die overeenkomstig deze PKI@BNPPF CP wordt gepubliceerd;
3. het Self-Signed Certificate van de Isabel Certification Authority;
4. de meest recente versie van deze PKI@BNPPF Certificate Policy.

Het elektronische repository kan via elektronische weg 24 uur op 24 rechtstreeks worden geraadpleegd.

Het elektronische repository kan niet worden geraadpleegd door personen die geen BNP Paribas Fortis Customer zijn, noch door hun vertegenwoordigers.

2.2. AANSPRAKELIJKHEID

2.2.1. AANSPRAKELIJKHEID VAN DE CA

2.2.1.1. GARANTIES EN BEPERKINGEN OP DE GARANTIES

Isabel garandeert enkel dat alle uitgegeven PKI@BNPPF Certificates worden uitgegeven overeenkomstig de bepalingen van deze PKI@BNPPF CP voor het geboden garantieniveau. Aanvullend kan de wet in andere garanties voorzien.

Tenzij anders is overeengekomen, en binnen de grenzen van de toepasselijke wetgeving, weigert Isabel elke vorm van garanties en verplichtingen te verlenen, inclusief garanties inzake verhandelbaarheid, geschiktheid voor een bepaald gebruiksdoel en nauwkeurigheid van de verstrekte informatie, en wijst zij elke aansprakelijkheid af voor enige nalatigheid of onzorgvuldigheid vanwege BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties. De garanties gelden voor de BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties.

2.2.1.2. UITSLUITING VAN DE AANSPRAKELIJKHEID VAN ISABEL TEN AANZIEN VAN BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS EN RELYING PARTIES

De beperking van de aansprakelijkheid van Isabel houdt de uitsluiting in van elke aansprakelijkheid voor indirecte, bijzondere, incidentele of gevolgschade.

Isabel is, tenzij hieronder anders is bepaald, niet aansprakelijk voor enig verlies of enige schade geleden door, voor vorderingen ingesteld tegen of voor kosten gemaakt door BNP Paribas Fortis Subscribers, Subjects, Customers en/of Relying Parties voor zover dergelijk verlies of dergelijke schade, vorderingen of kosten voortvloeien uit:

1. het verlies of de compromittering van de Private Key van Isabel, tenzij Isabel de in deze PKI@BNPPF CP vastgestelde voorschriften niet heeft nageleefd, in welk geval BNP Paribas Fortis aansprakelijk is (behoudens andere beperkingen of uitsluitingen die hieronder worden bepaald) ten aanzien van een Relying Party, voor zover de betrokken Relying Party kan aantonen dat zij een verlies of schade heeft geleden als gevolg van de niet-naleving van de voorschriften door Isabel;
2. onnauwkeurige of foute informatie in een door Isabel uitgegeven PKI@BNPPF Certificate, tenzij Isabel niet alle redelijke inspanningen heeft geleverd om de nauwkeurigheid en de juistheid van dergelijke informatie te garanderen of Isabel de authenticiteit van alle documentaire bewijsstukken van dergelijke informatie overeenkomstig deze PKI@BNPPF CP niet heeft gecontroleerd, in welk geval Isabel aansprakelijk is (behoudens andere beperkingen of uitsluitingen die hieronder worden bepaald) ten aanzien van een Relying Party, voor zover de betrokken Relying Party kan aantonen dat zij als gevolg daarvan een verlies of schade heeft geleden;
3. het feit dat een Relying Party haar vertrouwen heeft gesteld in een ingetrokken PKI@BNPPF Certificate die door Isabel was uitgegeven, wanneer die Relying Party het heeft nagelaten bij de Validation Authority na te gaan of het betrokken PKI@BNPPF Certificate niet was ingetrokken;
4. het feit dat een Relying Party haar vertrouwen heeft gesteld in een door Isabel uitgegeven PKI@BNPPF Certificate, wanneer die Relying Party wist of redelijkerwijs had moeten weten dat het betrokken PKI@BNPPF Certificate was ingetrokken, maar desalniettemin het betrokken PKI@BNPPF Certificate heeft aanvaard en er haar vertrouwen in heeft gesteld;
5. de onbeschikbaarheid van de Validation Authority of het repository, om welke reden dan ook;
6. foute of onnauwkeurige informatie in de CRL van Isabel die gebruikt wordt door de Validation Authority, tenzij Isabel de CRL niet heeft bijgewerkt volgens de in deze PKI@BNPPF CP vastgestelde procedures, in welk geval Isabel aansprakelijk is, behoudens andere beperkingen of uitsluitingen die hieronder worden bepaald, ten aanzien van een Relying Party, voor zover de betrokken Relying Party kan aantonen dat zij als gevolg van deze niet-naleving van de voorschriften een verlies of schade heeft geleden;

7. het feit dat een PKI@BNPPF Registration Authority zijn verplichtingen niet is nagekomen die voortvloeien uit deze PKI@BNPPF CP dan wel (indien van toepassing) een overeenkomst tussen een Relying Party en de betrokken PKI@BNPPF Registration Authority, naargelang het geval;
8. het verlies of de compromittering van de Private Key van een PKI@BNPPF Registration Authority;
9. de niet-nakoming door een Revocation Service (intrekkingsdienst) van zijn uit de geldende PKI@BNPPF CP voortvloeiende verplichtingen;
10. het verlies of de compromittering van een Revocation Service Private Key;
11. de niet-naleving door een andere partij, met inbegrip van PKI@BNPPF Registration Authority's, van haar verplichtingen tegenover een Relying Party;
12. elk ander gebruik van het PKI@BNPPF Certificate, de Private Key en/of de software dan voor de in deze PKI@BNPPF CP voorziene doelen;
13. wijzigingen of gewijzigde situaties die niet aan Isabel zijn gemeld;
14. verkeerd gebruik of misbruik door BNP Paribas Fortis Subscribers, Subjects, Customers en/of Relying Parties.

2.2.1.3. INDIRECTE EN GEVOLGSCHADE VOOR BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS EN RELYING PARTIES

Zelfs indien Isabel in kennis werd gesteld van de mogelijkheid van dergelijke schade is Isabel geenszins aansprakelijk voor:

1. indirect of resulterend verlies dan wel indirecte of gevolgschade;
2. winstderving;
3. schadevergoedingen als sanctie;
4. gevolgen van procedures en vorderingen die derde partijen inleiden tegen BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties;
5. verlies van goodwill;
6. niet-verwezenlijking van verwachte besparingen;
7. inkomstenderving;
8. gemiste zakelijke kansen;
9. onderbreking van zakelijke activiteiten; of
10. verlies van informatie of gegevens.

2.2.1.4. BEPERKING VAN DE AANSPRAKELIJKHEID VAN ISABEL TEGENOVER BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS EN RELYING PARTIES

Indien Isabel aansprakelijk is, bedraagt de totale aansprakelijkheid van Isabel tegenover alle partijen, met inbegrip van, maar niet beperkt tot BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties, met betrekking tot individuele vorderingen of een reeks gerelateerde vorderingen, geenszins meer dan de hieronder voor dergelijke PKI@BNPPF Certificates vastgestelde aansprakelijkheidslimiet. De totale aansprakelijkheid van Isabel tegenover welke persoon ook bedraagt voor alle handtekeningen en verrichtingen die verband houden met een dergelijk PKI@BNPPF Certificate maximaal 2.500 EUR. Die aansprakelijkheidslimiet van 2.500 EUR geldt tussen Isabel enerzijds en de BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties anderzijds.

Die begrenzing van de schadevergoeding geldt voor alle vormen van verlies en schade geleden door een persoon, inclusief zonder enige beperking BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties, als gevolg van diens vertrouwen in of diens gebruik van een PKI@BNPPF Certificate dat Isabel uitgeeft, beheert, gebruikt, intrekt of een dergelijk certificaat dat vervalt. Die beperking van de schadevergoeding geldt eveneens voor contractuele aansprakelijkheid, onrechtmatige daden en enige andere vorm van aansprakelijkheidsvorderingen. De aansprakelijkheidslimiet is voor elk PKI@BNPPF Certificate gelijk, ongeacht het aantal digitale handtekeningen, verrichtingen of vorderingen dat met het betrokken certificaat in verband wordt gebracht. Indien de aansprakelijkheidsgrens wordt overschreden, wordt het bedrag van de maximale aansprakelijkheid eerst toegewezen aan de eerste vorderingen om het geschil definitief te beslechten, tenzij een rechter of een andere bevoegde rechterlijke instantie anders bepaalt. Isabel is per certificaat geenszins verplicht meer te betalen dan de totale aansprakelijkheidslimiet.

2.2.1.5. OVERMACHT

Indien Isabel haar verplichtingen niet kan nakomen, laattijdig nakomt of bij het nakomen ervan gehinderd wordt, ongeacht of het verplichtingen betreft uit hoofde van dit document dan wel verplichtingen die voortvloeien uit een ander toepasselijk document, door een geval van overmacht, zoals oorlog, terrorisme, een opstand, stakingen, sociale conflicten, ongevallen, brand, overstromingen of incidenten met derde partijen (zoals vertragingen in transport of levering, defecten in apparatuur of problemen met gegevensoverdrachtsverbindingen), is Isabel niet aansprakelijk voor:

1. de laattijdige of niet-nakoming van dergelijke verplichtingen in zoverre dit het gevolg is van de overmacht; en
2. verlies of schade geleden door, vorderingen ingesteld tegen of kosten gedaan door Relying Parties als gevolg van de laattijdige of de niet-nakoming van dergelijke verplichtingen door Isabel als gevolg van de overmacht.

2.2.1.6. BEPERKING VAN DE UITSLUITING OF DE BEPERKING VAN DE AANSPRAKELIJKHEID VAN ISABEL

Niets in dit document beperkt de aansprakelijkheid van Isabel of sluit die uit voor het volgende:

1. een overlijden of persoonlijke verwondingen als gevolg van nalatigheid van Isabel; of
2. bedrog door Isabel.

2.2.2. PKI@BNPPF RA AANSPRAKELIJKHEID

2.2.2.1. GARANTIES EN BEPERKINGEN OP DE GARANTIES

BNP Paribas FortisBNP Paribas garandeert uitsluitend dat elk uitgegeven PKI@BNPPF Certificate wordt uitgegeven overeenkomstig de bepalingen in deze PKI@BNPPF CP voor het geboden garantieniveau. Aanvullend kan de wet in andere garanties voorzien.

Tenzij anders is overeengekomen, en binnen de grenzen van de toepasselijke wetgeving, wijst BNP Paribas Fortis alle vormen van garanties en verplichtingen af, met inbegrip van garanties inzake verhandelbaarheid, geschiktheid voor een bepaald gebruiksdoel en nauwkeurigheid van verstrekte informatie, en weigert BNP Paribas Fortis voorts elke aansprakelijkheid voor nalatigheid of onzorgvuldigheid vanwege BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties.

2.2.2.2. UITSLUITING VAN DE AANSPRAKELIJKHEID VAN BNP PARIBAS FORTIS TEN AANZIEN VAN BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS EN RELYING PARTIES

BNP Paribas FortisBNP Paribas Fortis is, tenzij hieronder anders wordt bepaald, niet aansprakelijk voor enig verlies of enige schade geleden door, vorderingen ingesteld tegen of kosten opgelopen door BNP Paribas Fortis Subscribers, Subjects, Customers en/of Relying Parties, voor zover het verlies of de schade, vorderingen of kosten voortvloeien uit:

1. het verlies of de compromittering van de Private Key van BNP Paribas Fortis Subjects, tenzij BNP Paribas Fortis de in deze CP vastgestelde voorschriften niet heeft nageleefd, in welk geval BNP Paribas Fortis aansprakelijk is (behoudens andere beperkingen of uitsluitingen die hieronder worden bepaald) tegenover een Relying Party op voorwaarde dat de betrokken Relying Party kan aantonen dat zij verlies of schade heeft geleden als gevolg van de niet-naleving van de voorschriften door BNP Paribas Fortis;
2. onnauwkeurige of foute informatie in een PKI@BNPPF Certificate dat werd uitgegeven door een Isabel CA, tenzij BNP Paribas Fortis niet alle redelijke inspanningen heeft geleverd om de nauwkeurigheid en juistheid van dergelijke informatie te garanderen of tenzij BNP Paribas Fortis de authenticiteit van alle documentaire bewijzen van dergelijke informatie niet heeft gecontroleerd overeenkomstig deze PKI@BNPPF CP, in welk geval BNP Paribas Fortis aansprakelijk is (behoudens andere beperkingen en uitsluitingen die hieronder worden bepaald) tegenover een Relying Party voor zover de betrokken Relying Party kan aantonen dat zij verlies of schade heeft geleden als gevolg van de niet-geleverde inspanningen of de niet-controle door BNP Paribas Fortis;

3. het feit dat een Relying Party haar vertrouwen heeft gesteld in een ingetrokken PKI@BNPPF Certificate dat was uitgegeven door een Isabel CA, indien de betrokken Relying Party niet heeft gecontroleerd of het PKI@BNPPF Certificate in kwestie nog was ingetrokken;
4. het feit dat een Relying Party haar vertrouwen heeft gesteld in een door een Isabel CA uitgegeven PKI@BNPPF Certificate, indien die Relying Party wist of redelijkerwijze had moeten weten dat het betrokken PKI@BNPPF Certificate was ingetrokken, maar het PKI@BNPPF Certificate desondanks heeft aanvaard en erop heeft vertrouwd;
5. de onbeschikbaarheid van de CRL of het repository van Isabel, om welke reden dan ook;
6. foute of onnauwkeurige informatie in de CRL van Isabel;
7. enig ander gebruik van het PKI@BNPPF Certificate, de Private Key en/of de software dan voor de doeleinden die op basis van deze PKI@BNPPF CP zijn toegelaten;
8. wijzigingen of gewijzigde situaties die niet aan de PKI@BNPPF RA zijn gemeld;
9. verkeerd gebruik of misbruik door Subscribers, Subjects, Customers en/of Relying Parties.

2.2.2.3. INDIRECTE EN GEVOLGSCHADE VOOR BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS EN RELYING PARTIES

Zelfs indien BNP Paribas Fortis in kennis werd gesteld van de mogelijkheid van dergelijke schade, is BNP Paribas Fortis in geen geval aansprakelijk voor enig indirect of resulterend verlies dan wel enige indirecte of gevolgschade, met inbegrip van, maar niet beperkt tot:

1. winstderving;
2. schadevergoedingen als sanctie;
3. gevolgen van procedures en vorderingen die door derde partijen worden ingeleid tegen BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties;
4. verlies van goodwill;
5. niet-verwezenlijking van verwachte besparingen;
6. inkomstenderving;
7. gemiste zakelijke kansen;
8. onderbreking van zakelijke activiteiten; of
9. verlies van informatie of gegevens.

2.2.2.4. BEPERKING VAN DE AANSPRAKELIJKHEID VAN BNP PARIBAS FORTIS TEGENOVER BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS EN RELYING PARTIES

Indien BNP Paribas Fortis aansprakelijk is, bedraagt de totale aansprakelijkheid van BNP Paribas Fortis aan alle partijen, met inbegrip van, maar niet beperkt tot BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties, met betrekking tot een individuele vordering dan wel een reeks gerelateerde vorderingen, in geen geval meer dan de aansprakelijkheidslimiet die hieronder voor een PKI@BNPPF Certificate is vastgesteld. De totale aansprakelijkheid van BNP Paribas Fortis tegenover alle personen die betrokken zijn bij een PKI@BNPPF Certificate bedraagt voor alle handtekeningen en transacties die met een dergelijk PKI@BNPPF Certificate zijn verricht, niet meer dan het grootste van de twee onderstaande bedragen: 2.500 EUR of een bedrag dat overeenstemt met de vergoedingen die op één jaar voor de dienstverlening inzake PKI@BNPPF Certificates betaald worden.

Die beperking van schadevergoedingen geldt voor elk verlies en alle schade geleden door welke persoon dan ook, inclusief, maar niet beperkt tot BNP Paribas Fortis Subscribers, Subjects, Customers en Relying Parties, doordat hij/zij zijn/haar vertrouwen stelde in of gebruikgemaakt heeft van een PKI@BNPPF Certificate dat werd uitgegeven, beheerd, gebruikt of ingetrokken door een Isabel CA dan wel een PKI@BNPPF Certificate dat vervalt. Die beperking van de schadevergoeding geldt eveneens voor contractuele aansprakelijkheid, onrechtmatige daden en enige andere vorm van aansprakelijkheidsvorderingen. De aansprakelijkheidslimiet is voor elk PKI@BNPPF Certificate gelijk, ongeacht het aantal digitale handtekeningen, verrichtingen of vorderingen dat met een dergelijk PKI@BNPPF Certificate in verband wordt gebracht. Indien de aansprakelijkheidsgrens wordt overschreden, wordt het bedrag van de maximale aansprakelijkheid eerst toegewezen aan de eerste vorderingen om het geschil definitief te beslechten, tenzij een rechter of een andere bevoegde rechterlijke instantie anders bepaalt. BNP Paribas Fortis is in geen geval verplicht om voor elk PKI@BNPPF Certificate meer te betalen dan het maximumbedrag van de totale aansprakelijkheid.

2.2.2.5. OVERMACHT

Indien BNP Paribas Fortis haar verplichtingen niet kan nakomen, laattijdig nakomt of bij het nakomen ervan gehinderd wordt, ongeacht of het verplichtingen betreft uit hoofde van dit document dan wel verplichtingen die voortvloeien uit een ander toepasselijk document, door een geval van overmacht, zoals oorlog, terrorisme, een opstand, stakingen, sociale conflicten, ongevallen, brand, overstromingen of incidenten met derde partijen (zoals vertragingen in transport of levering, defecten in apparatuur of problemen met gegevensoverdrachtsverbindingen), is BNP Paribas Fortis niet aansprakelijk voor:

1. de laattijdige of niet-nakoming van dergelijke verplichtingen in zoverre dit het gevolg is van de overmacht; en
2. enige vorm van verlies of schade geleden door, vorderingen van welke aard ook ingesteld tegen of enige kosten gedaan door Relying Parties ingevolge de laattijdige of niet-nakoming van dergelijke verplichtingen door BNP Paribas Fortis als gevolg van de overmacht.

2.2.2.6. BEPERKING VAN DE UITSLUITING OF DE BEPERKING VAN DE AANSPRAKELIJKHEID VAN BNP PARIBAS FORTIS

Niets in dit document beperkt de aansprakelijkheid van BNP Paribas Fortis of sluit die uit voor:

1. een overlijden of persoonlijke verwondingen als gevolg van de nalatigheid van BNP Paribas Fortis of Isabel; of
2. bedrog door BNP Paribas Fortis of Isabel.

2.2.3. AANSPRAKELIJKHEID VAN BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS EN RELYING PARTIES

Door een PKI@BNPPF Certificate te aanvaarden of te gebruiken, stemmen BNP Paribas Fortis Subscribers, Subjects, Customers en/of Relying Parties ermee in BNP Paribas Fortis, Isabel en haar agent(en) en onderaannemers te vrijwaren tegen handelingen of het gebrek daaraan die leiden tot aansprakelijkheid, verlies of schade, rechtszaken en enigerlei kosten waarmee BNP Paribas Fortis, Isabel en haar agent(en) en onderaannemers eventueel geconfronteerd worden als gevolg van het gebruik of de publicatie van een PKI@BNPPF Certificate en te wijten zijn aan:

1. de niet-nakoming van hun in dezePKI@BNPPF CP beschreven verplichtingen;
2. leugens of een verkeerde voorstelling van zaken door de betrokken BNP Paribas Fortis Customer, Subscriber of Subject;
3. het niet melden door de BNP Paribas Fortis Customer, Subscriber of Subject van een belangrijk feit, indien de verkeerde voorstelling of weglating uit nalatigheid voortkwam of ten doel had BNP Paribas Fortis, een PKI@BNPPF RA of een andere persoon die het PKI@BNPPF Certificate ontvangt of erop vertrouwt, te misleiden;
4. het niet beschermen van de Private Key van de BNP Paribas Fortis Subscribers of Subjects, het niet gebruiken van een betrouwbaar systeem of het achterwege laten van andere voorzorgsmaatregelen die nodig zijn om de compromittering, het verlies, de onthulling, de wijziging of het ongeoorloofde gebruik van een dergelijke Private Key te voorkomen;
5. enig ander gebruik van het PKI@BNPPF Certificate, de Private Key en/of de software dan voor het door BNP Paribas Fortis toegelaten gebruiksdoel.

Alle BNP Paribas Fortis Customers, Subscribers, Subjects en Relying Parties aanvaarden dat het gebruik van een PKI@BNPPF Certificate buiten de BNP Paribas Fortis-gemeenschap (zie punt "1.3 – Gemeenschap en toepassingsgebied") zonder de uitdrukkelijke toestemming van BNP Paribas Fortis dan wel het gebruik van een PKI@BNPPF Certificate nadat een bepaald gebruik door BNP Paribas Fortis in een aanmaning (cease-and-desist letter) werd verboden de hierboven beschreven aansprakelijkheid in werking doet treden en dat een dergelijk verboden gebruik door het feit zelf als een schending van deze PKI@BNPPF CP wordt beschouwd.

2.3. FINANCIËLE AANSPRAKELIJKHEID

BNP Paribas Fortis BNP Paribas Fortis heeft met een gerenommeerde verzekeraar een verzekeringscontract afgesloten voor haar professionele financiële-aansprakelijkheidsrisico's die

voortvloeien uit haar activiteiten en haar aansprakelijkheid met betrekking tot de PKI@BNPPF Certificates-dienstverlening. Isabel NV/SA moeten een voldoende beroepsaansprakelijkheid verzekering hebben in het kader van de uitvoering van haar verplichtingen als CA.

2.3.1. SCHADELOOSSTELLING DOOR BNP PARIBAS FORTIS CUSTOMERS, RELYING PARTIES EN SUBJECTS EN DOOR BNP PARIBAS FORTIS

BNP Paribas FortisCustomers en/of Relying Parties en/of PKI@BNPPF Certificate Subjects moeten alle partijen (inclusief de Isabel Certification Authority en de Isabel PKI@BNPPF RA's) en/of BNP Paribas Fortis alle uit de niet-nakoming van hun verplichtingen voortvloeiende schade vergoeden.

Indien vastgesteld wordt dat een Relying Party niet in overeenstemming met de in deze PKI@BNPPF CP vastgestelde voorschriften heeft gehandeld, heeft deze geen verhaal tegen Isabel in geval van schade.

BNP Paribas Fortis BNP Paribas Fortis is niet aansprakelijk voor de gevolgen wanneer een Relying Party haar verplichtingen niet nakomt.

2.3.2. FIDUCIAIRE RELATIES

De relatie tussen BNP Paribas Fortis en PKI@BNPPF Certificate Subjects en tussen BNP Paribas Fortis en PKI@BNPPF Certificate Relying Parties is er geen van agent en principaal. PKI@BNPPF Certificate Subjects noch Relying Parties zijn gemachtigd om in naam van BNP Paribas Fortis verbintenissen aan te gaan, in het kader van een overeenkomst of anderszins.

2.3.3. ADMINISTRATIEF PROCES

BNP Paribas Fortis De rekeningen en het jaarverslag van BNP Paribas Fortis worden jaarlijks gepubliceerd en gecontroleerd overeenkomstig de Belgische wetgeving.

2.4. INTERPRETATIE EN HANDHAVING

In geval van tegenspraak of een gebrek aan samenhang tussen deze PKI@BNPPF CP en contracten die BNP Paribas Fortis Customers en PKI@BNPPF Certificate Subscribers en Subjects binden ten opzichte van BNP Paribas Fortis, hebben de bepalingen van deze PKI@BNPPF CP voorrang op die contracten en andere specifieke recentere overeenkomsten, tenzij anders is bepaald en voor zover zij van toepassing zijn op PKI@BNPPF Certificates.

2.4.1. TOEPASSELIJK RECHT

De afdwingbaarheid, de samenstelling, de interpretatie en de geldigheid van deze PKI@BNPPF CP worden geregeld door de wetgeving van België.

2.4.2. AFSPLITSBAARHEID, VANKRACHTBLIJVING, SAMENVOEGING, KENNISGEVING

Indien een rechter, een bevoegde rechtbank of een soortgelijke instantie bepalingen en voorwaarden in dit document ongeldig, niet-afdwingbaar of onwettelijk verklaart, worden de betrokken bepalingen en voorwaarden afgesplitst van de rest van het document, dat van kracht blijft. Die bepalingen en voorwaarden worden vervangen door clausules die de intentie van de ongeldige clausules zo goed mogelijk benaderen.

Indien, in uitzonderlijke gevallen, volgens de wetgeving van een grondgebied waaronder buitenlandse PKI@BNPPF Certificate Subscriber Subjects vallen, specifieke bepalingen van deze PKI@BNPPF CP onwettig zijn, zijn deze specifieke bepalingen van de CP uitsluitend voor de betrokken PKI@BNPPF Certificate Subscribers en Subjects ongeldig en kunnen zij alleen voor hen worden beschouwd als niet in de tekst opgenomen, in welk geval de eerste alinea van dit punt van toepassing is.

De bepalingen die door hun aard ook na de geldigheid van deze CP van kracht moeten blijven, blijven van kracht.

Alle officiële kennisgevingen die uit hoofde van deze CP vereist zijn, dienen schriftelijk te gebeuren, per aangetekende brief, per fax of met een e-mail die met een geavanceerde elektronische handtekening wordt ondertekend.

2.4.3. PROCEDURES VOOR DE BESLECHTING VAN GESCHILLEN

Alle betrokken partijen, de Isabel CA en PKI@BNPPF RA, alsmede de BNP Paribas Fortis Customers, Subscribers, Subjects en Relying Parties leveren te goeder trouw billijke inspanningen om vorderingen, geschillen en twisten in der minne te regelen.

Indien geen minnelijke schikking kan worden bereikt binnen een redelijke termijn, worden alle geschillen uitsluitend aan de rechtbanken van Brussel voorgelegd.

2.5. VERGOEDINGEN

Vergoedingen voor PKI@BNPPF Certificates en daarbij horende diensten en de modaliteiten daarvan worden vastgesteld in contracten tussen de PKI@BNPPF Certificate Customers/Subscribers/Subjects en BNP Paribas Fortis.

Die vergoedingen kunnen slechts worden terugbetaald indien dat vooraf uitdrukkelijk is overeengekomen.

2.6. PUBLICATIE EN REPOSITORY

2.6.1. PUBLICATIE VAN INFORMATIE

De volgende informatie moet worden gepubliceerd:

1. deze PKI@BNPPF CP;
2. de PKI@BNPPF Certificates die het Subject heeft aanvaard en waarover hij bijgevolg heeft verklaard dat de informatie ervan correct is;
3. de Certificate Revocation Lists voor PKI@BNPPF Certificates.
4. het Self-Signed Certificate en de kruiselingse certificaten van de Isabel CA's;
5. BNP Paribas Fortis de algemene voorwaarden van de certificeringsdiensten;
6. de modelcontracten van BNP Paribas Fortis voor de certificeringsdiensten.

Deze informatie wordt online bekendgemaakt en kan in diverse vormen worden gepubliceerd.

2.6.2. PUBLICATIEREGELMAAT

PKI@BNPPF Certificates worden gegarandeerd gepubliceerd binnen 24 uur na de aanvaarding ervan door hun Subject. Doorgaans worden PKI@BNPPF Certificates gepubliceerd binnen het halfuur nadat ze zijn aanvaard.

De Certificate Revocation Lists (CRL) worden normaal gezien binnen het halfuur na een verandering bijgewerkt en uiterlijk om de 24 uur wordt een nieuwe versie gepubliceerd.

De versiehistoriek van de PKI@BNPPF CP wordt nauwgezet bijgehouden en is als vermeld in dit document.

De publicatie van de PKI@BNPPF CP wordt behandeld in punt "8 – SPECIFICATIEBEHEER" van deze PKI@BNPPF CP.

2.6.3. TOEGANGSCONTROLE

De Isabel CA's zorgen ervoor dat passende controlemiddelen beschikbaar zijn voor de toegang, om te voorkomen dat onbevoegden certificaten, beleidsdocumenten, CRL's en andere in het repository opgenomen informatie plaatsen, wijzigen of verwijderen.

Deze PKI@BNPPF CP mag uitsluitend in de **"alleen lezen"-modus** worden ingekeken door:

1. de Isabel Certification Authority;
2. de PKI@BNPPF RA's;
3. de PKI@BNPPF Certificate Subscribers en Subjects;
4. de PKI@BNPPF Certificate Relying Parties.

Deze PKI@BNPPF CP mag worden geopend in de modus "schrijven en wijzigen" door de Policy Authority (zie punt "8 – SPECIFICATIEBEHEER").

De volgende partijen mogen PKI@BNPPF Certificates uitsluitend in de **"alleen lezen"-modus** openen:

1. de PKI@BNPPF RA's;
2. de PKI@BNPPF Certificate Subscribers en Subjects;
3. de BNP Paribas Fortis Policy Authority.

De PKI@BNPPF Certificates en de Certificate Revocation List voor PKI@BNPPF Certificates mag door de Isabel Certification Authority worden geopend in de modus **"schrijven en wijzigen"**.

De valideringsdienst is enkel toegankelijk voor de PKI@BNPPF CP Customer.

2.6.4. REPOSITORIES

De PKI@BNPPF Certificates en de Certificate Revocation Lists voor PKI@BNPPF Certificates worden in een directory van Isabel gepubliceerd.

Niet de Isabel Certification Authority maar wel Isabel nv staat in voor het beheer van die directory.

2.7. CONTROLE OP DE NALEVING VAN DE VOORSCHRIFTEN

BNP Paribas Fortis onderwerpt al haar procedures en de overeenstemming daarvan met deze PKI@BNPPF CP aan audits. Een audit kan worden uitgevoerd om te controleren of Isabel NV / SA is in lijn met de uitvoering van haar verplichtingen als CA.

2.7.1. REGELMAAT VAN DE CONTROLE OP DE NALEVING VAN DE VOORSCHRIFTEN DOOR DE ENTITEITEN

De regelmaat van deze audits wordt bepaald door:

1. BNP Paribas Fortis het interne beleid;
2. de toepasselijke Belgische wetgeving;
3. andere partijen die gemachtigd zijn om een audit uit te voeren uit hoofde van hun relatie met BNP Paribas Fortis.

2.7.2. IDENTITEIT EN KWALIFICATIES VAN DE AUDITEURS

De auditeurs zijn onafhankelijk en hebben gespecialiseerde kennis over Public Key Infrastructure.

De kwalificaties van de auditeurs zijn in overeenstemming met de beroepspraktijken en de wettelijke vereisten, indien van toepassing. De kerntaak van de auditeurs bestaat erin de CA of de veiligheid van het informatiesysteem te controleren en zij moeten zeer goed vertrouwd zijn met PKI-beleidsdocumenten (CPS'en en CP's).

2.7.3. RELATIE TUSSEN DE AUDITEUR EN DE GECONTROLEERDE PARTIJ

De auditeurs moeten onafhankelijk zijn ten aanzien van BNP Paribas Fortis en Isabel nv.

De auditeurs dienen een contractuele relatie te hebben met BNP Paribas Fortis voor de uitvoering van de audit en moeten in organisatorisch opzicht voldoende afgescheiden zijn van de gecontroleerde Isabel CA PKI@BNPPF RA en enig ander onderdeel van BNP Paribas Fortis of van de PKI met het oog op een objectieve en onafhankelijke evaluatie.

2.7.4. INHOUD VAN DE AUDITS

De audits hebben betrekking op:

1. de infrastructuur van de Isabel CA;
2. het beheer van de Isabel CA;
3. de voornaamste beleidslijnen en procedures van de Isabel CA;
4. de werking van de Isabel CA;
5. de werking van de PKI@BNPPF RA's;
6. de naleving van de PKI@BNPPF CP;
7. de naleving van de Belgische regelgeving.

2.7.5. MAATREGELEN NAAR AANLEIDING VAN TEKORTKOMINGEN

De auditverslagen worden beoordeeld door BNP Paribas Fortis. Afwijkingen van de PKI@BNPPF CP en andere onregelmatigheden krijgen prioriteit en er wordt een planning opgesteld om die bij te sturen, met inachtneming van het restrisico. Er kan een nieuwe audit worden uitgevoerd om de gevraagde verbeteringen te evalueren.

2.7.6. BEKENDMAKING VAN DE RESULTATEN

De auditresultaten worden in een verslag gegoten dat uitsluitend gericht is aan de Security Manager van BNP Paribas Fortis.

De informatie in het auditverslag wordt niet openbaar gemaakt, tenzij de nationale wetgeving dat vereist. De auditresultaten moeten in het kader van deze CP als strikt vertrouwelijk worden beschouwd.

2.8. VERTROUWELIJKHEID

2.8.1. GEHEIM TE HOUDEN INFORMATIETYPES

Alle informatie in verband met de aanvraag, de uitgifte, de aanvaarding en de intrekking van PKI@BNPPF Certificates wordt als vertrouwelijk gezien. De toegang ertoe is beperkt, tenzij de betrokken informatie is vermeld in punt "2.8.2 – Niet-vertrouwelijke informatietypes".

Die informatie kan deel uitmaken van een bilaterale overeenkomst tussen BNP Paribas Fortis en een derde partij en is mogelijk onthuld in het kader van een geheimhoudingsovereenkomst.

De volgende informatie is uitsluitend bestemd voor PKI@BNPPF Certificate Subscribers, Subjects en Relying Parties:

1. PKI@BNPPF Certificates en de informatie die zij bevatten;
2. de Self-Signed Certificates van de Isabel Certification Authorities.

2.8.2. NIET-VERTROUWELIJKE INFORMATIETYPES

Deze PKI@BNPPF CP is voor iedereen toegankelijk en valt dan ook niet onder de in dit punt opgelegde geheimhoudingsplicht.

Aangezien deze PKI@BNPPF CP niet wordt aangemerkt als een vertrouwelijk document, bevat zij geen vertrouwelijke informatie.

2.8.3. VERSTREKKING VAN INFORMATIE OVER DE INTREKKING VAN CERTIFICATEN

De redenen voor de intrekking van een certificaat worden overeenkomstig de norm X.509 van het ITU-T uitgedrukt met de extensie "Reason code" in de CRL-ingang.

PKI@BNPPF Certificate Subjects of PKI@BNPPF Certificate Subscribers die om de intrekking van het certificaat van een Subject hebben verzocht, worden bericht over de effectieve intrekking van het PKI@BNPPF Certificate.

De reden voor de intrekking wordt niet aan de Relying Parties meegedeeld.

2.8.4. VERSTREKKING AAN FUNCTIONARISSEN VAN WETSHANDHAVINGSINSTANTIES

Isabel CA's en PKI@BNPPF RA's mogen vertrouwelijke informatie vrijgeven indien daartoe een bevel is uitgevaardigd dat naar behoren is ondertekend door een rechter of gerechtsdienaar in het kader van een strafonderzoek dan wel indien de wet dat vereist.

2.8.5. VRIJGAVE IN HET KADER VAN "CIVIL DISCOVERY"

Geen bepalingen.

2.8.6. VERSTREKKING OP VERZOEK VAN EEN SUBSCRIBER OF SUBJECT

Isabel CA's en PKI@BNPPF RA's mogen vertrouwelijke informatie over PKI@BNPPF Certificate Subscribers en Subjects vrijgeven op verzoek van of met de goedkeuring van de betrokken PKI@BNPPF Certificate Subscribers en Subjects.

2.8.7. ANDERE OMSTANDIGHEDEN WAARIN INFORMATIE WORDT VRIJGEGEVEN

Geen bepalingen.

2.9. INTELLECTUELE-EIGENDOMSRECHTEN

Alle informatie in dit document maakt deel uit van de intellectuele-eigendomsrechten van BNP Paribas Fortis of Isabel. Dit geldt voor alle informatie die wordt gepubliceerd door BNP Paribas Fortis en Isabel, in het kader van een openbare dan wel een privérelatie.

Deze rechten staan boven eventuele contractuele relaties met BNP Paribas Fortis. Het PKI@BNPPF Certificate, de toegangsmiddelen en de middelen voor het plaatsen van handtekeningen, met inbegrip van de Public Key, zijn het exclusieve eigendom van Isabel. Ieder gebruik van de PKI@BNPPF Certificates, de toegangsmiddelen en de middelen voor het plaatsen van handtekeningen voor andere doeleinden dan de functies van het systeem van BNP Paribas Fortis moeten worden opgenomen in een contract met BNP Paribas Fortis. Wanneer alle aan een bepaalde Public Key gekoppelde certificaten zijn vervallen of ingetrokken, mag het Subject, de Subscriber of de Customer de gegevens betreffende het genereren van handtekeningen na de vervaldatum of de intrekking niet meer gebruiken om een handtekening te plaatsen of dergelijke gegevens te laten certifiëren door een andere certificeringsdienstverlener.

3. IDENTIFICATIE EN AUTHENTICATIE

In dit hoofdstuk worden de procedures beschreven volgens welke een PKI@BNPPF Certificate Subscriber vóór de uitgifte van het certificaat wordt geauthenticeerd. Tevens wordt erin beschreven hoe partijen die om een nieuw certificaat of de intrekking van een bestaand certificaat vragen, worden geauthenticeerd. Ten slotte wordt ingegaan op de naamgeving, inclusief de erkenning van naambezit en de beslechting van naamgeschillen.

3.1. EERSTE REGISTRATIE

Dit punt bevat de bepalingen inzake identificatie en authenticatie in het kader van de initiële registratie van een PKI@BNPPF Certificate Subject.

Er zijn 2 soorten PKI@BNPPF Certificate Subjects:

- Physical Person Subjects: het Subject wordt vertegenwoordigd door de natuurlijke persoon van wie de identiteit in het certificaat is opgenomen.
- Function Subjects: het Subject wordt vertegenwoordigd door één natuurlijke persoon die gemachtigd is om de functie waarvan de identiteit in het certificaat is opgenomen, te vertegenwoordigen (functievertegenwoordiger).

3.1.1. NAAMTYPES

Een Isabel CA moet de "X.500 Distinguished Name"-indeling gebruiken voor de velden van een PKI@BNPPF Certificate waarin de namen van het Subject en de Issuer worden opgenomen.

3.1.2. NAMEN MOETEN BETEKENIS HEBBEN

De PKI@BNPPF RA's moeten erop toezien dat de Distinguished Name van het Subject van een PKI@BNPPF Certificate in de X.500-naamruimte waarvoor Isabel gemachtigd is betekenis heeft.

Een Isabel CA geeft geen anonieme certificaten uit, noch certificaten onder een alias.

3.1.3. REGELS VOOR DE INTERPRETATIE VAN DE VERSCHILLENDE NAAMVORMEN

Distinguished Names in certificaten dienen te worden geïnterpreteerd overeenkomstig de X.500-normen en de ASN.1-norm. Zie RFC 2253 en RFC 2616 voor meer informatie over hoe X.500 Distinguished Names in certificaten worden geïnterpreteerd als Uniform Resource Identifiers en HTTP-verwijzingen.

3.1.4. NAAMUNICITEIT

Isabel CA's moeten de uniciteit garanderen van de Distinguished Name van het Subject in een PKI@BNPPF Certificate in de X.500-naamruimte waarvoor Isabel gemachtigd is en die is voorbehouden aan BNP Paribas Fortis.

Zie "7 – Certificaat-, CRL- en OCSP-profielen".

3.1.5. PROCEDURE VOOR DE BESLECHTING VAN NAAMGESCHILLEN

De Isabel CA's zijn gemachtigd om alle geschillen op te lossen in verband met de Distinguished Name van Subjects in PKI@BNPPF Certificates in de X.500-naamruimte(s) waarvoor Isabel bevoegd is.

3.1.6. ERKENNING, AUTHENTICATIE EN ROL VAN HANDELSMERKEN

PKI@BNPPF RAPKI@BNPPF RA's kunnen niet controleren of garanderen dat handelsmerken, dienstmerken en andere in PKI@BNPPF Certificates vermelde tekens rechtmatig kunnen worden gebruikt zonder dat intellectuele-eigendomsrechten worden geschonden. De RA's en CA's binnen de PKI zijn niet verplicht om een dergelijke eventuele schending te onderzoeken.

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

Geen bepalingen.

3.1.8. AUTHENTICATIE VAN DE IDENTITEIT VAN EEN ORGANISATIE

Een PKI@BNPPF RA moet verplicht de identiteit van een kandidaat-BNP Paribas Fortis Customer authenticeren voordat Subscribers van deze BNP Paribas Fortis Customer PKI@BNPPF Certificates mogen aanvragen.

De identiteit van een kandidaat-BNP Paribas Fortis Customer wordt geauthenticeerd in het kader van het inschrijvingsproces dat wordt gevolgd voor de ondertekening van een diensten- of productovereenkomst van BNP Paribas Fortis tussen deze BNP Paribas Fortis Customer en BNP Paribas Fortis. Het contract bevat voorts nadere informatie over de authenticatieprocedure en de bewijsstukken die een kandidaat- BNP Paribas Fortis Customer in het kader van het inschrijvingsproces aan de PKI@BNPPF RA moet verstrekken.

3.1.9. AUTHENTICATIE VAN DE INDIVIDUELE IDENTITEIT

De identiteit van een BNP Paribas Fortis Customer die een aanvraag heeft ingediend, wordt gecontroleerd en vastgesteld volgens een gedocumenteerde procedure die wordt uitgevoerd door de PKI@BNPPF RA's.

3.2. GEWONE VERNIEUWING VAN CERTIFICATEN

Niet-ingetrokken PKI@BNPPF Certificates worden automatisch door de Isabel CA vernieuwd wanneer het einde van de geldigheidsduur van de certificaten nadert.

3.3. TOEWIJZING VAN EEN NIEUW SLEUTELPAAR NA INTREKKING

Indien een PKI@BNPPF Certificate Subject van wie het PKI@BNPPF Certificate is ingetrokken een nieuw PKI@BNPPF Certificate wil aanvragen, dient hij/zij het hele PKI@BNPPF Certificate-proces opnieuw te doorlopen en moet zijn/haar identiteit opnieuw worden gecontroleerd en vastgesteld.

In dat geval wordt een nieuwe PKI@BNPPF Secure Signing Card uitgegeven, die aan de Subscriber wordt bezorgd.

3.4. INTREKKINGSVERZOEK

BNP Paribas Fortis Customers moeten de PKI@BNPPF RA verzoeken om hun PKI@BNPPF Certificate in te trekken. Indien deze onbereikbaar is, kan een beroep gedaan worden op de Card Stop Revocation Service.

3.4.1. AUTHENTICATIE DOOR DE PKI@BNPPF REVOCATION SERVICE PKI@BNPPF REVOCATION SERVICE

De PKI@BNPPF revocation service moet het Subject identificeren en authenticeren om een intrekkingsverzoek te genereren. Voor de authenticatie dient een handgeschreven formulier te worden gebruikt.

De PKI@BNPPF Revocation Service genereert een intrekkingsverzoek op basis van de informatie die het Subject in papieren vorm heeft verstrekt.

3.4.2. AUTHENTICATIE DOOR DE PKI@BNPPF REVOCATION SERVICE PKI@BNPPF REGISTRATION AUTHORITY

De PKI@BNPPF Registration Authority's worden beheerd door de BNP Paribas Fortis Operations Teams.

PKI@BNPPF Registration Authority De PKI@BNPPF Revocation Service genereert een intrekkingsverzoek op basis van de informatie die het Subject in papieren vorm heeft verstrekt.

3.4.3. AUTHENTICATIE DOOR DE CARD STOP REVOCATION SERVICE

De Card Stop Revocation Service mag slechts worden gebruikt indien de PKI@BNPPF Registration Authority niet beschikbaar is. De Card Stop Revocation Service wordt beheerd door:

Card Stop

Tel.: +32 (0)70 344 344

Fax: +32 (0)70 344 355

De Card Stop Revocation Service genereert een intrekkingsverzoek op basis van de informatie die het Subject via de telefoon verstrekt.

Achteraf dient een handgeschreven bevestiging te worden bezorgd voor authenticatiedoeleinden en ter bevestiging van het verzoek. De actualisering van de CRL en de publicatie van de geactualiseerde versie worden hierdoor niet vertraagd.

3.4.4. AUTHENTICATIE DOOR EEN ISABEL CA

De Isabel CA authenticeert een intrekkingsverzoek op basis van een digitale handtekening die wordt gegenereerd met de Private Key van de PKI@BNPPF RA en gecontroleerd met het certificaat van de PKI@BNPPF RA.

4. OPERATIONELE VOORSCHRIFTEN

4.1. CERTIFICAATAANVRAGEN

Wanneer een certificaat wordt aangevraagd, valideert een PKI@BNPPF RA de identiteit van de aanvrager. Vervolgens wordt de certificaatsaanvraag door de PKI@BNPPF RA goedgekeurd of verworpen. Een dergelijke goedkeuring of verwerping hoeft niet te worden gemotiveerd, noch tegenover de aanvrager, noch tegenover enige andere partij.

De PKI@BNPPF RA volgt gedocumenteerde procedures en bepaalt haar eigen praktijken.

De Isabel CA verwerkt op een veilige manier de PKI@BNPPF Certificate-verzoeken die onder haar toezicht door de PKI@BNPPF RA's worden uitgegeven en volgt de in punt "2.6.2 – Publicatieregelmaat" vastgestelde publicatieregelmaat. De Isabel CA aanvaardt dergelijke PKI@BNPPF Certificate-verzoeken uitsluitend van officieel erkende PKI@BNPPF RA's.

De Isabel CA verwerpt alle certificaatsaanvragen die niet lijken te voldoen aan de bepalingen van deze PKI@BNPPF CP.

4.2. UITGIFTE VAN CERTIFICATEN

Na de validering en de goedkeuring van een certificaataanvraag stuurt de PKI@BNPPF RA een verzoek tot uitgifte van een certificaat naar de Isabel CA.

Verzoeken van de PKI@BNPPF RA worden goedgekeurd, op voorwaarde dat zij op een geldige wijze worden overgemaakt en dat zij geldige gegevens over de Subscriber bevatten die volgens de specificaties van de Isabel CA zijn ingedeeld.

Uitgegeven PKI@BNPPF Certificates worden aan het Subject bezorgd. Het Subject ontvangt zijn PKI@BNPPF Secure Signing Card en wordt gevraagd zijn eigen PKI@BNPPF Certificate uit het Isabel Repository te downloaden.

4.3. AANVAARDING VAN CERTIFICATEN

De Isabel CA moet een bevestiging krijgen dat het PKI@BNPPF Certificate Subject zijn PKI@BNPPF Certificate aanvaardt.

Het PKI@BNPPF Certificate kan op drie manieren worden aanvaard: (1) met een uitdrukkelijke kennisgeving van de aanvaarding, (2) door het gebruik van het PKI@BNPPF Certificate door het Subject of (3) automatisch na de 10e dag volgend op de publicatie in het Repository indien het Subject geen kennisgeving van zijn aanvaarding heeft verzonden en geen opmerkingen heeft meegedeeld.

Wanneer het Subject zijn PKI@BNPPF Certificate downloadt, installeert en aanvaardt hij ook het Self-Signed Certificate van de Isabel CA.

4.4. SCHORSING EN INTREKKING VAN CERTIFICATEN

4.4.1. OMSTANDIGHEDEN VOOR INTREKKING

Intrekking van een PKI@BNPPF Certificate betekent dat de gebruiksperiode van het certificaat definitief wordt beëindigd voordat het einde van de opgegeven geldigheidsduur is bereikt. De Isabel CA trekt een digitaal certificaat in indien:

- de aan het digitale certificaat gekoppelde Private Key verloren is gegaan dan wel werd gestolen, gewijzigd, onrechtmatig onthuld of anderszins gecompromitteerd;
- de Subscriber, het Subject, Isabel of BNP Paribas Fortis een belangrijke uit deze PKI@BNPPF CP voortvloeiende verplichting niet is nagekomen;
- de Subscriber, Isabel of BNP Paribas Fortis de uit deze PKI@BNPPF CP voortvloeiende verplichtingen laattijdig of helemaal niet uitvoert vanwege een natuurramp, een computerdefect, een communicatieprobleem dan wel enige andere oorzaak die de betrokkene niet onder controle heeft en waardoor de informatie van een andere persoon ernstig in gevaar is gekomen of werd gecompromitteerd;
- Isabel of BNP Paribas Fortis een wettig en bindend bevel van een overheidsinstantie of toezichthouder krijgen om het PKI@BNPPF Certificate in te trekken;
- de informatie over de Subscriber die in het PKI@BNPPF Certificate is opgenomen, is gewijzigd.

4.4.2. WIE KAN EEN INTREKKINGSVERZOEK INDIENEN?

De intrekking van het PKI@BNPPF Certificate van een Physical Person Subject of Function Subject mag worden gevraagd door:

- de natuurlijke persoon van wie de identiteit is opgenomen in een PKI@BNPPF Certificate van een Physical Person Subject;
- de natuurlijke persoon die een Function vertegenwoordigt in een PKI@BNPPF Certificate;
- iedere natuurlijke persoon die door een BNP Paribas Fortis Customer gemachtigd is om de intrekking te vragen van de PKI@BNPPF Certificates van zijn Subject;
- de PKI@BNPPF RA;
- de Isabel CA die het certificaat heeft uitgegeven.

4.4.3. PROCEDURE VOOR INTREKKINGSVERZOEKEN

De Isabel CA verwerkt verzoeken tot intrekking van PKI@BNPPF Certificates die onder haar toezicht door de PKI@BNPPF RA's zijn uitgegeven op een veilige manier en publiceert de intrekking overeenkomstig de in punt "2.6.2 – Publicatieregelmaat" vastgestelde publicatieregelmaat.

4.4.4. BEDENKTIJD VOOR INTREKKINGSVERZOEKEN

Er wordt geen bedenktijd gegeven.

4.4.5. OMSTANDIGHEDEN VOOR DE SCHORSING VAN CERTIFICATEN

Geen bepalingen.

4.4.6. WIE KAN OM DE SCHORSING VAN CERTIFICATEN VERZOEKEN?

Geen bepalingen.

4.4.7. PROCEDURE VOOR SCHORSINGSVERZOEKEN

Geen bepalingen.

4.4.8. BEGRENZING VAN DE SCHORSINGSTERMIJN

Geen bepalingen.

4.4.9. PUBLICATIEREGELMAAT VAN DE CRL

De bijgewerkte Certificate Revocation List wordt overeenkomstig punt "2.6.2 – Publicatieregelmaat" gepubliceerd na de intrekking van een PKI@BNPPF Certificate.

4.4.10. CRL-CONTROLEVEREISTEN

Geen bepalingen.

4.4.11. BESCHIKBAARHEID ONLINEDIENST GELDIGHEIDSCONTROLE (INTREKKINGSSTATUS)

De Isabel CA zorgt ervoor dat de geldigheid (intrekkingsstatus) van certificaten online kunnen worden gecontroleerd.

4.4.12. VOORSCHRIFTEN INZAKE GELDIGHEIDSCONTROLES VIA INTERNET

De onlinedienst voor het controleren van de geldigheid van certificaten geeft statusinformatie op basis van de meest recente CRL.

4.4.13. ANDERE BESCHIKBARE MIDDELEN TER BEKENDMAKING VAN DE INTREKKING VAN CERTIFICATEN

Geen bepalingen.

4.4.14. CONTROLEVEREISTEN VOOR ANDERE MIDDELEN TER BEKENDMAKING VAN DE INTREKKING VAN CERTIFICATEN

Geen bepalingen.

4.4.15. BIJZONDERE VOORSCHRIFTEN INZAKE GECOMPROMITTEERDE SLEUTELS

Geen bepalingen.

4.5. PROCEDURES VOOR DE VEILIGHEIDSAUDITS

De procedure van de veiligheidsaudits moet in overeenstemming zijn met "2.7 – Controle op de naleving van de voorschriften".

4.5.1. SOORTEN OPGESLAGEN GEGEVENS

De CA's en de PKI@BNPPF RA's van Isabel registreren alle gebeurtenissen in verband met een PKI@BNPPF Certificate in controlelogbestanden. Deze bestanden worden gedurende tien jaar bewaard, met name om in het kader van gerechtelijke procedures over bewijsmateriaal te beschikken met betrekking tot de uitgifte of de intrekking van certificaten. Zie ook ref. [2] in punt 9.2 – Bijlage B – Referentiedocumenten voor de in de Belgische nationale wetgeving vastgestelde voorschriften betreffende de registratie van gebeurtenissen.

De gebeurtenissen die worden geregistreerd hebben een aanzienlijke invloed op de CA-omgeving en het beheer van de Keys en de certificaten. Het betreft met name:

- alle gebeurtenissen die verband houden met de levenscyclus van CA Keys;
- alle gebeurtenissen in verband met de levenscyclus van PKI@BNPPF Certificates;
- alle gebeurtenissen in verband met de voorbereiding van een PKI@BNPPF Secure Signing Card;
- alle verzoeken en verslagen in verband met de intrekking van certificaten en de uiteindelijke actie die wordt ondernomen.

Een Isabel CA garandeert dat alle registratiegerelateerde gebeurtenissen, inclusief aanvragen voor PKI@BNPPF Certificates, zoals aanvragen voor de toewijzing van een nieuw sleutelpaar of de verlenging van een certificaat, worden geregistreerd, met name:

- documenten die de PKI@BNPPF Certificate Subscriber aan de PKI@BNPPF RA verstrekt in het kader van de registratie overeenkomstig de overeenkomst tussen de PKI@BNPPF RA en de BNP Paribas Fortis Customer;
- de opslaglocatie van kopieën van identificatiedocumenten, inclusief de ondertekende PKI@BNPPF Certificate-aanvraag;
- eventuele specifieke keuzes in de aanvraag van de Subscriber;
- de identiteit van de BNP Paribas Fortis Customer die de PKI@BNPPF Certificate-aanvraag aanvaardt;
- de methode die wordt gebruikt om identificatiedocumenten te valideren, indien van toepassing;
- de naam van de ontvangende CA en/of de indienende RA, indien van toepassing.

De details van de gebeurtenissen en de bij te houden gegevens worden gedocumenteerd volgens de interne procedures van Isabel.

4.5.2. REGELMAAT VAN DE LOGBESTANDENCONTROLE

Bevoegde medewerkers van de Isabel CA's nemen de controlelogbestanden geregeld door, met een minimum van één keer per week.

4.5.3. BEWAARTERMIJN VAN CONTROLELOGBESTANDEN

Alle informatie met betrekking tot PKI@BNPPF Certificates wordt gedurende 10 jaar bijgehouden.

4.5.4. BESCHERMING VAN CONTROLELOGBESTANDEN

De geheimhouding en integriteit van de actuele en de gearchiveerde gebeurtenissen met betrekking tot PKI@BNPPF Certificates moeten worden gegarandeerd.

4.5.5. PROCEDURES VOOR HET MAKEN VAN BACK-UPS VAN DE CONTROLELOGBESTANDEN

Isabel zorgt ervoor dat geregeld back-ups worden gemaakt van de controlelogbestanden.

4.5.6. SYSTEEM VOOR HET VERZAMELEN VAN DE CONTROLELOGBESTANDEN (INTERN VS. EXTERN)

Het systeem voor het verzamelen van de controlelogbestanden is ingebouwd in het systeem van de Isabel CA en BNP Paribas Fortis.

4.5.7. KENNISGEVING AAN SUBJECTS DIE DE OORZAAK ZIJN VAN EEN GEBEURTENIS

Geen bepalingen.

4.5.8. KWETSBAARHEIDSONDERZOEK

De beveiliging van de systemen van de Isabel CA's en BNP Paribas Fortis wordt geregeld aan controles onderworpen, die worden uitgevoerd volgens het interne beleid van het systeem van de Isabel CA's.

4.6. GEGEVENSARCHIVERING

4.6.1. GEREGISTREERDE GEBEURTENISTYPES

De volgende elementen worden gearchiveerd:

- PKI@BNPPF CertificatePKI@BNPPF RA's;
- de Certificate Revocation List van Isabel;
- PKI@BNPPF Certificate Policy
- alle gebeurtenissen en verzoeken die leiden tot veranderingen in PKI@BNPPF Certificates en de Certificate Revocation List.

4.6.2. BEWAARTERMIJN VOOR HET ARCHIEF

Alle informatie met betrekking tot PKI@BNPPF Certificates wordt gedurende 10 jaar bijgehouden.

4.6.3. BESCHERMING VAN HET ARCHIEF

Elektronische en papieren archieven worden beschermd met fysieke en logische toegangscontrolemechanismen om de toegang door onbevoegden te voorkomen. De archieven worden beschermd tegen gevaren uit de omgeving, zoals temperatuur, brand, overstromingen, vocht en magnetisme.

4.6.4. BACK-UPPROCEDURES VOOR HET ARCHIEF

Er bestaande meerdere kopieën van het archief om de beschikbaarheid ervan te garanderen.

Het archief wordt geregeld overgezet naar dragers van de jongste generatie om te garanderen dat de bewaartermijn wordt nageleefd en om verouderde dragers te vermijden.

4.6.5. VOORSCHRIFTEN BETREFFENDE HET AANBRENGEN VAN TIJDSTEMPELS OP TE ARCHIVEREN INFORMATIE

Te archiveren informatie wordt digitaal ondertekend en krijgt een tijdstempel.

4.6.6. ARCHIEFVERZAMELSYSTEEM (INTERN OF EXTERN)

Het archiefverzamelsysteem is ingebouwd in het systeem van de Isabel CA's.

4.6.7. PROCEDURES OM INFORMATIE UIT HET ARCHIEF OP TE VRAGEN EN TE CONTROLEREN

Een PKI@BNPPF Certificate Subject heeft toegang tot gearchiveerde informatie die op hem betrekking heeft, zonder dat daardoor de algemene geheimhoudingsplicht van de CA en de PKI@BNPPF RA's van Isabel wordt geschonden. Alle verzoeken om informatie uit het archief moeten schriftelijk aan de Security Manager van BNP Paribas Fortis worden bezorgd.

De informatie in het archief moet geregeld worden gecontroleerd om ervoor te zorgen dat die beschikbaar blijft tijdens de bewaartermijn.

4.7. OVERGANG NAAR EEN NIEUWE SLEUTEL

De Isabel CA's ziet erop toe dat hun Private Keys niet worden gebruikt nadat zij zijn vervallen. Wanneer Private Keys van Isabel CA's vervallen, wordt het daarbij horende certificaat ingetrokken.

4.8. HERSTEL NA COMPROMITTERING EN RAMPEN

De Isabel CA heeft een beleid en procedures vastgesteld om in geval van een ramp, inclusief de compromittering van de Private Key van een CA, de dienstverlening zo snel mogelijk te herstellen.

Geen verdere bepalingen.

4.9. STOPZETTING VAN EEN CA OF RA

Wanneer een CA om welke reden dan ook wordt opgeheven, deelt Isabel dit tijdig mee. Isabel ziet tevens toe op de overdracht van alle verantwoordelijkheden naar de opvolger van de CA en op de instandhouding van de gegevens en voorziet met de instemming van BNP Paribas Fortis in de voortzetting van alle activiteiten in verband met PKI@BNPPF Certificates.

Wanneer de activiteiten van een Isabel CA worden stopgezet, handelt Isabel overeenkomstig de Belgische wetgeving. Zie ref. [2] in punt 9.2 – Bijlage B – Referentiedocumenten.

Indien een PKI@BNPPF RA wordt opgedoekt, meldt BNP Paribas Fortis dit tijdig aan de Isabel CA.

5. FYSIEKE, PROCEDURELE EN PERSOONLIJKE VEILIGHEIDSMAATREGELEN

5.1. FYSIEKE MAATREGELEN

Geen bepalingen.

5.2. PROCEDURELE MAATREGELEN

5.2.1. VERTROUWDE ROLLEN

De Isabel CA's eisen dat de in de volgende punten omschreven rollen worden waargenomen door vertrouwd personeel.

5.2.1.1. CA OPERATOR

Deze personen treden op als beheerders van het CA-systeem van Isabel en gebruiken daartoe het CA-werkstation onder dubbele controle. Er zijn twee groepen CA Operators.

5.2.1.2. CA SYSTEM ADMINISTRATORS

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

5.2.1.3. CA SECURITY OFFICERS

Deze personen voeren het CA-beleid uit, zien toe op de naleving van de PKI@BNPPF CP en controleren de controlelogbestanden.

5.2.2. VEREIST AANTAL PERSONEN PER TAAK

Geen bepalingen.

5.2.3. IDENTIFICATIE EN AUTHENTICATIE VOOR ELKE ROL

Vertegenwoordigers van elke vertrouwde rol worden geauthenticeerd met een digitale handtekening die zij genereren met de Private Key die op hun smartcard is opgeslagen.

5.3. MAATREGELEN TEN AANZIEN VAN HET PERSONEEL

Er moeten maatregelen ten aanzien van het personeel worden getroffen overeenkomstig het beleid van Isabel en het interne beleid van BNP Paribas Fortis.

6. TECHNISCHE VEILIGHEIDSMAATREGELEN

6.1. GENEREREN EN INSTALLEREN VAN SLEUTELPAREN

De Isabel CA's gebruiken passende encryptieapparaten voor het sleutelbeheer van de CA. Die encryptieapparaten worden Hardware Security Modules (HSM's) genoemd.

Dergelijke apparaten voldoen aan formele eisen, die onder meer garanderen dat geknoei met de apparatuur meteen wordt opgemerkt en dat Private Keys het apparaat nooit onversleuteld kunnen verlaten. Hardware- en softwaremechanismen die de Private Keys van CA's beschermen, zijn gedocumenteerd.

6.1.1. GENEREREN VAN SLEUTELPAREN

Een Isabel CA genereert haar eigen Private Key(s) op een veilige manier en beschermt die met behulp van een betrouwbaar systeem. Zij neemt voorts de nodige voorzorgsmaatregelen om te voorkomen dat de sleutels gecompromitteerd worden of ongeoorloofd worden gebruikt.

Het sleutelpaar van het BNP Paribas Fortis Subject wordt centraal gegenereerd door de Isabel CA, met behulp van een betrouwbaar systeem en volgens een gedocumenteerde procedure.

De Isabel CA moet de uniciteit van elk sleutelpaar binnen de PKI garanderen.

6.1.2. LEVERING VAN DE PRIVATE KEY AAN EEN ENTITEIT

Isabel CA bezorgt de Private Key van een BNP Paribas Fortis Subject, opgeslagen op een PKI@BNPPF Secure Signing Card, aan de plaatselijke PKI@BNPPF RA-zetel van de PKI@BNPPF Certificate Subscriber.

Het Isabel CA bezorgt de activeringsgegevens van de PKI@BNPPF Secure Signing Card op een veilige manier rechtstreeks aan het Subject indien het een natuurlijke persoon betreft en aan de Subscriber indien het Subject een functie is.

De PKI@BNPPF Secure Signing Card en de daarbij horende pincode mogen zich *nooit* op hetzelfde moment op dezelfde plaats bevinden, tenzij na afhaling van de PKI@BNPPF Secure Signing Card door de BNP Paribas Fortis Subscriber.

6.1.3. LEVERING VAN DE PUBLIC KEY AAN DE EMITTENT VAN HET CERTIFICAAT

BNP Paribas Fortis Sleutelparen van Subjects worden centraal gegenereerd met een "Key Generator", die werkt op basis van een betrouwbaar systeem. De Public Key wordt via een elektronisch bericht aan de CA geleverd, waarbij wordt toegezien op de integriteit en de herkomst (dit gebeurt intern bij de Isabel CA).

6.1.4. LEVERING VAN DE PUBLIC KEY VAN DE CA AAN GEBRUIKERS

De Public Key van de Isabel CA wordt in de Isabel Repository gepubliceerd. Entiteiten kunnen dit repository de klok rond en 7 dagen per week raadplegen, zij het uitsluitend in "alleen lezen"-modus.

6.1.5. SLEUTELOMVANG

Public Keys (n-modulus) die gecertifieerd zijn door een PKI@BNPPF Certificate en gekoppeld zijn aan een PKI@BNPPF Secure Signing Card moeten ten minste 1024 bits tellen.

De sleutels van de Isabel CA moeten ten minste 2048 bits tellen.

6.1.6. PARAMETERS VOOR HET GENEREREN VAN PUBLIC KEYS

Het proces voor het genereren van Isabel-sleutels is eigendom van Isabel.

De kwaliteit van het genereringsproces is gecontroleerd.

De kwaliteit van de parameters van het genereringsproces wordt continu opgevolgd.

6.1.7. CONTROLE VAN DE PARAMETERKWALITEIT

De Isabel CA controleert de generering van sleutels met behulp van een hardwareonderdeel.

6.1.8. HARDWARE/SOFTWARE VOOR HET GENEREREN VAN SLEUTELS

De Isabel CA gebruikt voor het genereren van sleutels een hardwareonderdeel dat een hoog veiligheidsniveau garandeert dat minstens even hoog is als dat van de PKI@BNPPF Secure Signing Card waarop de gegenereerde Private Key wordt opgeslagen.

6.1.9. GEBRUIKSDOELEN VAN DE SLEUTELS (VOLGENS HET KEYUSAGE-VELD IN VERSIE 3 VAN NORM X.509)

Het gebruik van de certificaten door de eindentiteiten is beperkt door het gebruik van certificaatextensies voor het gebruik en het uitgebreide gebruik van sleutels. Elk gebruik van een certificaat dat niet in overeenstemming is met die extensies, is niet toegelaten.

6.2. BESCHERMING VAN DE PRIVATE KEYS

Isabel moedigt het gebruik van veilige apparaten en manipulatieveilige uitrusting aan om certificaten op een veilige manier uit te geven, te beheren en op te slaan. Isabel gebruikt betrouwbare apparatuur met een goede reputatie om te voorkomen dat haar Private Key wordt gecompromitteerd.

6.2.1. NORMEN VOOR DE ENCRYPTIEMODULE

De Private Key van een Subject wordt opgeslagen op een PKI@BNPPF Secure Signing Card, die een EAL-score van 4+ heeft.

6.2.2. CONTROLE PRIVATE KEY (N VAN M) DOOR MEERDERE PERSONEN

De Private Keys van de CA's staan onder een drievoudige controle.

BNP Paribas FortisPrivate Keys van Subscribers moeten uitsluitend worden gecontroleerd door de BNP Paribas Fortis Subscribers.

6.2.3. INBEWAARGEVING VAN PRIVATE KEYS

De Private Keys van de Isabel CA's worden niet aan derden in bewaring gegeven.

BNP Paribas Fortis De Private Keys van de Subscribers worden niet aan derden in bewaring gegeven.

6.2.4. BACK-UP VAN PRIVATE KEYS

Er wordt een back-up gemaakt van de Private Keys van de Isabel CA's.

BNP Paribas Fortis Er hoeft geen back-up te worden gemaakt van de Private Keys van de Subscribers.

6.2.5. ARCHIVERING VAN PRIVATE KEYS

BNP Paribas Fortis De Private Keys van de Subscribers worden niet gearchiveerd.

6.2.6. INVOER VAN DE PRIVATE KEYS IN DE ENCRYPTIEMODULE

De Private Keys van de Isabel CA's worden op een veilige manier in de encryptiemodule ingevoerd.

6.2.7. METHODE VOOR DE ACTIVERING VAN PRIVATE KEYS

De Private Keys van de Isabel CA's zijn beschermd door een pincode en een wachtwoord.

6.2.8. METHODE VOOR DE DEACTIVERING VAN PRIVATE KEYS

De Private Keys van de Isabel CA's worden gedeactiveerd door de apparatuur uit te schakelen.

BNP Paribas Fortis Private Keys worden gedeactiveerd wanneer de PKI@BNPPF Secure Signing Card uit de smartcardlezer wordt verwijderd.

6.2.9. METHODE VOOR HET VERNIETIGEN VAN PRIVATE KEYS

Een Private Key van een Isabel CA wordt op een veilige manier vernietigd wanneer de sleutel niet langer door de Isabel CA gebruikt wordt.

BNP Paribas Fortis Private Keys van Subscribers worden vernietigd wanneer de PKI@BNPPF Secure Signing Card wordt vernietigd.

6.3. ANDERE ASPECTEN VAN HET BEHEER VAN DE SLEUTELPAREN

6.3.1. ARCHIVERING VAN PUBLIC KEYS

PKI@BNPPF Certificates en bijgevolg ook de Public Key waaraan zij gekoppeld zijn, moeten gedurende minstens 10 jaar in het archief worden bewaard.

6.3.2. GEBRUIKSTERMIJN VOOR PUBLIC EN PRIVATE KEYS

Geen bepalingen.

6.4. ACTIVERINGSGEGEVENS

De activeringsgegevens voor het BNP Paribas Fortis Subject, met name een initiële pincode voor de PKI@BNPPF Secure Signing Card, worden centraal gegenereerd door de Isabel CA. De Isabel CA garandeert dat de initiële pincode op een veilige manier wordt doorgegeven aan de BNP Paribas Fortis Subscriber. Na de levering ervan is het de verantwoordelijkheid van het Subject zijn/haar pincode geheim te houden. Isabel neemt geen back-up van de initiële pincodes van Subjects, geeft die niet in bewaring en neemt ze niet op in het archief.

6.4.1. GENEREREN EN INSTALLEREN VAN DE ACTIVERINGSGEGEVENS

BNP Paribas Fortis De initiële pincode van de Subjects wordt op een veilige manier gegenereerd en aan de Subjects bezorgd. De Private Key, m.a.w. de PKI@BNPPF Secure Signing Card, en de initiële pincode mogen zich nooit op hetzelfde moment op dezelfde plaats bevinden, tenzij na afhaling door de BNP Paribas Fortis Customer.

Tijdens de installatie wordt de BNP Paribas Fortis Subscriber gevraagd de door de Isabel CA toegewezen oorspronkelijke pincode te vervangen door een persoonlijke pincode.

6.4.2. BESCHERMING VAN DE ACTIVERINGSGEGEVENS

De geheimhouding en integriteit van de pincode wordt gewaarborgd tot zij wordt geleverd aan en aanvaard door de PKI@BNPPF Certificate Subscriber.

6.4.3. ANDERE ASPECTEN VAN DE ACTIVERINGSGEGEVENS

Geen bepalingen.

6.5. CONTROLE VAN DE COMPUTERBEVEILIGING

De beveiliging van computers wordt gecontroleerd overeenkomstig het interne beleid van Isabel voor de Isabel CA en dat van BNP Paribas Fortis voor de PKI@BNPPF RA's.

6.6. TECHNISCHE CONTROLEMAATREGELEN IN DE LEVENSCYCLUS

De technische controlemaatregelen in de levenscyclus worden ten uitvoer gelegd overeenkomstig het interne beleid van Isabel voor de Isabel CA en dat van BNP Paribas Fortis voor de PKI@BNPPF RA's.

6.7. NETWERKBEVEILIGINGSMAATREGELEN

De netwerkbeveiligingsmaatregelen worden ten uitvoer gelegd overeenkomstig het interne beleid van Isabel voor de Isabel CA en dat van BNP Paribas Fortis voor de PKI@BNPPF RA's.

6.8. TECHNISCHE VEILIGHEIDSMAATREGELEN VOOR DE ENCRYPTIEMODULE

Geen bepalingen.

7. Certificaat-, CRL- en OCSP-profielen

7.1. CERTIFICAATPROFIELEN

Een voor een Subject (natuurlijke persoon of functie) uitgegeven PKI@BNPPF Certificate heeft het volgende profiel:

Certificaatveld	Waarde of structuur van de waarde
Versie	GEHEEL GETAL {V3(2)} (Opmerking: het gehele getal 2 stemt overeen met v3-certificaten)
SerialNumber	GEHEEL GETAL {0..MAX} Het cijfer is opgebouwd als yyyydddnnnnn, waarbij: • yyyy staat voor het jaar waarin het certificaat is uitgegeven; • ddd staat voor de dag van het jaar; • nnnnn een volgnummer voor die dag is.
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*
Validity	*notBefore*=UTCTime *notAfter*=UTCTime
subject (Normal)	• verplicht veld: CN= <Familienaam>+<Voornaam>, voor natuurlijke personen <Functienaam>, voor functies • verplicht veld OU = <Gebruikersidentificatie> • verplicht veld: OU= <Technische identificatie van de Subscribing Entity> • verplicht veld: OU= <ISO-landencode van de Subscribing Entity>+<Ondernemingsnummer van de Subscribing Entity> • verplicht veld: O= <Naam van de Subscribing Entity> • L= Isabel • C=BE
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption* *OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1}*

7.1.1. VERSIENUMMER

Alle door Isabel Certification Authorities geleverde PKI@BNPPF Certificates moeten voldoen aan versie 3 van de norm X.509 van het ITU-T. Zie ref. [3] in het punt "9.2 – Bijlage B – Referentiedocumenten" van deze PKI@BNPPF CP.

7.1.2. CERTIFICAATEXTENSIES

De voor X.509v3-certificaten gedefinieerde extensies zijn een methode om aanvullende attributen te koppelen aan gebruikers of Public Keys en de certificatenhiërarchie te beheren. Dit veld mag enkel verschijnen indien het versie 3-certificaten betreft. Dit veld is een opeenvolging van een of meer certificaatextensies.

Een toepassing MOET het certificaat weigeren indien een essentiële extensie wordt aangetroffen die niet wordt herkend. Niet-essentiële extensies mogen echter worden genegeerd indien zij niet worden herkend.

Hieronder wordt een lijst gegeven van de standaardextensies van certificaten (als gedefinieerd in norm X.509 van het ITU-T) die gebruikt worden in Isabel Certificates die geleverd worden door een Isabel Certification Authority, alsook een beschrijving van de manier waarop zij worden gebruikt, inclusief de vermelding of de extensies essentieel dan wel niet-essentieel zijn.

Voor een meer volledige beschrijving van de certificaatextensies wordt verwezen naar norm X.509v3 van het ITU-T.

De onderstaande tabel geeft een overzicht van de VERPLICHTE extensies en hun waarde voor een PKI@BNPPF Certificate dat is afgeleverd aan een natuurlijke persoon of een functie:

Certificaatextensieveld	Essentieel?	Waarde of structuur van de waarde
authorityKeyIdentifier	Nee	Dit veld geeft aan welke Public Key van een CA moet worden gebruikt om de handtekening op de certificaten te controleren. OCTET STRING ::= {4341 3032} ("CA02")
subjectPublicKeyInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8.1}	Nee	Dit veld is een eigen extensie van Isabel. *Uitsluitend voor intern gebruik*
subjectContractInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8.2}	Nee	Dit veld specificeert het type contract tussen Isabel en BNP Paribas Fortis: "PKI@BNPPF" *Uitsluitend voor intern gebruik*
SerialNumber (OID 2.5.4.5)	Nee	Dit veld bevat de identifier (CardID) van de PKI@BNPPF Secure Signing Card.
KeyUsage	Nee	Dit veld bevat een lijst van de voor de sleutel toegelaten gebruiksdoelen. BIT STRING ::= {digitalSignature(0), nonRepudiation(1), keyEncipherment(2), dataEncipherment(3)}

Certificaatextensieveld	Essentieel?	Waarde of structuur van de waarde
CertificatePolicies	Nee	Dit veld bevat een reeks van een of meer beleidsinformatietermen, die elk bestaan uit een object identifier (OID) en facultatieve qualifiers. Deze beleidsinformatietermen geven aan op grond van welk beleid het certificaat is uitgegeven, alsmede de doeleinden waarvoor het certificaat mag worden gebruikt. Bevat de waarde {joint-iso-ccitt(2) allocation per country (16) Belgium (56) Isabel (1) certification-policies(9) policy-specification(…)}, die geldt voor deze PKI@BNPPF CP: 2.16.56.1.9.48.1.1 Het veld bevat ook een attribuut dat een URI is voor de volledige versie van de PKI@BNPPF CP en verwijst naar de website voor Easy Banking Business
ExtKeyUsage	Nee	Dit veld geeft aan welke aanvullende gebruiksdoelen voor de sleutel zijn toegelaten. Het betreft een lijst van OID's. KeyPurposeID ::= {id-kp-clientAuth, id-kp-emailProtection}
AuthorityInfoAccess	Nee	Dit veld verwijst naar een onlinedienst voor de controle van de geldigheid (intrekkingsstatus) van het certificaat. De waarde is: https://pki.isabel.be/ocsp

7.1.3. ALGORITHM OBJECT IDENTIFIERS

sha-1WithRSAEncryption
OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(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
PKI@BNPPF Certificate Subjects;	*Zie hierboven.*
Isabel Certification Authority	*CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE*

In het PKI@BNPPF Certificate opgenomen e-mailadressen en namen kunnen niet worden beschouwd als een identificatie-element op basis waarvan het PKI@BNPPF Certificate wordt uitgegeven.

7.1.5. NAAMBEPERKINGEN

Er wordt geen Name Constraint-extensie in de PKI@BNPPF Certificates gebruikt.

7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIER

Zie punt 1.2 – Identificatie van deze PKI@BNPPF Certificate Policy.

7.1.7. GEBRUIK VAN DE POLICY CONSTRAINTS-EXTENSIE

De Policy Constraint-extensie wordt niet in de PKI@BNPPF Certificates gebruikt.

7.1.8. SYNTACTISCHE EN SEMANTISCHE KENMERKEN VAN POLICY QUALIFIERS

Er wordt een policy qualifier gedefinieerd voor de in de Certificate Policy-extensie gedefinieerde Certificate Policy.

Deze qualifier is een URI voor de volledige versie van de PKI@BNPPF CP en verwijst naar de website Easy Banking Business van BNP Paribas Fortis.

7.1.9. VERWERKING VAN DE SEMANTISCHE KENMERKEN VOOR DE ESSENTIËLE CERTIFICATE POLICY-EXTENSIE

De Certificate Policy-extensie is aangemerkt als niet-essentieel. Zie 7.1.2.

7.2. CRL-PROFIEL

Ten behoeve van BNP Paribas Fortis wordt de CRL intern gehouden. BNP Paribas Fortis Customers kunnen valideringsinformatie bij voorkeur bekomen met behulp van het OCSP.

7.3. OCSP-PROFIEL

De Isabel CA legt in een intern technisch document vast welk OCSP-profiel zij gebruikt. De Isabel CA beslist naar eigen goeddunken of dat document al dan niet openbaar wordt gemaakt.

8. SPECIFICATIEBEHEER

8.1. PROCEDURES VOOR DE WIJZIGING VAN SPECIFICATIES

Opmerkingen, vragen en wijzigingsverzoeken met betrekking tot deze PKI@BNPPF CP dienen te worden gericht aan de Policy Authority die wordt genoemd in punt "1.3.7 – Contactgegevens" van deze PKI@BNPPF CP.

BNP Paribas FortisBNP Paribas Fortis kan deze PKI@BNPPF CP op elk moment wijzigen.

8.2. PUBLICATIE- EN KENNISGEVINGSBELEID

Deze PKI@BNPPF Certificate Policy valt onder het rechtstreekse toezicht van de Policy Authority. Zie "1.3.5 – Policy Authorities". Het hoger management van BNP Paribas Fortis verbindt zich ertoe ervoor te zorgen dat de in deze PKI@BNPPF CP beschreven praktijken correct ten uitvoer worden gelegd.

De Policy Authority herziet deze PKI@BNPPF Certificate Policy geregeld, teneinde rekening te houden met veranderingen in de omstandigheden, de wetgeving, de technologische stand van zaken en veiligheidsrisico's.

De Policy Authority formuleert aanbevelingen tot wijziging van deze PKI@BNPPF Certificate Policy, die het voorwerp uitmaken van een raadplegingsprocedure binnen BNP Paribas Fortis en moeten worden goedgekeurd door de General Manager "Multichannel Banking" alvorens enige wijzigingen ten uitvoer worden gelegd.

Deze PKI@BNPPF Certificate Policy en de latere versies ervan worden gepubliceerd op de website Easy Banking Business van BNP Paribas Fortis.De publicatiedatum, de datum van inwerkingtreding en het versienummer worden vermeld op de titelpagina van deze PKI@BNPPF Certificate Policy. De versie die gepubliceerd wordt op deze URL is de enige geldige versie zolang zij op die locatie te vinden is.

Kennisgevingen in verband met deze PKI@BNPPF Certificate Policy worden eveneens op de bovenstaande URI gepubliceerd.

Het verdere gebruik van een PKI@BNPPF Certificate na de publicatie van een nieuwe versie van de PKI@BNPPF Certificate Policy houdt in dat het Subject de nieuwe versie aanvaardt.

De nieuwste versie van deze PKI@BNPPF CP is online beschikbaar. Oudere versies worden door BNP Paribas Fortis gearchiveerd.

8.3. PKI@BNPPF CERTIFICATE POLICY GOEDKEURINGSPROCEDURES VOOR DE PKI@BNPPF CERTIFICATE POLICY

De Policy Authority van deze PKI@BNPPF Certificate Policy en de General Manager "Multichannel Banking" moeten dit document goedkeuren.

9. Bijlagen

9.1. BIJLAGE A – DEFINITIES

9.1.1. ACRONIEMEN

Acroniem	Beschrijving
CA	Certification Authority (certificeringsautoriteit)
CP	Certificate Policy (certificeringsbeleid)
CPS	Certification Practice Statement (certificeringspraktijkverklaring)
CRL	Certificate Revocation List (lijst met ingetrokken certificaten)
HSM	Hardware Security Module (veiligheidsmodule (hardware))
OCSP	Online Certificate Status Protocol (online-certificaatstatusprotocol)
OID	Object Identifier (objectidentificatiecode)
PIN	Personal Identification Number (persoonlijk identificatienr.)
PKI	Public Key Infrastructure (openbare sleutelinfrastructuur)
RA	Registration Authority (registratie-autoriteit)
URI	Uniform Resource Identifier (eenvormige bronidentificatiecode)
URL	Uniform Resource Locator (eenvormige bronlocator)

9.1.2. VERKLARENDE WOORDENLIJST

Term	Beschrijving
Activeringsgegevens	Alle gegevens die worden gebruikt om de Private Key, zoals het wachtwoord, de pincode enz. te beschermen. De activeringsgegevens van PKI@BNPPF Certificates omvatten een tijdelijke pincode, die naar de Subscriber wordt gezonden bij de aanmaak van zijn PKI@BNPPF Secure Signing Card en bij het eerste gebruik moet worden gewijzigd.
Authenticatie	Het proces waarbij de identiteit wordt vastgesteld op basis van het bezit van een vertrouwd legitimatiebewijs.
BNP Paribas Fortis	Fortis Bank nv, Warandeberg 3, 1000 Brussel – België, RPR Brussel, BTW BE0403.199.702.
PKI@BNPPF Certificate	Een digitaal certificaat dat een Isabel CA heeft afgegeven aan een PKI@BNPPF Certificate Subscriber.
PKI@BNPPF Certificate Relying Parties	Een PKI@BNPPF Certificate Relying Party is een natuurlijke persoon of een functie die een BNP Paribas Fortis Customer is of daartoe behoort en die vertrouwt op de informatie die vervat zit in een PKI@BNPPF Certificate en/of digitale handtekeningen die met dit certificaat worden gecontroleerd en/of enige andere informatie die wordt gepubliceerd door een Isabel CA die PKI@BNPPF Certificates uitgeeft.
PKI@BNPPF Certificate verzoek	Verstrekking van gevalideerde informatie uit een PKI@BNPPF Certificate-aanvraag door een PKI@BNPPF RA aan een Isabel CA met het oog op de uitgifte van een PKI@BNPPF Certificate. PKI@BNPPF Certificate
PKI@BNPPF Certificate Subjects;	Een natuurlijke persoon of een functie (bv. boekhouder) die in een certificaat wordt geïdentificeerd als de houder van de Private Key die gekoppeld is aan de in het certificaat gegeven Public Key. Het PKI@BNPPF Certificate Subject heeft een PKI@BNPPF Certificate ontvangen binnen de grenzen van zijn/haar activiteiten en ontcijfert en/of plaatst handtekeningen met de Private Key die gekoppeld is aan dat PKI@BNPPF Certificate in naam van de BNP Paribas Fortis Customer tot wie hij/zij behoort. Een PKI@BNPPF Certificate Subject wordt vertegenwoordigd door: - in geval van een Physical Person Subject: de natuurlijke persoon van wie de identiteit in het certificaat is opgenomen; - in geval van een Function Subject: een natuurlijke persoon die gemachtigd is om de functie de vertegenwoordigen die in het certificaat is vermeld (functievertegenwoordiger).
PKI@BNPPF Certificate Subscriber	Een natuurlijke persoon die door een BNP Paribas Fortis Customer gemachtigd is om een PKI@BNPPF Certificate aan te vragen in naam van een of meer natuurlijke personen of functies.
BNP Paribas Fortis Customer	Een entiteit die een BNP Paribas Fortis-contract met BNP Paribas Fortis heeft ondertekend teneinde diensten en/of producten van BNP Paribas Fortis te ontvangen.
PKI@BNPPF RA	Zie PKI@BNPPF Registration Authority.
PKI@BNPPF Registration Authority	RA's worden aangesteld door BNP Paribas Fortis en werken onder het gezag en het toezicht van een Isabel CA voor PKI@BNPPF Certificates.

Term	Beschrijving
PKI@BNPPF Secure Signing Card	Een smartcard waarop de Private Key van een Subject is opgeslagen en die door dit Subject gebruikt wordt om digitale handtekeningen te plaatsen. De digitale handtekeningen worden gegenereerd in de PKI@BNPPF Secure Signing Card.
Certificate Policy	Een bepaalde reeks voorschriften die de geldigheid aangeven van een certificaat voor een bepaalde gemeenschap en/of categorie toepassingen met gemeenschappelijke veiligheidsvereisten.
Certificate Revocation List	Een lijst met nummers van ingetrokken certificaten die digitaal is ondertekend door de uitgevende CA.
Certification Authority	Een autoriteit die het vertrouwen van de gebruikers geniet voor de uitgifte en het beheer van certificaten. De CA kan eventueel het sleutelpaar van de gebruikers genereren.
Certification Practice Statement	Een verklaring over de praktijken volgens welke een CA certificaten uitgeeft.
Digitaal certificaat	Een digitaal certificaat is de Public Key van een Subject, de identiteit van het Subject en enkele andere gegevens, die niet-namaakbaar zijn gemaakt door encryptie met de Private Key van de CA die het certificaat heeft uitgegeven.
Isabel Certification Authority	Een door Isabel beheerde CA. De term Isabel CA verwijst ook naar de technische organisatie rond de Certification Authority, die wordt beheerd door de vennootschap Isabel nv.
Isabel	Isabel nv, Keizerinlaan 13-15, 1000 Brussel – België – RPR Brussel, BTW BE0455.530.509.
Isabel Repository	Een entiteit rond de Isabel CA die instaat voor de publicatie van de certificaten en de Certification Revocation List.
Personal Identification Number	Een geheime code (PIN) die gebruikt wordt om te voorkomen dat onbevoegden zich toegang verschaffen tot een Private Key.
Policy Authority	De entiteit die verantwoordelijk is voor het opstellen en valideren van de CP's.
Private Key	Het deel van een openbaar-privaat sleutelpaar dat geheim moet worden gehouden en waarvan enkel het Subject op de hoogte mag zijn.
Public Key	Het deel van en openbaar-privaat sleutelpaar dat openbaar mag zijn of verspreid mag worden zonder de veiligheid van het encryptiesysteem in gevaar te brengen.
Public Key Infrastructure (openbare sleutelinfrastructuur)	Een structuur van hardware, software, mensen, processen en beleidsmaatregelen waarin gebruikgemaakt wordt van digitale-handtekeningentechnologie om een controleerbare band te creëren tussen het openbare deel van een asymmetrische Public Key en een specifiek Subject dat de overeenkomstige Private Key bezit.
Registration Authority	Een entiteit die verantwoordelijk is voor de vaststelling van de identiteit en de authenticatie van Subjects van certificaten, maar geen certificaten ondertekent of uitgeeft. Een RA kan helpen in het aanvraagproces of het intrekkingsproces van certificaten dan wel in beide, overeenkomstig de toepasselijke CP.
PKI@BNPPF Certificate Relying Parties.	Zie PKI@BNPPF Certificate Relying Party.

Term	Beschrijving
Self-Signed Certificate	Certificaat dat is ondertekend met de Private Key waarvoor de Public Key in het certificaat zit. Dit wordt doorgaans gebruikt voor "CA root certificates" (stamcertificaten van de CA), waarbij de Root Key is opgenomen in een certificaat dat is ondertekend met de overeenkomstige Private Key.
PKI@BNPPF Certificate Subjects;	Zie PKI@BNPPF Certificate Subject.
PKI@BNPPF Certificate Subscribers;	Zie PKI@BNPPF Certificate Subscriber.
Validation Authority	Een autoriteit die PKI@BNPPF Certificate Relying Parties de mogelijkheid biedt informatie over de geldigheid (intrekkingsstatus) van PKI@BNPPF Certificates op te vragen.

9.2. BIJLAGE B – REFERENTIEDOCUMENTEN

	Titel	Eigenaar	Datum
[1]	Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.	Europees Parlement en Europese Raad	13 december 1999
[2]	Wet houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische hantekeningen en certificatiediensten	Belgisch Parlement	9 juli 2001
[3]	ITU-T-aanbeveling 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	Internationale Organisatie voor Normalisatie	22 oktober 2002