Certificate Policy BNP Paribas Fortis

Certificate Authority

BNP Paribas Fortis Customer Ephemeral Certification Authority

itg

Herziening		
Naam	Functie	Datum

Goedkeuring		
Naam	Functie	Datum

Follow-up van de versies			
Versie	Datum	Auteur	Aard van de wijzigingen
1.0	07/11/2016	Cédric SZANIEC	Versie goedgekeurd door de PMA

Inhoud

I. Inleiding

I.A. Algemene presentatie

Dit document beschrijft de Certificate Policy van de Certificate Authority 'BNP Paribas Fortis Customer Ephemeral Certification Authority <N>' ('BNPPF Instant CA' in de rest van dit document):

- handelend als Certificate Authority (CA);
- om tegemoet te komen aan de behoeften van business toepassingen die gebruikmaken van de oplossingen van Safran I&S (in het bijzonder de toepassingen om online contracten af te sluiten).

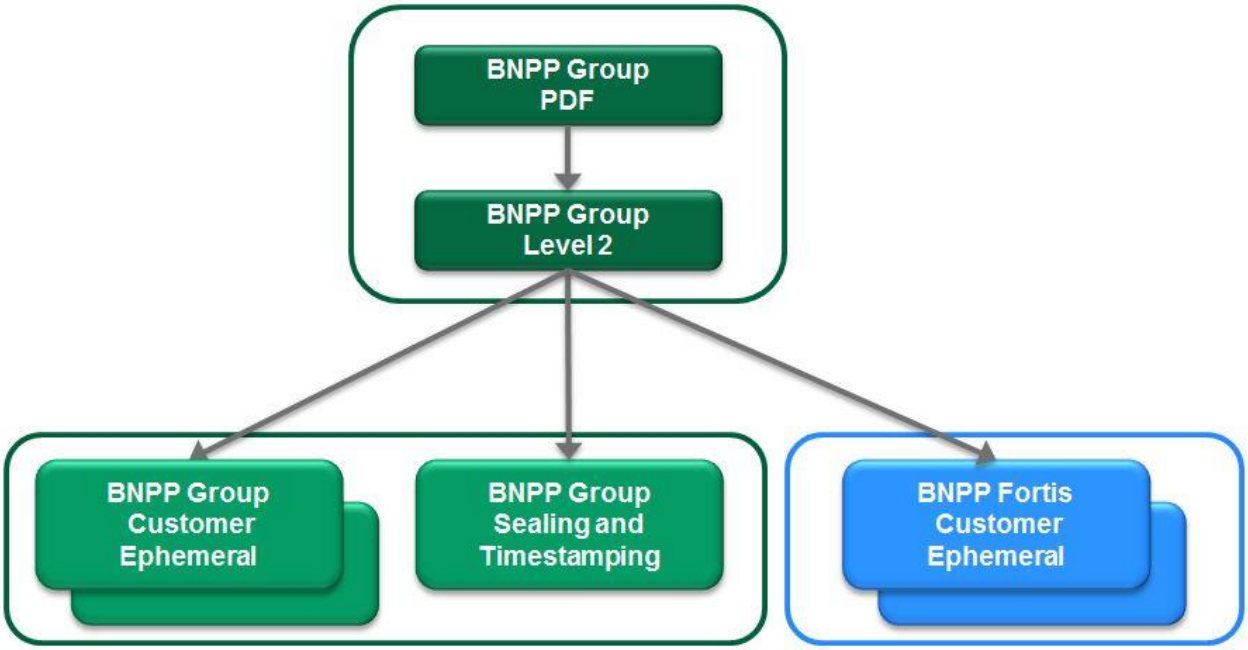
Dit Certificate Policy wordt in de rest van dit document CP genoemd:

- het heeft betrekking op de functies voor het aanbrengen van een elektronische handtekening en een tijdstempel op documenten in het formaat PDF, XML (XAdES, XML-DSig) of CMS;
- de autoriteit 'BNPPF Instant CA' voldoet aan de handtekeningbehoeften van de klanten van de organisatie die gebruikmaken van persoonlijke certificaten.

Dit Certificate Policy past in het kader van een kwalificatieproces ETSI TS 102 042 en geeft een beschrijving van:

- de verbintenissen van de autoriteit 'BNPPF Instant CA' met betrekking tot de uitgifte en het beheer van certificaten die gebruikmaken van de producten van Safran I&S;
- de verbintenissen van de autoriteit 'BNPPF Instant CA' met betrekking tot de definitie van de regels voor de uitgifte van certificaten door BNP Paribas Fortis en de correcte toepassing van die regels;
- de gebruiksvoorwaarden van de certificaten uitgegeven door de CA 'BNPPF Instant CA'.

Dit Certificate Policy voldoet aan de eisen van de 'Lightweight Certificate Policy' (LCP) zoals bepaald in de norm ETSI TS 102 042. Dit is de LCP OID: 0.4.0.2042.1.3.



I.B. Identificatie van het document

Dit Certificate Policy wordt geïdentificeerd aan de hand van zijn Object ID (OID, footer op elke pagina van dit document). Het kan ook worden geïdentificeerd aan de hand van specifiekere elementen zoals de naam, het versienummer en de bijwerkingsdatum.

De OID-nummers voor dit Certificate Policy:

- BNPPF Instant CA nr. 1: 1.2.250.1.62.10.7.1.1.1
- BNPPF Instant CA nr. 2: 1.2.250.1.62.10.8.1.1.1

Neerlegging van de OID-tak van BNP Paribas: {iso(1) member-body(2) fr(250) type-org(1) BNP Paribas(62)} Signel(10) Autoriteiten BNPPF Instant CA(7 of 8) Certificate Policy(1) Certificaatmodel(1) Versie(1)

Geldig voor de certificaten uitgegeven vanaf 29 november 2016.

I.C. Entiteiten die tussenkomen in de PKI

Om de identificatie van de eisen te verduidelijken en te vereenvoudigen en in overeenstemming met de documenten van het ETSI betreffende de functionele uitsplitsing van het CP van 'BNPPF Instant CA' is die autoriteit georganiseerd rond de volgende entiteiten:

- Certificate Authority (CA)
- Operator
- Registratieautoriteit (RA)
- Houders
- Gebruikerstoepassing
- PMA (Policy Management Authority)

Het gebruik zoals bepaald in het CP vereist geen escrowfuncties.

I.C.1. Certificate Authority

De Certificate Authority 'BNPPF Instant CA' is belast met de levering van de diensten voor het beheer van certificaten tijdens hun volledige levenscyclus (aanmaak, verspreiding, vernieuwing, intrekking enz.) en maakt daarvoor gebruik van een public key infrastructure (PKI).

Om de identificatie van de eisen te verduidelijken en te vereenvoudigen volgt hierna een overzicht van de verschillende functies in die PKI, in overeenstemming met de documenten van het ETSI (Europees Telecommunicatie en Standaardisatie Instituut):

- **Functie voor de aanmaak van certificaten** – Deze functie maakt de certificaten aan (aanmaak van het formaat, elektronische handtekening met de bijbehorende private sleutel):
  - ofwel gebruikmakend van de eigen tools van de technische componenten of van de toekomstige certificaathouders;
  - ofwel gebruikmakend van de tools van de eigen PKI.
- **Functie voor de uitgifte aan de houder** – Deze functie overhandigt de houder minstens het certificaat of de certificaatketen.
- **Publicatiefunctie** – Deze functie stelt de verschillende betrokken partijen het volgende ter beschikking: het gepubliceerde beleid, de certificaten van de autoriteit en alle andere relevante informatie voor de houders en/of de gebruikers van certificaten, buiten de informatie over de status van de certificaten.
- **Functie voor het beheer van de intrekkingen** – Deze functie behandelt de intrekkingsaanvragen en bepaalt de vereiste acties. De resultaten van de behandeling worden verspreid via de functie voor informatie over de status van de certificaten.
- **Functie voor informatie over de status van de certificaten** – Deze functie geeft de gebruikers van certificaten informatie over de status van de certificaten (vooral of ze zijn ingetrokken). Deze functie publiceert informatie die in een lijst met ingetrokken certificaten (Certificate Revocation List of CRL) wordt opgenomen.
- **Functie voor het beheer van de PKI** – Deze functie wordt gekoppeld aan de rol die het functionele gedrag en de technische instellingen van de PKI bepaalt.

Technisch gezien bestaat de Certificate Authority 'BNPPF Instant CA' uit twee afzonderlijke PKI-diensten. Ze worden geïdentificeerd met een CN en volgend achtervoegsel:

- CN = BNP Paribas Fortis Customer Ephemeral Certification Authority <N>

  Waarbij <N> gelijk is aan 1 of 2

I.C.2. Certificaat operator

De certificaatoperator levert technische diensten, meer bepaald versleutelings- en hostingdiensten, om aan de eisen van deze policy te voldoen.

De rol van certificaatoperator wordt opgenomen door Safran I&S en is uitvoerig beschreven in de Certificate Practice Statement of CPS van de CA BNPP Fortis.

I.C.3. Registratieautoriteit (RA)

Deze functie controleert de informatie voor de identificatie van de toekomstige certificaathouder, samen met eventuele andere specifieke kenmerken, voordat ze de overeenkomstige aanvraag (aanmaak, intrekking) aan de betrokken functie van de PKI doorgeeft.

De RA heeft de opdracht om de identiteit van de aanvrager van het certificaat te controleren om de aanvraag voor de uitgifte van het certificaat goed te keuren.

Ze moet de procedures voor de identificatie van natuurlijke personen toepassen om certificaten uit te geven volgens een procedure die in overeenstemming is met de Belgische bankregelgeving, en met name de regelgeving ter voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme (wet van 11 januari 1993 ter voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme).

De PKI van de groep BNP Paribas beschikt over twee RA-componenten:

- **een functionele RA:** belast met de controle van de identiteit van de houder en de bewaring van de identiteitsbewijzen die de houder heeft voorgelegd bij zijn relatieopening met de bank en die in de loop van de tijd worden bijgehouden volgens de Belgische bankregelgeving. Het gaat om een commercieel agentschap van BNP Paribas Fortis, dat de identiteitsbewijzen verzamelt. Die documenten worden elektronisch gearchiveerd;
- **een technische RA:** verantwoordelijk voor de aanmaak en de voorlegging van de certificaataanvragen aan de Certificate Authority. Ze maakt ook een bewijsbestand aan (spoor van audit, optioneel metiergegevens van de toepassing van BNP Paribas Fortis, bewijsbestanden voor de goedkeuring van de handtekening) bij elke ondertekening door de houder.

De functionele RA BNP Paribas Fortis heeft de volgende taken:

- de identiteit van de toekomstige certificaathouder controleren:
    - bij de start van het proces om klant van de bank te worden:
        - face to face: de identiteitsgegevens controleren op basis van bewijsstukken overeenkomstig de regelgeving die van toepassing is op de kredietinstellingen:
            - voor een Belgische inwoner wordt gebruikgemaakt van de elektronische identiteitskaart (of eventueel een ander document) uitgegeven door de Belgische overheid;
            - voor een niet-ingezetene wordt gebruikmaakt van de identiteitskaart of eventueel het paspoort uitgegeven door het verblijfland. Er werden speciale processen uitgewerkt voor als er geen identiteitsbewijs voorhanden is;
        - wanneer de identificatiegegevens zijn gecontroleerd, wordt het acceptatieproces om klant van de bank te worden opgestart;
        - na acceptatie van de klant moet de bank de volgende taken verrichten:
            - de klant zijn intelligente bankkaart overhandigen (EMV-standaard);
            - uitgifte van zijn pincode;
            - uitgifte van de UCR met het label van BNP Paribas Fortis;
        - alle bewijzen van identiteitsdocumenten worden bewaard in het bankarchief, dat ter beschikking wordt gesteld van alle bankkantoren;

    - bij de start van het proces dat het mogelijk maakt om online contracten af te sluiten.

De klant kan:

- zich op unieke wijze authenticeren (SMID: klantnummer) als natuurlijke persoon in zijn elektronisch bankkanaal met zijn bankkaart (challenge M1);
- een product/dienst selecteren;
- de overeenkomstige instructies voor de aankoop van het product of de dienst volgen;
- overgaan naar de stap voor de elektronische ondertekening van het product of de dienst;

- bij de start van het proces dat het mogelijk maakt om elektronisch te ondertekenen;
  - de klant toetst de challenge M2 van zijn bankkaart als natuurlijke persoon (SMID) in zijn elektronische bankkanaal in;
  - het banksysteem maakt een certificaat op naam van de klant (voornaam-naam) aan;
  - de klant stemt in met:
    - zijn identificatiegegevens die op het klantcertificaat staan;
    - de aanmaak van een elektronische handtekening op naam van de klant op een specifiek contractueel document (tussen BNP Paribas Fortis en zijn klant);
  - het aangemaakte certificaat wordt gebruikt voor de ondertekening van het document dat de klant op wettelijke wijze met de bank verbindt;
  - de klant kan de GTC's en de CP's raadplegen;
  - de klant kan het proces voor de elektronische handtekening beëindigen door:
    - te klikken op 'annuleren' in plaats van met zijn bankkaart te ondertekenen (machtigingsscherm). Het handtekeningproces wordt geannuleerd en de klant keert terug naar het scherm van het geselecteerde product/de geselecteerde dienst. Er wordt geen certificaat aangemaakt;
    - te klikken op 'annuleren' in plaats van in te stemmen (machtigingsscherm). Het aangemaakte certificaat wordt ingetrokken. De klant keert terug naar het handtekeningscherm;

- de elementen voor de controle van de certificaathouder bewaren in toepassing van de regelgeving die op de kredietinstellingen van toepassing is *(wet van 11 januari 1993 ter voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme);*

- de certificaataanvraag opstellen en doorsturen naar de betrokken functie van de PKI volgens de organisatie van die PKI en de aangeboden diensten;

- de vertrouwelijkheid en de integriteit van de persoonsgegevens voor de authenticatie van de houder vrijwaren in overeenstemming met de bankregelgeving.

  ➔ Alle informatie over de vertrouwelijke gegevens wordt opgeslagen in het bankarchief.

I.C.4. Certificaathouder

In dit Certificate Policy is een certificaathouder een klant van BNP Paribas Fortis.

I.C.5. Toepassingen die gebruikmaken van certificaten

Toepassingen die gebruikmaken van certificaten:

- een door BNP Paribas en Safran I&S contractueel bepaalde toepassing;
- alle software voor de weergave en de goedkeuring van elektronische handtekeningen.

I.D. Gebruik van de certificaten

I.D.1. Sleutelparen en certificaten van de houders

De tijdelijke certificaten die worden uitgegeven in het kader van dit Certificate Policy, worden alleen gebruikt voor oplossingen van Safran I&S met het oog op de elektronische ondertekening en de goedkeuring van documenten in een door BNP Paribas Fortis bepaald formaat.

I.D.2. Sleutelparen en certificaten van de autoriteit 'BNPPF Instant CA'

De certificaten van de autoriteit 'BNPPF Instant CA' zoals bepaald in dit CP worden gebruikt om persoonlijke certificaten met tijdelijke handtekening en CRL's te ondertekenen.

I.E. Beheer van de Certificate Policy

I.E.1. Entiteit die de Certificate Policy beheert

De entiteit die is belast met de administratie en het beheer van dit Certificate Policy is ITP ITG, in samenspraak met BNP Paribas Fortis. Ze is verantwoordelijk voor de uitwerking, de follow-up en de eventuele wijziging van dit CP.

I.E.2. Contactpersoon

Er kan contact worden opgenomen met BNP Paribas Fortis voor alle vragen over dit CP. De klant moet naar het Easy Banking Center (EBC) bellen op het nummer 02 762 60 00 (NL) of 02 762 20 00 (FR).

Er kan contact worden opgenomen met Fintro voor alle vragen over dit CP. De klant moet naar het Easy Banking Fintro (Web en App) bellen op het nummer 02 433 45 10 (NL) of 02 433 45 20 (FR).

Als de klant meent dat het antwoord/de behandeling nog altijd niet toereikend is, kan hij contact opnemen met de afdeling Klachtenmanagement.

I.E.3. Entiteit die bepaalt of een CPS in overeenstemming is met dit Certificate Policy

De PMA (Policy Management Authority), de governance-instantie van de PKI, wijst de personen (of diensten) aan die bepalen of de verklaring met betrekking tot de certificatiepraktijk in overeenstemming is met dit Certificate Policy.

I.E.4. Procedures voor de goedkeuring van de conformiteit van het CP

Dit Certificate Policy zal worden goedgekeurd tijdens een procedure van de PMA (Policy Management Authority), de governance-instantie van deze PKI.

I.F. Definities en afkortingen

In dit CP worden de volgende afkortingen gebruikt:

- **AA** : Autorité d'Archivage
- **AC** : Autorité de Certification
- **ACR** : Autorité de Certification Racine
- **AE** : Autorité d'Enregistrement

- **CAP** : Client Acceptance Procedure
- **CFU** : Customer Follow-up
- **CGU** : Conditions générales d'utilisation
- **CP** : Certificate Policy
- **CPS** : Certificate Practice Statement
- **CRL** : Certificate Revocation List / Liste de Certificats Révoqués
- **DN** : Distinguished Name
- **DPC :** Déclaration des Pratiques de Certification
- **EMV** : Europay/Mastercard/Visa
- **GTC** : General Terms and Conditions
- **IGC** : Infrastructure de Gestion de Clés
- **OID** : Object Identifier
- **PMA** : Policy Management Authority
- **PC** : Politique de Certification
- **RGS** : Référentiel Général de Sécurité
- **RSA** : Rivest Shamir Adleman
- **SMID** : Single Multichannel Identifier
- **UCR** : Unconnected card reader
- **URL** : Uniform Resource Locator

Public Key Infrastructure (PKI)	Geheel van fysieke componenten, procedures en software om de levenscyclus van de certificaten te beheren en authenticatie-, versleutelings- en handtekeningdiensten aan te bieden.
Certificaat	Elektronisch bestand, afgeleverd door een Certificate Authority die de identiteit van een houder (natuurlijke persoon, apparaat enz.) bevestigt. Het certificaat is geldig gedurende een bepaalde periode die erin staat vermeld.
Certificate Authority (CA)	Dienst die is belast met de ondertekening, de uitgifte en het onderhoud van de certificaten van een public key infrastructure, overeenkomstig een Certificate Policy. Softwarediensten voor het beheer van de certificaten uitgegeven door de Certificate Authority van de certificaathouder.
Certificate Policy (CP)	Een reeks regels en eisen die een Certificate Authority moet naleven bij het organiseren en het verstrekken van haar diensten.
Verklaring met betrekking tot de certificatiepraktijk (CPS)	Beschrijving van de praktijken (organisatie, operationele procedures, technische en menselijke middelen) die de Certificate Authority toepast in het kader van het leveren van haar elektronische certificatiediensten, overeenkomstig de Certificate Policy dat zij moet naleven.
Lijst met ingetrokken certificaten (CRL)	Door de Certificate Authority gepubliceerde lijst met de certificaten die niet langer betrouwbaar zijn (ingetrokken, ongeldig enz.). Gemakshalve worden daaraan ook de intrekkingslijsten van autoriteiten (ARL genoemd) gekoppeld.
Sleutelpaar	Sleutelpaar bestaand uit een private en publieke sleutel.
X 509	Norm van de Internationale Telecommunicatie Unie (ITU) over de public key infrastructures (PKI), met onder andere de standaardformaten voor de componenten: elektronische certificaten,

	intrekkingslijsten, validatiealgoritme enz.
UTF-8	Codering van de door Unicode bepaalde tekens, waarbij elk teken wordt gecodeerd op basis van een reeks van een tot zes woorden van acht bits (er bestaan momenteel geen gecodeerde tekens met meer dan vier woorden).
Distinguished Name (DN)	Element voor de unieke identificatie van een certificaathouder of -autoriteit.
Object Identifier (OID)	Universele ID, voorgesteld in de vorm van een reeks gehele getallen, in het kader van een PKI gekoppeld aan een referentie-element, zoals de Certificate Policy of de verklaring met betrekking tot de certificatiepraktijk.

ITP ITG is de functie Informatica en Technologie van de Groep (ITG), opgericht binnen Technologie en Processen (ITP), de functie van BNP Paribas die zich bezighoudt met de informatica, de aankopen, het bedrijfsvastgoed en de veiligheid.

II. Verantwoordelijkheden in verband met de terbeschikkingstelling van de te publiceren informatie

II.A. Entiteiten belast met de terbeschikkingstelling van de informatie

Voor de terbeschikkingstelling van de te publiceren informatie voor de certificaathouders en -gebruikers richt de autoriteit 'BNPPF Instant CA' binnen haar PKI een publicatiefunctie en een functie voor informatie over de status van de certificaten in.

Dit beleid beschrijft de methodes voor de terbeschikkingstelling en de overeenkomstige URL's (publicatiewebservers).

II.B. Te publiceren informatie

De autoriteit 'BNPPF Instant CA' publiceert de volgende informatie voor de certificaathouders en -gebruikers:

- dit Certificate Policy;
- de lijsten met ingetrokken certificaten;
- de geldige certificaten van de autoriteiten 'BNPPF Instant CA';
- de algemene gebruiksvoorwaarden van de tijdelijke certificaten.

II.C. Publicatietermijnen en -frequenties

De publicatietermijnen en -frequenties hangen af van de betrokken informatie:

- informatie over de PKI (nieuwe versie van het CP, algemene gebruiksvoorwaarden) wordt gepubliceerd zodra nodig zodat de gepubliceerde informatie en de effectieve verbintenissen van de CA altijd coherent blijven. Die termijn mag niet langer zijn dan zeven werkdagen;
- voor informatie over de status van de certificaten verwijzen we naar IV.I;
- voor de systemen die deze informatie publiceren, verbinden BNP Paribas en Safran I&S zich ertoe om de volgende beschikbaarheidseisen te vervullen:
    - de systemen garanderen dat de informatie over de PKI (nieuwe versie van het CP, algemene gebruiksvoorwaarden) beschikbaar is op werkdagen, met een maximale onbeschikbaarheid per onderbroken dienst (defect of onderhoud) van acht uur (op werkdagen) en een aanvaarde maximale onbeschikbaarheid van 2 uur en 10 minuten per maand, behalve bij gepland onderhoud en overmacht (aangetoond ernstig veiligheidsincident);
    - de systemen garanderen dat de CA-certificaten en de lijsten met ingetrokken certificaten de klok rond beschikbaar zijn, met een aanvaarde maximale onbeschikbaarheid van 2 uur 10 minuten per maand, behalve voor gepland onderhoud en overmacht (aangetoond ernstig veiligheidsincident).

II.D. Controle op de toegang tot de gepubliceerde informatie

Alle gepubliceerde informatie voor de certificaatgebruikers is vrij toegankelijk om te worden gelezen. De toegang om de informatie te wijzigen in de publicatiesystemen (toevoeging, schrapping, wijziging van de gepubliceerde informatie) is strikt beperkt tot de gemachtigde interne functies van de PKI.

III. Identificatie en authenticatie

III.A. Naamgeving

III.A.1. Type namen

De gebruikte namen zijn in overeenstemming met de specificaties van de norm X.500.

In elk X509 v3-certificaat worden de uitgevende autoriteit (*issuer*) en de houder (*subject*) geïdentificeerd met een '*Distinguished Name*' (DN) van het type X.501, waarvan het exacte formaat wordt beschreven in hoofdstuk VII waarin het profiel van de certificaten wordt beschreven.

III.A.2. Noodzaak om expliciete namen te gebruiken

De gekozen namen om de certificaathouders aan te duiden, moeten expliciet zijn. De DN volgt de structuur van de identiteit die wordt gebruikt in de referentiesystemen van BNP Paribas Fortis en die de bank in haar functie van technische RA meedeelt aan de operator met het oog op de ondertekening van het overeenkomstige certificaat.

De common name (CN) van het subject moet verwijzen naar de identiteit van de ontvanger van wie de identiteit werd gecontroleerd (zie § III.B) en mag in geen geval iets anders voorstellen dan zijn identiteit in verband met zijn burgerlijke staat (geen toestelnaam of identiteit van een andere persoon).

III.A.3. Pseudoniemen van de houders

De certificaten van de houders krijgen geen pseudoniem.

III.A.4. Regels voor de interpretatie van de verschillende naamvormen

De functionele RA is verantwoordelijk voor de uniciteit van de namen van haar houders en de beslechting van geschillen over hun opeising van het gebruik van een naam.

III.A.5. Uniciteit van namen

a) Voor een tijdelijk certificaat

Om de continuïteit te waarborgen van de unieke identificatie van de houder in het domein van de CA 'BNPPF Instant CA' maakt de DN van het veld 'subject' van elk houdercertificaat een unieke identificatie van de overeenkomstige houder in het domein van de CA mogelijk.

De DN moet daarom aan de volgende eisen voldoen:

- Voor Belgische houders:
- CN = identiteit van het subject/de natuurlijke persoon, in de vorm 'voornaam-naam'
- SN = uniek nummer (UUID)
- OU = F+ (SMID van de klant)
- C = BE

b) Voor een certificaat van de Certificate Authority 'BNPPF Instant CA'

Aan de hand van het serienummer dat in het subject van de Certificate Authority is opgenomen, kan de CA die het tijdelijke certificaat heeft uitgegeven, worden geïdentificeerd.

III.A.6. Identificatie, authenticatie en rol van gedeponeerde merken

Het merk BNP Paribas is gedeponeerd door BNP Paribas:

- BNP PARIBAS, Frans merk, gedeponeerd op 3 september 1999 in de klassen 35, 36 en 38 onder het nummer 99810625.
- BNP PARIBAS, gemeenschapsmerk, gedeponeerd op 8 oktober 1999 in de klassen 35, 36 en 38 onder het nummer 1338888.

Het merk BNP Paribas Fortis is een merk dat op 17 februari 2010 door BNP Paribas in de Europese Unie werd gedeponeerd in de klassen 9, 35, 36 en 41 onder het nummer 008373185.

- Het merk werd op 3 januari 2013 gedeponeerd bij het Benelux-Merkenbureau in de klassen 35, 36 en 42 onder het nummer 0931084.

Het merk Fintro is een merk dat op 10 mei 2007 door BNP Paribas Fortis in de Europese Unie werd gedeponeerd in de klasse 36 onder het nummer 004046173.

- Het merk werd op 27 september 2004 door BNP Paribas Fortis gedeponeerd bij het Benelux-Merkenbureau in de klasse 36 onder het nummer 0764125.

III.B. Oorspronkelijke goedkeuring van de identiteit

III.B.1. Methode om het bezit van de private sleutel te bewijzen

De aanvraag van een certificaat aangemaakt door de component van Safran I&S van de technische RA BNP Paribas wordt ondertekend op basis van de bijbehorende private sleutel, terwijl het sleutelpaar wordt aangemaakt door de versleutelingsmodule van de technische RA.

III.B.2. Goedkeuring van de identiteit van de klantinstelling van BNP Paribas

Niet van toepassing.

III.B.3. Goedkeuring van de identiteit van een individu

De registratie van een houder (zie hoofdstuk I.C.3 voor meer informatie) voor de uitgifte van een certificaat wordt verricht door BNP Paribas Fortis in zijn functie van functionele RA.

BNP Paribas Fortis mag de regels voor de controle van de identiteit van de houder vrij bepalen in het kader van zijn activiteit en in zijn rol van functionele RA.

De procedure voor de uitgifte van een certificaat berust op de specificaties van de technische RA die gebruikmaakt van de informatie van de houder op basis van de gegevens die de business toepassing van BNP Paribas Fortis aan de technische RA doorgeeft.

Deze procedure voor de controle van de burgerlijke staat van de houder in de vorm 'voornaam-naam' valt enkel onder de verantwoordelijkheid van BNP Paribas Fortis in het kader van zijn bankactiviteit.

De common name (CN) van het certificaat mag enkel worden gekoppeld aan een natuurlijke persoon en zeker niet aan de naam van een dienst, toepassing of daarmee vergelijkbaar.

III.B.4. Niet-gecontroleerde informatie van de houder

De technische RA maakt enkel gebruik van de informatie die BNP Paribas Fortis doorgeeft in zijn functie van functionele RA, en ze kan niet aansprakelijk worden gesteld voor foute informatie.

III.B.5. Goedkeuring van de autoriteit van de aanvrager

Zie hoofdstuk III.B.4.

III.B.6. Kruiscertificaat van CA

Niet van toepassing.

III.C. Identificatie en goedkeuring van een aanvraag voor de vernieuwing van de sleutels

III.C.1. Identificatie en goedkeuring voor een gewone vernieuwing

Overeenkomstig het document [RFC 3647] stemt het begrip 'certificaatvernieuwing' overeen met de aflevering van een nieuw certificaat waarvan alleen de geldigheidsdata worden gewijzigd, alle andere informatie is hetzelfde als bij het vorige certificaat (inclusief de publieke sleutel van de houder).

De vernieuwing is niet van toepassing in het kader van dit CP.

III.C.2. Identificatie en goedkeuring voor een vernieuwing na intrekking

Niet van toepassing.

III.D. Identificatie en goedkeuring van een intrekkingsaanvraag

a) Voor een tijdelijk certificaat

De aanvraag voor de intrekking van het eindcertificaat kan enkel door de houder worden ingediend in het kader van zijn online-inschrijving. De aanvraag wordt automatisch aanvaard. De houder vraagt de intrekking door de handtekeningaanvraag te annuleren wanneer hij de informatie van de CN in het tijdelijke certificaat (voornaam-naam) krijgt voorgesteld.

De voorwaarden voor die aanvraag worden beschreven in hoofdstuk IV.I.

De methode voor de goedkeuring van een intrekkingsaanvraag is hetzelfde als bij de oorspronkelijke goedkeuring van de houder.

b) Voor een certificaat van de Certificate Authority 'BNPPF Instant CA'

De goedkeuring van een intrekkingsaanvraag van een Certificate Authority komt slechts uitzonderlijk voor.
De voorwaarden voor die aanvraag worden beschreven in hoofdstuk IV.I.

IV. Operationele eisen voor de levenscyclus van de certificaten

IV.A. Certificaataanvraag

IV.A.1. Herkomst van een certificaataanvraag

De certificaataanvraag mag enkel worden uitgegeven door een business toepassing van BNP Paribas Fortis in zijn functie van functionele RA. De business toepassing van BNP Paribas Fortis en de technische RA worden grondig geauthenticeerd voor elke aanvraag van een houdercertificaat.

IV.A.2. Proces en verantwoordelijkheden voor de opstelling van een certificaataanvraag

De certificaataanvraag vereist een uitgebreide authenticatie van de technische componenten van de business toepassing van BNP Paribas Fortis en de technische RA, door gebruik te maken van beveiligde protocollen.

- De functionele RA controleert de statussen van die certificaten voordat ze de aanvraag behandelt.
- De business toepassing van BNP Paribas Fortis is verantwoordelijk voor de controle van de integriteit van de gegevens die via de functionele RA aan de technische RA worden doorgespeeld.
- Het proces voor de aanvraag voor de opstelling van een houdercertificaat wordt beschreven in hoofdstuk I.C.3.

IV.B. Behandeling van een certificaataanvraag

IV.B.1. Uitvoering van de processen voor de identificatie en de goedkeuring van de aanvraag

Procedure voor de identificatie en de goedkeuring van de aanvraag van een houdercertificaat:

- de aanvraag wordt automatisch in elektronische vorm opgesteld door de functionele RA van de metierorganisatie van BNP Paribas Fortis en naar de technische RA van BNP Paribas doorgestuurd;
- er wordt een bewijs voor het bezit van de sleutel aangemaakt en geformatteerd door de technische RA, met de te certificeren informatie, in de vorm van een certificaataanvraag.
- Dat bewijs wordt naar de certificaatoperator verzonden voor ondertekening van het certificaat.

IV.B.2. Aanvaarding of afwijzing van de aanvraag

De houder aanvaardt de certificaataanvraag door zijn oorspronkelijke aanvraag elektronisch te ondertekenen met zijn bankkaart en zijn UCR (challenge M2). Het document wordt hem voorgelegd door de business toepassing van BNP Paribas Fortis en de houder stemt ermee in vóór ondertekening.

IV.B.3. Duur van de opstelling van het certificaat

Het certificaat wordt opgesteld meteen na de ontvangst van de aanvraag door de technische RA en binnen maximaal 24 uur na de ontvangst van de aanvraag.

IV.C. Aflevering van het certificaat

IV.C.1. Acties van de CA voor de aflevering van het certificaat aan de houder

Na authenticatie van de technische RA tegenover de CA 'BNPPF Instant CA' wordt de door de technische RA doorgegeven certificaataanvraag automatisch ondertekend door de CA 'BNPPF Instant CA', na controle van de conformiteit van de inhoud, namelijk:

- de naleving van de samenstelling van de kenmerken van het subject (DN), zie hoofdstuk III.A.5;
- de versleutelingskenmerken van de aanvraag (omvang van de sleutel).

Het certificaat wordt aan de houder doorgegeven via het ondertekende document dat aan het einde van een metiertransactie van BNP Paribas Fortis wordt overhandigd.

IV.C.2. Kennisgeving van de aflevering van het certificaat aan de houder

Het gaat om een automatische verrichting tijdens een proces voor het online afsluiten van contracten.

De houder wordt op de hoogte gebracht van de aflevering aan het einde van de uitvoering van dit proces.

IV.D. Aanvaarding van het certificaat

IV.D.1. Proces voor de aanvaarding van het certificaat

De houder stemt in door de CN van het in zijn naam aangemaakte certificaat uitdrukkelijk te aanvaarden, zie hoofdstuk I.C.3. Hij aanvaardt om de gegevens die hem worden voorgelegd door de functionele RA van BNP Paribas Fortis, te ondertekenen.

IV.D.2. Publicatie van het certificaat

De certificaten worden niet gepubliceerd in het kader van dit CP. De CA 'BNPPF Instant CA' bewaart de uitgegeven certificaten in een database volgens de technische specificaties van haar PKI.

IV.D.3. Kennisgeving van de aflevering van het certificaat

We verwijzen naar het hoofdstuk over de CPS.

IV.E. Gebruik van het sleutelpaar en het certificaat

IV.E.1. Gebruik van de private sleutel en het certificaat door de houder

Het gebruik van de private sleutel van de houder en het bijbehorende certificaat is strikt beperkt tot de ondertekeningsdienst die gebruikmaakt van de producten van Safran I&S. De houders moeten het toegestane gebruik van de sleutelparen en de certificaten strikt naleven. Anders worden zij aansprakelijk gesteld.

De algemene gebruiksvoorwaarden van het certificaat verduidelijken de rollen en de verantwoordelijkheden van de partijen.

IV.E.2. Gebruik van de private sleutel en het certificaat door de gebruiker van het certificaat

Zie hoofdstuk I.C.3 voor de beschrijving van de technische RA.

IV.F. Vernieuwing van een certificaat

Niet van toepassing in het kader van dit CP.

IV.G. Aflevering van een nieuw certificaat na een verandering van het sleutelpaar

De aflevering van een nieuw certificaat voor een bepaalde houder valt onder de verantwoordelijkheid van de functionele RA volgens dezelfde procedure als voor een eerste certificaat.

IV.H. Wijziging van het certificaat

De wijziging van een certificaat stemt overeen met de aflevering van een nieuw certificaat voor dezelfde publieke sleutel, als gevolg van andere informatiewijzigingen dan de geldigheidsdata en het serienummer (anders gaat het om een certificaatvernieuwing).

In dit beleid zijn geen certificaatwijzigingen toegestaan.

IV.I. Intrekking en opschorting van de certificaten

De opschorting is niet van toepassing in het kader van dit CP.

De procedures voor de intrekking van een CA worden beschreven in het CP van de CA's buiten de lijnen 'BNPP PDF CA' en 'BNPP LEVEL2 CA' met respectievelijk de volgende OID's: 1.2.250.1.62.10.1.1.1.1 en 1.2.250.1.62.10.2.1.1.1. In de rest van de alinea wordt alleen de informatie over de intrekking van de eindcertificaten beschreven.

IV.I.1. Mogelijke oorzaken van een intrekking

De volgende omstandigheden kunnen aan de basis liggen van de intrekking van het certificaat van een houder:

- de informatie van de houder in zijn certificaat stemt niet overeen met zijn identiteit;
- de houder zag af van zijn online-inschrijving.

IV.I.2. Herkomst van een intrekkingsaanvraag

De aanvraag voor de intrekking wordt ingediend door de houder door zijn certificaat te weigeren bij een vergissing in zijn identiteit of door van zijn transactie af te zien.

IV.I.3. Procedure voor de behandeling van een intrekkingsaanvraag

De intrekkingsaanvraag van een houder wordt automatisch behandeld door de technische RA.

IV.I.4. Aan de houder toegekende termijn voor de formulering van de intrekkingsaanvraag

Een intrekkingsaanvraag is sowieso dringend. De intrekking van het certificaat gaat in zodra het serienummer van het certificaat wordt ingevoerd in de intrekkingenlijst van de CA 'BNPPF Instant CA' en de lijst beschikbaar is om te downloaden.

De formulering van de aanvraag moet worden behandeld tijdens de sessietijd van een online-inschrijving van een toepassing van BNP Paribas Fortis.

IV.I.5. Behandelingstermijn van een intrekkingsaanvraag

De behandelingstermijn van de intrekking mag niet langer zijn dan zes uur, in overeenstemming met de levensduur van het tijdelijke certificaat.

IV.I.6. Eisen voor de controle van de intrekking door de certificaatgebruikers

De technische RA is ertoe gehouden te controleren of het certificaat van de Certificate Authority 'BNPPF Instant CA' die het certificaat van de houder heeft uitgegeven, wel geldig is.

Voor de ingetrokken certificaten van de houders worden geen eisen geformuleerd.

IV.I.7. Frequentie van de opstelling van de CRL's

Om de 24 uur wordt er een CRL aangemaakt.

IV.I.8. Maximumtermijn voor de publicatie van een CRL

Een CRL moet binnen 30 minuten na aanmaak worden gepubliceerd.

IV.I.9. Beschikbaarheid van een systeem om de intrekking en de status van de certificaten online te controleren

Naast de publicatie van CRL's en certificaten op het internet voorziet de CA niet in een afzonderlijk systeem om de intrekking en de status van de certificaten online te controleren (geen OCSP bijvoorbeeld).

IV.I.10. Eisen voor de onlinecontrole van de intrekking van de certificaten door de certificaatgebruikers

Niet van toepassing.

IV.I.11. Andere beschikbare informatiemiddelen in verband met de intrekkingen

Niet van toepassing.

IV.I.12. Specifieke eisen bij schending van de private sleutel

We verwijzen naar het hoofdstuk over de CPS.

IV.I.13. Mogelijke oorzaken van een opschorting

Niet van toepassing.

IV.J. Functie voor informatie over de status van de certificaten

IV.J.1. Operationele kenmerken

De CA 'BNPPF Instant CA' gebruikt drie adressen om de status van een certificaat te controleren:

- Voor de certificaten van houders:
  - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral1-ca.crl**
  - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral2-ca.crl**
- Voor de certificaten van de Certificate Authority 'BNPPF Instant CA' zelf:
  - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-level2-ca.crl**

IV.J.2. Beschikbaarheid van de functie

Een CRL wordt binnen 30 minuten na aanmaak gepubliceerd. Het beschikbaarheidspercentage is minstens 99,7 procent, de klok rond.

IV.K. Einde van de relatie met de houder

Wanneer de relatie tussen de houder en BNP Paribas Fortis wordt beëindigd, heeft de houder geen toegang meer tot de functionele RA en kan hij dus geen certificaat meer aanvragen.

IV.L. Sleutelescrow en herstel

Private sleutels van de houders in escrow geven is verboden.

V. Niet-technische veiligheidsmaatregelen

De eisen die in de rest van dit hoofdstuk worden beschreven, zijn de minimumeisen die de autoriteiten 'BNPPF Instant CA' moeten naleven in het kader van de hosting van de PKI BNP Paribas bij Safran I&S. De CPS beschrijft de ingezette middelen voor de naleving van die eisen.

V.A. Fysieke veiligheidsmaatregelen

V.A.1. Geografische ligging en constructie van de locaties

De hostinglocaties worden beschreven in het contract tussen Safran I&S en zijn dienstverlener.

De locaties die de te publiceren informatie bevatten, stemmen overeen met de locaties van de host van Safran I&S.

V.A.2. Fysieke toegang

De toegang is strikt beperkt tot de personen die zijn gemachtigd om de lokalen te betreden, en de toegangen moeten traceerbaar zijn. Buiten de openingsuren wordt de veiligheid versterkt door middelen voor de detectie van fysieke en logische indringing in te zetten.

De toegang tot de apparaten (servers, cryptoboxen, administratorpost van de CA, actieve elementen van het netwerk) is strikt beperkt tot de personen die zijn gemachtigd om verrichtingen uit te voeren waarvoor een fysieke toegang tot de apparaten is vereist (toegangscontrole door biometrie, gekoppelde rechten).

V.A.3. Stroomvoorziening en klimaatregeling

De kenmerken van de uitrusting voor de stroomvoorziening en de klimaatregeling maken het mogelijk om rekening te houden met de gebruiksvoorwaarden van de uitrusting van de PKI zoals bepaald door de leveranciers van de uitrusting.

Ze maken het ook mogelijk om rekening te houden met de eisen van dit CP en met de verbintenissen van de CA met betrekking tot de beschikbaarheid van haar functies, met name de functies voor het beheer van de intrekkingen en voor informatie over de status van de certificaten.

V.A.4. Kwetsbaarheid voor waterschade

De beschermingsmiddelen tegen waterschade maken het mogelijk om rekening te houden met de eisen van dit CP en met de verbintenissen van de CA met betrekking tot de beschikbaarheid van haar functies, met name de functies voor het beheer van de intrekkingen en voor informatie over de status van de certificaten.

V.A.5. Brandpreventie en -bescherming

De brandpreventie- en bestrijdingsmiddelen maken het mogelijk om rekening te houden met de eisen van dit CP en met de verbintenissen van de CA met betrekking tot de beschikbaarheid van haar functies, met name de functies voor het beheer van de intrekkingen en voor informatie over de status van de certificaten.

V.A.6. Bewaring van de dragers

De dragers (papier, harde schijf, cd enz.) die de informatie over de activiteit van de PKI (beheer- en opslagfuncties enz.) bevatten, worden behandeld en bewaard in een beveiligde ruimte die alleen toegankelijk is voor de gemachtigde personen.

V.A.7. Buitendienststelling van de dragers

De papieren en magnetische dragers die niet meer bruikbaar zijn, worden systematisch met geschikte middelen vernietigd om elk verlies van vertrouwelijkheid te vermijden.

De opslagdragers (harde schijf van servers) van de PKI worden niet voor andere doeleinden hergebruikt voordat de aan de PKI verbonden informatie die ze eventueel nog bevatten, volledig is vernietigd.

V.A.8. Off-site opslag

De opgeslagen gegevens worden op de verschillende productielocaties van de host van de PKI bewaard: in een lokaal op de primaire locatie en op afstand via automatische synchronisatiesystemen.

V.B. Veiligheidsmaatregelen voor de procedures

V.B.1. Vertrouwensrollen

We onderscheiden de volgende rollen:

- **Security Officer van de PKI**: is belast met de toepassing van de Certificate Policy van BNPPF Instant CA;
- **Chief Physical Security**: is belast met de fysieke toegangscontroles tot de uitrusting van de systemen van de CA-component buiten de RA. Deze leidinggevende wordt benoemd door de partnerhost van Safran I&S;
- **Technische operatoren van de PKI**: zijn belast met het gebruik, de configuratie en het technische onderhoud van de uitrusting, cryptoboxen en servers. Zij ontwikkelen in het bijzonder het technische verloop van de sleutelceremonie;
- **Auditor**: persoon aangewezen door een bevoegde autoriteit (bijvoorbeeld overeenkomstig de 'instructie met betrekking tot de machtigingsprocedure van de organismen die de vertrouwensdienstverleners kwalificeren') die als opdracht heeft regelmatig conformiteitscontroles te verrichten in verband met de organisatie van de door de component aangeleverde functies voor de Certificate Policy, de verklaringen met betrekking tot de certificatiepraktijk van de PKI en het veiligheidsbeleid van de component. De auditor wordt benoemd door BNP Paribas of Safran I&S.

V.B.2. Vereiste aantal personen per taak

Het aantal en de hoedanigheid van de personen die absoluut aanwezig moeten zijn als actoren of als getuigen, kunnen verschillen naargelang het type verrichtingen.

Om veiligheidsredenen worden de gevoelige functies over verschillende personen verdeeld. Dit CP bepaalt een aantal eisen voor die verdeling, met name voor de verrichtingen verbonden aan de versleutelingsmodules van de PKI.

V.B.3. Identificatie en authenticatie voor elke rol

De directie van Safran I&S en ITP ITG laten de identiteit en de machtigingen van hun personeelsleden controleren voordat ze hen een rol en de overeenkomstige rechten toekennen.

V.B.4. Rollen die een scheiding van bevoegdheden vragen

Eenzelfde persoon kan verschillende rollen toevertrouwd krijgen op voorwaarde dat die cumulatie de veiligheid van de vervulde functies niet in gevaar brengt. Voor de vertrouwensrollen is het echter raadzaam dat eenzelfde persoon niet verschillende rollen opneemt en moeten minstens de onderstaande eisen voor niet-cumulatie worden nageleefd.

De aan elke rol verbonden bevoegdheden moeten worden beschreven in de CPS van de CA en in overeenstemming zijn met het veiligheidsbeleid van de betrokken component.

V.C. Veiligheidsmaatregelen tegenover het personeel

V.C.1. Vereiste kwalificaties, vaardigheden en machtigingen

Alle personeelsleden die in de componenten van de PKI aan de slag gaan, zijn contractueel onderworpen aan een veiligheidsbeding.

Elke dienst die werkzaam is voor een component van de PKI, moet erover waken dat de bevoegdheden van zijn personeelsleden die in de component zullen werken, in overeenstemming zijn met hun professionele vaardigheden.

De CA en de certificaatoperator informeren iedereen die een taak vervult in het kader van de vertrouwensrollen van de PKI over:

- zijn verantwoordelijkheden met betrekking tot de diensten van de PKI;
- de procedures voor de beveiliging van het systeem en de controle van het personeel.

Iedere persoon beschikt minstens over de relevante documenten met betrekking tot de operationele procedures en de specifieke tools die hij gebruikt, en over het algemene beleid en de algemene praktijken van de component waarin hij actief is.

De relevante documenten worden beschreven in hoofdstuk V.C.8.

V.C.2. Procedures voor de controle van antecedenten

De personeelsleden van de PKI worden geïdentificeerd en mogen geen veroordeling hebben opgelopen die in strijd is met hun bevoegdheden.

V.C.3. Eisen inzake basisopleiding

Het uitvoerend personeel moet een opleiding hebben gevolgd inzake de software, de hardware en de interne werkingsprocedures van de component waarvoor het werkzaam is.

V.C.4. Eisen en frequentie van de bijscholing

Het betrokken personeel moet relevante informatie en een relevante opleiding krijgen vóór elke wijziging in de systemen, de procedures, de organisatie enz., naargelang de aard van die wijzigingen.

V.C.5. Rotatiefrequentie en -volgorde voor verschillende bevoegdheden

Voor het loopbaanbeheer van de beheerders gelden de regels van de werkgever.

V.C.6. Sancties bij niet-toegestane acties

De Certificate Authority beslist over de toe te passen sancties wanneer een medewerker misbruik maakt van zijn rechten of een verrichting uitvoert die niet strookt met zijn bevoegdheden.

V.C.7. Eisen tegenover het personeel van de externe dienstverleners

De personeelsleden-contractanten die voor Safran I&S werken, moeten aan dezelfde voorwaarden voldoen als opgesomd in hoofdstukken V.C.1 tot V.C.4.

De personeelsleden-contractanten die voor BNP Paribas werken, moeten het HR-beleid en de controles naleven die door hun onderneming worden opgelegd.

V.C.8. Aan het personeel verstrekte documenten

Het personeel moet over de volgende documenten beschikken:

- verklaring met betrekking tot de certificatiepraktijk, specifiek voor het certificatiedomein;
- documenten van de bouwers van de gebruikte hardware en software;
- Certificate Policy onderschreven door de component waartoe hij behoort;

- interne werkingsprocedures.

De Certificate Authority en -operator moeten erop toezien dat hun respectieve personeel (zoals bepaald in de CPS) wel in het bezit is van de hierboven vermelde documenten volgens hun behoefte zoals vermeld in de CPS.

V.D. Procedures voor de verzameling van auditgegevens

Logging bestaat erin gebeurtenissen manueel of elektronisch te registreren door ze in te voeren of automatisch aan te maken.

De papieren of elektronische resultaten die eruit voortvloeien, moeten het mogelijk maken om de uitgevoerde verrichtingen te traceren en toe te wijzen.

V.D.1. Te registreren types gebeurtenissen

De PKI van de groep BNP Paribas wordt gehost bij Safran I&S en houdt van bij de start van een systeem automatisch elektronische logbestanden bij voor de systemen verbonden aan de functies die zij in het kader van de PKI organiseert, met betrekking tot de volgende gebeurtenissen:

- aanmaak/wijziging/schrapping van gebruikersaccounts (toegangsrechten) en overeenkomstige authenticatiegegevens (paswoorden, certificaten enz.);
- opstart en stopzetting van informaticasystemen en toepassingen;
- gebeurtenissen verbonden aan de loggingactiviteit: opstarten en afsluiten van de logfunctie, wijziging van de loginstellingen, ondernomen acties na een storing in de logfunctie;
- in- en uitloggen van de gebruikers met vertrouwensrollen en overeenkomstige mislukte pogingen.

De Security Officer van Safran I&S moet ook nog andere gebeurtenissen kunnen optekenen met elektronische of manuele middelen. Het gaat om gebeurtenissen die betrekking hebben op de veiligheid en niet automatisch door de informaticasystemen worden aangemaakt, namelijk:

- de fysieke toegangen;
- het onderhoud en de wijzigingen in de configuratie van de systemen;
- de veranderingen in het personeel;
- het vernietigen en het resetten van dragers die vertrouwelijke informatie bevatten (sleutels, activeringsgegevens, persoonlijke informatie over de houders enz.).

Naast die gemeenschappelijke loggingeisen voor alle componenten en alle functies van de PKI, moeten ook logbestanden worden bijgehouden van specifieke gebeurtenissen voor de verschillende functies van de PKI, met name:

- ontvangst van een certificaataanvraag (eerste aanvraag en vernieuwing);
- goedkeuring/afwijzing van een certificaataanvraag;
- gebeurtenissen verbonden aan de handtekeningsleutels en certificaten van de CA (aanmaak (sleutelceremonie), bewaring, herstel, intrekking, vernieuwing, vernietiging enz.);
- aanmaak van de certificaten van de houders;
- publicatie en bijwerking van de informatie over de CA (CP, CA-certificaten, algemene gebruiksvoorwaarden enz.);
- ontvangst van een intrekkingsaanvraag;
- goedkeuring/afwijzing van een intrekkingsaanvraag;
- aanmaak en publicatie van CRL's.

Elke registratie van een gebeurtenis in een logbestand moet minstens de volgende velden bevatten:

- type gebeurtenis;
- naam van de uitvoerder of het aanspreekpunt van het systeem dat de gebeurtenis in gang zet;
- datum en tijdstip van de gebeurtenis;
- resultaat van de gebeurtenis (mislukking of succes).

Een actie wordt toegeschreven aan de persoon, het organisme of het systeem die (dat) ze heeft uitgevoerd. De naam of de ID van de uitvoerder moet uitdrukkelijk worden vermeld in een van de velden van het gebeurtenissenlogboek.

V.D.2. Frequentie van de behandeling van de gebeurtenissenlogboeken

De inhoud van de gebeurtenissenlogboeken moet regelmatig en minstens eenmaal per kwartaal worden geanalyseerd.

V.D.3. Bewaringsperiode van de gebeurtenissenlogboeken

De gebeurtenissenlogboeken worden vijf jaar bewaard.

V.D.4. Bescherming van de gebeurtenissenlogboeken

De PKI van de groep BNP Paribas treft de vereiste maatregelen om de integriteit en de beschikbaarheid van de gebeurtenissenlogboeken voor de betrokken component te waarborgen, overeenkomstig de eisen van dit beleid.

V.D.5. Procedure voor de back-up van de gebeurtenissenlogboeken

De PKI van de groep BNP Paribas treft de vereiste maatregelen om de integriteit en de beschikbaarheid van de gebeurtenissenlogboeken voor de betrokken component te waarborgen, overeenkomstig de eisen van dit beleid.

Na elke ceremonie op de platformen van de PKI van de groep BNP Paribas wordt er een back-up van de gebeurtenissenlogboeken gemaakt.

V.D.6. Verzamelsysteem van de gebeurtenissenlogboeken

De PKI van de groep BNP Paribas steunt op de verzamelsystemen binnen elk van haar componenten.

V.D.7. Kennisgeving van de registratie van een gebeurtenis aan de verantwoordelijke voor de gebeurtenis

Niet van toepassing.

V.D.8. Evaluatie van de kwetsbaarheden

Het proces voor de evaluatie van de kwetsbaarheden is identiek aan de risicoanalyse van Safran I&S en BNP Paribas voor haar PKI met ETSI 102 042-certificering.

Er worden ook regelmatig aanvullende indringingstesten verricht.

V.E. Archivering van de gegevens

V.E.1. Te archiveren gegevenstypes

Dankzij de archivering is het mogelijk om:

- de duurzaamheid te garanderen van de logboeken die door de verschillende componenten van de PKI werden aangemaakt;
- de papierstukken te bewaren van de certificatieverrichtingen en ze zo nodig beschikbaar te maken.

De volgende gegevens moeten worden gearchiveerd:

- de (uitvoerbare) software en de configuratiebestanden van de informatica-uitrusting;
- het CP;
- de certificaten en CRL's zoals uitgegeven of gepubliceerd;
- de auditgegevens;
- de gebeurtenissenlogboeken van de verschillende entiteiten van de PKI;

- de papierstukken van de PKI.

V.E.2. Procedure voor de samenstelling van het archief

Voor alle informatie over het archief met betrekking tot de klantcertificaten, verwijzen we naar de informatie over de opgeslagen gegevens in het bewijsdossier in de bijlagen van de CPS.

We verwijzen naar het hoofdstuk over de CPS.

V.E.3. Bewaringsperiode van het archief

Bewaartermijn van het elektronisch archief:

- bewaartermijn van het archief voor de gebeurtenissenlogboeken: vijf jaar;
- bewaartermijn van het archief voor de vervallen certificaten en CRL's: vijf jaar;
- de gegevens in verband met de kennis van de klant worden minstens voor de duur van de klantenrelatie vermeerderd met tien jaar bewaard.

V.E.4. Termijn voor opvraging uit het archief

Het archief kan in minder dan vijf werkdagen worden opgevraagd.

V.E.5. Bescherming van het archief

Tijdens de volledige bewaringstermijn zijn het archief en de back-ups:

- beschermd op het vlak van integriteit;
- toegankelijk voor de gemachtigde personen;
- toegankelijk om te herlezen en te gebruiken.

De CPS beschrijft de ingezette middelen om de stukken in alle veiligheid te archiveren.

V.E.6. Eisen voor de tijdstempel van de gegevens

We verwijzen naar het hoofdstuk over de CPS.

V.E.7. Verzamelsysteem van het archief

Als verzamelsysteem van het archief wordt het informatiesysteem van Safran I&S en zijn host gebruikt.

V.E.8. Procedures voor de opvraging en de controle van het archief

Het archief wordt beheerd door de PKI van de groep BNP Paribas. Het opvragingsproces moet het voorwerp vormen van een interne werkingsprocedure die in de CPS van de online-CA's wordt vermeld. De opgevraagde gegevens moeten binnen een termijn van maximaal vijf werkdagen beschikbaar zijn.

V.F. Verandering van sleutel van de autoriteit

De CA verandert haar sleutelpaar als het niet langer in overeenstemming is met het standaard versleutelingsreferentiesysteem zoals uitgegeven door het ANSSI. De maximale levensduur van een CA-certificaat moet coherent zijn met het versleutelingsreferentiesysteem van het ANSSI.

De autoriteit 'BNPPF Instant CA' mag geen certificaat aanmaken waarvan de einddatum later valt dan de vervaldatum van haar eigen certificaat. Daarom is de geldigheidsperiode van haar eigen certificaat langer dan van de certificaten die ze ondertekent.

Ook als zij een certificaataanvraag behandelt, bepaalt de autoriteit 'BNPPF Instant CA' de levensduur van het gevraagde certificaat zodanig dat het nooit langer geldig is dan de einddatum van de geldigheid van het certificaat van het sleutelpaar dat ze voor de handtekening heeft gebruikt.

V.G. Hervatting na schending en schade

V.G.1. Procedures voor de melding en de behandeling van incidenten en schendingen

De beheerteams van Safran I&S hanteren procedures en middelen voor de melding en de behandeling van incidenten, met name door de bewustmaking en de opleiding van hun personeelsleden.

De analyse van de verschillende gebeurtenissenlogboeken wordt gecontroleerd door de Security Officer van Safran I&S.

V.G.2. Hervattingsprocedures bij corruptie van de informaticamiddelen (hardware, software en/of gegevens)

Door de back-up van de componenten van de PKI kan de activiteit bij schade binnen 48 uur worden hervat. Dat geldt alleen als er dringend CRL's moeten worden aangemaakt.

V.G.3. Hervattingsprocedures bij schending van de private sleutel van een component

Bij schending van een autoriteitsleutel wordt het overeenkomstige certificaat onmiddellijk ingetrokken (volgens de realisatietermijn van de sleutelceremonie).

V.G.4. Hervattingsprocedures bij schending van een algoritme van een component

Bij schending van een algoritme dat wordt gebruikt in een Certificate Authority, wordt het overeenkomstige certificaat ingetrokken via een sleutelceremonie.

V.G.5. Bedrijfscontinuïteitsmogelijkheden na schade

De verschillende componenten van de PKI van de groep BNP Paribas beschikken over de nodige middelen om hun activiteiten voort te zetten overeenkomstig de eisen van dit beleid.

Voor de onlineautoriteit bestaat de bedrijfscontinuïteit in het herstel van de PKI op basis van de back-ups en de geheime codes.

V.H. Einde van de levensduur van de PKI van de groep BNP Paribas

Een of meer componenten van de PKI kunnen hun activiteit moeten stopzetten of naar een andere entiteit moeten overbrengen.

De activiteitsoverdracht wordt gedefinieerd als de beëindiging van de activiteit van een component van de PKI zonder invloed op de geldigheid van de vóór de betrokken activiteitsoverdracht uitgegeven certificaten en de hervatting van die activiteit, door de CA georganiseerd in samenwerking met de nieuwe entiteit.

De stopzetting van de activiteit wordt gedefinieerd als de beëindiging van de activiteit van een component van de PKI met een invloed op de geldigheid van de certificaten die vóór de betrokken stopzetting werden uitgegeven.

Bij stopzetting van de activiteit verbinden BNP Paribas en Safran I&S zich ertoe om menselijke middelen in te zetten voor de intrekking van alle CA-certificaten van de PKI.

Als Safran I&S ten slotte niet in staat zou zijn om de vereiste kosten voor de voortzetting van de verrichtingen van de CA ten laste te nemen, bijvoorbeeld bij stopzetting van de activiteit, dan verbindt BNP Paribas zich ertoe om die kosten te dekken.

V.H.1. Overdracht of stopzetting van de activiteit met invloed op een component van de PKI

De activiteitsoverdracht komt niet aan bod in het kader van dit Certificate Policy.

Om een constant vertrouwensniveau te garanderen tijdens en na dergelijke gebeurtenissen heeft de CA onder meer de volgende verplichtingen:

- procedures invoeren met als doel een constante dienstverlening te garanderen, in het bijzonder voor de archivering (met name de archivering van de certificaten van de houders en de informatie over de certificaten);
- de continuïteit van de intrekking garanderen (rekening houden met een intrekkings- en publicatieaanvraag voor de CRL's), overeenkomstig de beschikbaarheidseisen voor de functies zoals bepaald in dit CP;
- vooraf haar voornemen voor de activiteitsoverdracht op een bepaalde datum meedelen;
- alle beschikbare middelen inzetten om haar partners (eindgebruikers, andere componenten, andere PKI's enz.) in te lichten over haar voornemen om haar activiteit stop te zetten;
- de CA moet in haar CPS verduidelijken wie zij moet waarschuwen, hoe de overdracht van de verplichtingen verloopt (archief en logs naar een andere entiteit) en hoe de nog geldige, maar in te trekken certificaten zullen worden behandeld.

V.H.2. Stopzetting van de activiteit met invloed op de CA

De activiteit kan volledig of gedeeltelijk worden stopgezet (bv. stopzetting van de activiteit enkel voor een welbepaalde familie van certificaten). De gedeeltelijke stopzetting van de activiteit moet geleidelijk gebeuren zodat alleen de verplichtingen zoals bedoeld in de eerste drie items hieronder moeten worden uitgevoerd door de CA of een derde entiteit die de activiteiten overneemt zodra het laatste door haar uitgegeven certificaat vervalt.

Bij een volledige stopzetting van de activiteit moet de CA of als dat onmogelijk is, elke entiteit die in haar plaats komt op grond van een wet, reglement, gerechtelijke beslissing of een eerder met die entiteit gesloten overeenkomst, de certificaten intrekken en de ARL's publiceren overeenkomstig de in haar CP aangegane verbintenissen.

VI. Technische veiligheidsmaatregelen

VI.A. Aanmaak en installatie van sleutelparen

VI.A.1. Aanmaak van sleutelparen

a) Autoriteitsleutels

De vertrouwelijkheid van de sleutels wordt met name gegarandeerd door technische maatregelen die worden beschreven in de CPS.

De handtekeningsleutels van de autoriteit 'BNPPF Instant CA' worden aangemaakt en gebruikt in een cryptobox waarvan de kenmerken worden beschreven in de CPS.

De handtekeningsleutels van de autoriteit 'BNPPF Instant CA' worden aangemaakt in perfect gecontroleerde omstandigheden, door personeelsleden in vertrouwensrollen, in het kader van 'sleutelceremonies'. Die ceremonies verlopen volgens vooraf bepaalde scripts.

De opstart van de PKI en/of de aanmaak van de handtekeningsleutels van de autoriteit 'BNPPF Instant CA' gaan gepaard met de aanmaak van delen van geheime codes (beschermingsprincipe n op m). Die delen van geheime codes zijn gegevens op basis waarvan na de sleutelceremonie de private handtekeningsleutels van de autoriteiten 'BNPPF Instant CA' kunnen worden beheerd en bewerkt, met name om later nieuwe versleutelingsmodules op te starten met de handtekeningsleutels van de rootautoriteit.

De cryptobox, gebruikt door alle autoriteiten van de PKI van BNP Paribas om de handtekeningsleutels aan te maken en te gebruiken (voor de aanmaak van elektronische certificaten, intrekkingslijsten) heeft als doel:

- de vertrouwelijkheid en de integriteit van de private handtekeningsleutels te waarborgen tijdens hun volledige levenscyclus en hun veilige vernietiging te garanderen aan het einde van hun levensduur;
- in staat te zijn om de gebruikers, houders van geheime codes voor de activering van de box, te identificeren en te authenticeren;
- de mogelijkheid te bieden om een beveiligde elektronische handtekening aan te maken om de door de autoriteit aangemaakte certificaten te ondertekenen, die niet kan worden vervalst zonder kennis van die private sleutels;
- auditregistraties aan te maken voor elke actie die via een autoriteitsleutel wordt verricht.

b) Sleutels van de houders

Software van Safran I&S maakt het sleutelpaar van een houder aan via een materiële versleutelingsmodule (HSM) waarvan de eisen worden beschreven in § VI.B.1.

VI.A.2. Overdracht van de private sleutel aan de eigenaar

a) Autoriteitsleutels

We verwijzen naar het hoofdstuk over de CPS.

b) Sleutels van de houders

De private sleutel van de houder wordt enkel onder controle van de persoon zelf behouden via software van Safran I&S en kan door die software enkel worden gebruikt bij de ondertekening van een document dat BNP Paribas ter beschikking stelt. De sleutel wordt meteen na gebruik vernietigd.

VI.A.3. Overdracht van de publieke sleutel aan de CA

De publieke sleutels van de houders worden afgegeven aan de CA op basis van aanvragen die in het formaat PKCS #10 worden aangemaakt door software van Safran I&S. De aanvraag PKCS #10 wordt ondertekend met behulp van de private sleutel van de houder. De handtekening wordt gecontroleerd door de CA. Zij geeft een certificaat uit als de controle in orde is. De integriteit van de aflevering wordt aldus van begin tot einde beschermd bij de aanvraag voor de aanmaak van het certificaat.

VI.A.4. Overdracht van de publieke sleutel van de CA aan de certificaatgebruikers

BNP Paribas stelt alle autoriteitcertificaten ter beschikking via zijn publicatiedienst.

De CA kan haar certificaat ook rechtstreeks aan de deelnemers van een sleutelceremonie bezorgen op een verwisselbare drager.

VI.A.5. Omvang van de sleutels

De autoriteiten gebruiken sleutels van 4.096 bits.

De houders gebruiken sleutels van minstens 2.048 bits.

De CA volgt de versleutelingsaanbevelingen van het ANSSI in het kader van RGS.

VI.A.6. Controle van de aanmaak van de parameters van de sleutelparen en hun kwaliteit

De uitrusting voor de aanmaak van sleutelparen maakt gebruik van parameters die de specifieke veiligheidsnormen van het algoritme van het sleutelpaar naleven (zie hoofdstuk VII).

VI.A.7. Levensduur van de sleutels

Zie hoofdstuk VI.C.2.

VI.A.8. Doelstellingen van het gebruik van de sleutel

Het gebruik van een private CA-sleutel en het bijbehorende certificaat is strikt beperkt tot de ondertekening van certificaten en CRL's.

Het gebruik van de private sleutel van de houder en het bijbehorende certificaat is strikt beperkt tot de ondertekeningsdienst die gebruikmaakt van de producten van Safran I&S.

VI.B. Veiligheidsmaatregelen voor de bescherming van de private sleutels en voor de versleutelingsmodules

VI.B.1. Veiligheidsnormen en -maatregelen voor de versleutelingsmodules

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

De private sleutel van de houder is beschermd door een cryptobox met een minimaal weerstandsniveau FIPS 140-2 level 2.

VI.B.2. Controle van de private sleutel door meerdere personen

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

De private sleutel van de houders wordt niet door meerdere personen gecontroleerd.

VI.B.3. Escrow van de private sleutel

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

De private sleutels van de houders worden niet in escrow gegeven.

VI.B.4. Back-up van de private sleutel

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

De CA maakt geen back-up van de private sleutels van de houders.

VI.B.5. Archivering van de private sleutel

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

De private sleutels van de houders worden in geen geval gearchiveerd.

VI.B.6. Overdracht van de private sleutel van/naar de versleutelingsmodule

Zie hoofdstuk VI.B.4.

VI.B.7. Opslag van de private sleutel in een versleutelingsmodule

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

De private sleutels van de houders worden opgeslagen in een versleutelingsmodule die minstens aan de eisen van hoofdstuk XI hierna beantwoordt.

VI.B.8. Methode voor de activering van de private sleutel

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

We verwijzen naar het hoofdstuk over de CPS.

VI.B.9. Methode voor de deactivering van de private sleutel

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

We verwijzen naar het hoofdstuk over de CPS.

VI.B.10. Methode voor de vernietiging van de private sleutels

a) Autoriteitsleutels

Zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

b) Sleutels van de houders

Na ondertekening wordt de vernietiging van de sleutels opgestart door software van Safran I&S.

VI.B.11. Veiligheidsevaluatieniveau van de versleutelingsmodule

a) Autoriteitsleutels

De versleutelingsmodules van een CA van de PKI van de groep BNP Paribas worden geëvalueerd op een niveau dat overeenstemt met het beoogde gebruik, zoals beschreven in hoofdstuk XI hierna.

b) Sleutels van de houders

Zie vorige alinea.

VI.C. Andere aspecten van het beheer van de sleutelparen

VI.C.1. Archivering van de publieke sleutels

a) Autoriteitsleutels

De publieke sleutels van de CA's van de PKI van de groep BNP Paribas worden gearchiveerd in het kader van de archivering van de overeenkomstige certificaten.

a) Sleutels van de houders

Ze worden niet gearchiveerd.

VI.C.2. Levensduur van de sleutelparen en de certificaten

Voor een CA-certificaat:

- bedraagt de levensduur van de sleutels 23 jaar.

Voor een tijdelijk certificaat:

- kan de levensduur van de certificaten worden ingesteld en bedraagt hij maximaal 1 uur;
- is de levensduur van de sleutelparen beperkt tot hun koppeling aan een certificaat.

De einddatum van de geldigheid van een CA-certificaat valt na het einde van de levensduur van de certificaten die ze uitgeeft.

VI.D. Activeringsgegevens

VI.D.1. Aanmaak en installatie van de activeringsgegevens van de HSM

a) Voor de autoriteitsleutels

De aanmaak en de installatie van de activeringsgegevens van een versleutelingsmodule van de PKI gebeuren tijdens de opstart- en personaliseringsfase van de cryptobox. De activeringsgegevens worden gekozen en ingevoerd door de verantwoordelijken voor die gegevens zelf.

Ze zijn alleen gekend door de met naam geïdentificeerde verantwoordelijken in het kader van de rollen die hen zijn toevertrouwd, en het management van Safran I&S moet toestemming geven voor hun toegang.

b) Voor de sleutels van houders

De aanmaak en de installatie van de activeringsgegevens van een versleutelingsmodule van de PKI gebeuren tijdens de opstart- en personaliseringsfase van de cryptobox. De activeringsgegevens worden gekozen en ingevoerd door de verantwoordelijken voor die gegevens zelf.

Ze zijn alleen gekend door de leden van ITP ITG in het kader van de rollen die hen zijn toevertrouwd.

VI.D.2. Bescherming van de activeringsgegevens van de HSM

De integriteit en de vertrouwelijkheid van de activeringsgegevens die zijn aangemaakt voor de versleutelingsmodules van de PKI van de groep BNP Paribas, worden beschermd tot de uitgifte aan de ontvanger.

VI.D.3. Bescherming van de activeringsgegevens overeenstemmend met de private sleutels van de houders

We verwijzen naar het hoofdstuk over de CPS.

VI.D.4. Andere aspecten met betrekking tot de activeringsgegevens

We verwijzen naar het hoofdstuk over de CPS.

VI.E. Veiligheidsmaatregelen voor de informaticasystemen

VI.E.1. Specifieke technische veiligheidseisen voor de informaticasystemen

We verwijzen naar het hoofdstuk over de CPS.

VI.E.2. Kwalificatieniveau van de informaticasystemen

De versleutelingsmodule die wordt gebruikt door de PKI van de groep BNP Paribas, vormt het voorwerp van een 'common criteria'-certificering EAL4+.

VI.F. Veiligheidsmaatregelen voor de ontwikkeling van de systemen

De ontwikkelingsomgeving is afgescheiden van de productieomgeving.

VI.F.1. Maatregelen voor het beheer van de veiligheid

Alle belangrijke ontwikkelingen in een systeem van een component van de PKI van de groep BNP Paribas moeten worden gedocumenteerd en opgenomen in de interne werkingsprocedures van de betrokken component en moeten in overeenstemming zijn met het onderhoudsschema van de conformiteitswaarborg voor geëvalueerde producten.

VI.F.2. Veiligheidsevaluatieniveau van de levenscyclus van de systemen

Dit beleid bevat hierover geen specifieke eisen.

VI.G. Veiligheidsmaatregelen voor het netwerk

De onderlinge verbindingen en toegangen tot de middelen van de PKI worden gecontroleerd door uitrusting en software die een segmentering van de gegevens, diensten en gebruikers per rol en functie mogelijk maken. Die oplossingen garanderen een controle van de inkomende en uitgaande stromen. De wijzigingen van de geopende poorten, toegangsrechten en andere wijzigingen moeten systematisch worden opgespoord in een ruimte voor de follow-up van wijzigingen in de logische toegangen.

VI.H. Tijdstempel/dateringssysteem

Om deze gebeurtenissen te dateren gebruiken de verschillende componenten van de PKI de systeemtijd van de PKI en zorgen ze ervoor dat de systeemklokken van de PKI onder elkaar minstens tot op de minuut zijn gesynchroniseerd, en minstens tot op de seconde ten opzichte van een betrouwbare UTC-tijdbron.

VII. Profielen van de certificaten, OCSP en CRL's

VII.A. Profiel van de certificaten

VII.A.1. Versienummer

De certificaten die worden uitgegeven in het kader van de PKI van de groep BNP Paribas, voldoen aan de norm X.509 v3.

VII.A.2. Basisvelden

De certificaten volgen het basisformaat van de certificaten zoals bepaald in de aanbeveling x.509v3 en bevatten minstens de volgende basisvelden:

Naam van het veld	Beschrijving	Inhoud
Version	Versie van het certificaat X.509	Bevat de waarde 2 om aan te geven dat het om een certificaat x.509v3 gaat.
SerialNumber	Serienummer van het certificaat	Bevat een geheel getal om het serienummer van het certificaat aan te geven. Die waarde moet uniek zijn voor elk certificaat dat de rootautoriteit uitgeeft.
Signature	Handtekening van de autoriteit om het certificaat te authenticeren	Sha2WithRSAEncryption
Issuer	Naam van de autoriteit	Bevat de DN (X.500) van de autoriteit.
Validity	Geldigheidsperiode van het certificaat	Bevat de activerings- en vervaldatum van het certificaat.
Subject	Naam van de houder	Bevat de DN van de houder.
Subject Public Key Info	Informatie over de publieke sleutel van de abonnee	Bevat de OID van het algoritme en de publieke sleutel van de abonnee.
Extensions	Lijst met de extensies	Zie volgend hoofdstuk.

VII.A.3. Extensies van het certificaat

De certificaten die worden uitgegeven door de Certificate Authority 'BNPPF Instant CA' bevatten de volgende X.509v3-extensies. Het CPS verduidelijkt de gebruikte waarden.

Extensie	Kritieke extensie	Beschrijving
Authority Key Identifier	N	Identificatie-element van de publieke sleutel van de autoriteit die het certificaat ondertekent

Extensie	Kritieke extensie	Beschrijving
KeyUsage	O	Beschrijving van het toegestane gebruik van de private sleutel: Non repudiation
Certificate Policies	N	OID van het CP dat van toepassing is op het certificaat, wettelijke vermelding en naam van het CP
Authority Information Access	N	Informatie over de toegang tot het certificaat van de autoriteit
Subject Key Identifier	N	Identificatie-element van de publieke sleutel van de houder
CRL Distribution Point	N	Bevat de URL van de CRL

VII.A.4. OID van de algoritmen

De identificatiecodes van algoritmen moeten worden bijgehouden in een register (bv. een internationaal register zoals ISO).

Het gebruikte hash-algoritme in het kader van de PKI van de groep BNP Paribas is SHA-2 (OID 2.16.840.1.101.3.4.2.1). Het gebruikte versleutelingsalgoritme in het kader van de PKI van de groep BNP Paribas is RSA.

De handtekening wordt geplaatst in RSA-SHA256 met als OID 1.2.840.113549.1.1.11.

VII.A.5. Vorm van de namen

De aan de houders toegekende namen in het kader van de PKI van de groep BNP Paribas voldoen aan de norm X.500, zoals beschreven in hoofdstuk III.A van dit document.

VII.A.6. OID van de Certificate Policy

a) Autoriteitcertificaten

De actoren die aanwezig zijn bij de sleutelceremonie, gaan na of de uitgegeven certificaten de OID 'Any Policy' (2.5.29.32.0) bevatten.

b) Certificaten van de houders

De certificaten van de houders verwijzen naar de OID van dit Certificate Policy.

VII.A.7. Gebruik van de extensie 'beleidscriteria'

Dit beleid bevat hierover geen bijzondere eisen.

VII.A.8. Betekenis en vorm van de beleidsqualifiers

Dit beleid bevat hierover geen bijzondere eisen.

VII.A.9. Betekenis voor de behandeling van de kritieke extensies van de Certificate Policy

Dit beleid bevat hierover geen bijzondere eisen.

VII.B. Profiel van de CRL's

VII.B.1. Versienummer

De uitgegeven CRL's maken gebruik van versie 2 van het formaat dat in de ISO-norm [9594-8] is vastgelegd.

VII.B.2. Basisvelden

Dit zijn de basisvelden van de CRL's die door de rootautoriteit worden uitgegeven:

Veld	Beschrijving
Version	Versie van de CRL X.509
Signature	Identifier van het gebruikte algoritme om het integriteitszegel van de lijst aan te maken Sha2WithRSAEncryption geselecteerd voor dit CP
Issuer	Naam van de autoriteit van de PKI van de groep BNP Paribas
This Update	Uitgiftedatum van de CRL
Next Update	Uiterste datum voor de uitgifte van de CRL
Revoked Certificates	Lijst voor de registratie van intrekkingen Voor elke intrekking worden de waarden in de volgende velden ingevuld: - User Certificate (serienummer van het ingetrokken certificaat); - Revocation Date (intrekkingsdatum van het certificaat).
CRL Extensions	Algemene extensies van de CRL

De eindversie van de CRL bevat de volgende elementen:

Veld	Beschrijving
tbsCertlist	Alle hierboven beschreven velden
signatureAlgorithm	De identifier van het gebruikte algoritme om het integriteitszegel van de lijst aan te maken Sha2WithRSAEncryption geselecteerd voor dit CP
signatureValue	Het resultaat van dit algoritme op alle velden van tbsCertList

VII.C. CRL-extensies en CRL-inputextensies

De CRL's bevatten de basisvelden van de vorige alinea en daarnaast ook de volgende inputextensies:

Inputextensie	Beschrijving

Authority Key Identifier	Identificeert de publieke sleutel van de autoriteit die de CRL ondertekende
CRL Number	Geeft een opeenvolgend toenemend getal voor elke uitgegeven CRL
MS "CA Version"	Extensie Microsoft AD CS verbonden aan de versie van de CA-sleutels
MS "CRL Next Publish"	Extensie Microsoft AD CS verbonden aan de datum van de volgende publicatie
Reason Code	Identificeert de oorzaak van de intrekking van het certificaat.

VIII. Conformiteitsaudit en andere evaluaties

VIII.A. Frequentie en/of omstandigheden van de evaluaties

Elk jaar wordt er een conformiteitscontrole van de volledige PKI van de groep BNP Paribas verricht. BNP Paribas verricht ook een jaarlijkse interne audit.

VIII.B. Identiteit/kwalificaties van de evaluators

De controle van een component moet door de directie van Safran I&S of BNP Paribas worden toegewezen aan een team van bekwame actoren op het gebied van de beveiliging van de informatiesystemen en in het werkgebied van de gecontroleerde component.

De actoren die de interne audits verrichten, moeten eveneens voldoen aan de voorwaarden die in de vorige alinea worden bepaald.

VIII.C. Relaties tussen evaluators en geëvalueerde entiteiten

De organisatie van de interne audits wordt beschreven in de bijbehorende CPS.

VIII.D. Onderwerpen die in de evaluaties aan bod komen

De conformiteitscontroles of interne controles van BNP Paribas hebben betrekking op de volledige PKI van de groep BNP Paribas en zijn bedoeld ter controle van de naleving van de verbintenissen en praktijken zoals bepaald in dit Certificate Policy en in de overeenkomstige CPS en van de elementen die eruit voortvloeien (operationele procedures, ingezette middelen enz.).

VIII.E. Ondernomen acties op grond van de conclusies van de evaluaties

Na een conformiteitscontrole of een interne audit bezorgt de evaluator een conformiteitsrapport met aanbevelingen aan ITP ITG.

ITP ITG, bij delegatie aan de in dit beleid geïdentificeerde actoren, moet de niet-conforme punten verhelpen en beslissen over de te treffen maatregelen.

VIII.F. Mededeling van de resultaten

De resultaten van de conformiteitsaudits zijn vertrouwelijk en mogen alleen op uitdrukkelijk verzoek aan derden worden meegedeeld.

Bovendien worden de resultaten van de conformiteitsaudits en de interne audits aan de PMA meegedeeld.

IX. Bijlage 1 – Andere kwesties in verband met het metier en de wetgeving

IX.A. Tarieven

De tarifering die BNP Paribas Fortis toepast voor de gebruiker van het certificaat, klant van BNP Paribas Fortis, wordt vermeld in de algemene voorwaarden die van toepassing zijn op het kanaal van BNP Paribas Fortis waarin het certificaat wordt gebruikt.

IX.B. Financiële aansprakelijkheid

De financiële aansprakelijkheid van BNP Paribas Fortis tegenover de gebruiker van het certificaat, klant van BNP Paribas Fortis, wordt vermeld en beperkt in de algemene voorwaarden die van toepassing zijn op het kanaal van BNP Paribas Fortis waarin het certificaat wordt gebruikt.

IX.C. Vertrouwelijkheid van de professionele gegevens

IX.C.1. Scope van de vertrouwelijke gegevens

Minstens de volgende gegevens worden als vertrouwelijk beschouwd:

- de overeenkomstige CPS van dit CP;
- de private sleutels van de componenten en de houders van certificaten van de PKI van de groep BNP Paribas;
- de activeringsgegevens gekoppeld aan de private sleutels van de autoriteiten van de PKI van de groep BNP Paribas;
- alle geheime codes van de PKI van de groep BNP Paribas;
- de gebeurtenissenlogboeken van de componenten van de PKI van de groep BNP Paribas;
- het registratiedossier van de houders;
- de verslagen van de sleutelceremonies.

IX.C.2. Informatie buiten de scope van de vertrouwelijke gegevens

Niet van toepassing.

IX.C.3. Verantwoordelijkheden voor de bescherming van de vertrouwelijke gegevens

BNP Paribas Fortis is er als Certificate Authority toe gehouden om de geldende wetgeving en regelgeving op het Belgische grondgebied na te leven.

IX.D. Bescherming van de persoonsgegevens

BNP Paribas past de toepasselijke wetgeving en regelgeving toe in verband met de bescherming van de persoonsgegevens, zowel voor de verzameling als voor het gebruik van de persoonsgegevens (wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992; Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) vanaf 25 mei 2018).

IX.D.1. Beleid voor de bescherming van de persoonsgegevens

Er wordt overeengekomen dat de persoonsgegevens door de componenten van de PKI van de groep BNP Paribas worden verzameld en gebruikt met strikte naleving van de geldende wetgeving en regelgeving.

IX.D.2. Persoonsgegevens

Minstens de volgende gegevens worden als persoonlijk beschouwd:

- alle gegevens betreffende het registratiedossier van de houders.

IX.D.3. Niet-persoonsgegevens

Er worden hierover geen specifieke eisen gesteld.

IX.D.4. Aansprakelijkheid voor de bescherming van de persoonsgegevens

BNP Paribas Fortis is verantwoordelijk voor de verwerking van de persoonsgegevens van de certificaatgebruikers, klanten van BNP Paribas Fortis.

IX.D.5. Kennisgeving van en instemming met het gebruik van de persoonsgegevens

De verwerking van de persoonsgegevens van de certificaatgebruikers, klanten van BNP Paribas Fortis, vormt het voorwerp van de informatie, kennisgevingen en toestemmingen zoals vermeld in de algemene voorwaarden die van toepassing zijn op het kanaal van BNP Paribas Fortis waarin het certificaat wordt gebruikt.

IX.D.6. Voorwaarden voor de verspreiding van persoonsgegevens aan de gerechtelijke of administratieve autoriteiten

Zie geldende wetgeving en regelgeving op het Belgische grondgebied.

IX.D.7. Andere omstandigheden voor de verspreiding van persoonsgegevens

Zie geldende wetgeving en regelgeving op het Belgische grondgebied.

IX.E. Intellectuele en industriële eigendomsrechten

Toepassing van de geldende wetgeving en regelgeving op het Belgische grondgebied.

IX.F. Contractuele interpretaties en waarborgen

De componenten van de PKI hebben de volgende gemeenschappelijke verplichtingen:

- de integriteit en de vertrouwelijkheid van hun geheime en/of private sleutels beschermen en waarborgen;
- hun encryptiesleutels (publieke, private en/of geheime sleutels) enkel gebruiken voor de bij de uitgifte bepaalde doeleinden en met de tools vermeld in de voorwaarden zoals vastgelegd in het CP van de CA en de documenten die eruit voortvloeien;
- het deel van de CPS dat op hen betrekking heeft, naleven en toepassen;
- zich onderwerpen aan de conformiteitscontroles verricht door het auditteam dat door de CA is gemachtigd (zie hoofdstuk VIII);
- de akkoorden of contracten naleven waardoor ze onder elkaar of met de houders zijn verbonden;
- de vereiste (technische en menselijke) middelen inzetten voor de verwezenlijking van de taken waartoe ze zich verbinden onder voorwaarden die de kwaliteit en de veiligheid garanderen.

IX.F.1. Certificate Authority

Verplichtingen van de CA:

- de gebruikers van haar certificaten kunnen aantonen dat ze een certificaat heeft uitgegeven voor een bepaalde houder en dat die houder het certificaat heeft aanvaard, overeenkomstig de eisen in hoofdstuk IV.4 hierboven;
- garanderen dat haar CPS coherent is en blijft met haar CP;
- alle redelijke maatregelen nemen om zich ervan te vergewissen dat haar houders op de hoogte zijn van hun rechten en hun plichten in het kader van het gebruik en het beheer van de sleutels, certificaten of gebruikte uitrusting en software in het kader van de PKI. De relatie tussen een houder en de CA wordt geformaliseerd via een contractuele band waarin de rechten en de plichten van de partijen en meer bepaald de door de CA verleende waarborgen worden verduidelijkt.

IX.F.2. Registratiedienst

Zie alinea **Error! Reference source not found.**.

IX.F.3. Certificaathouders

De houder is verplicht om juiste en bijgewerkte informatie te verstrekken bij het identificatieproces (identiteit van de klant bijvoorbeeld) en die informatie te controleren.

IX.F.4. Certificaatgebruikers

De certificaatgebruiker, klant van BNP Paribas Fortis, mag het certificaat alleen gebruiken in het kanaal van BNP Paribas Fortis waarin de aanmaak van het certificaat wordt voorgesteld en louter in het kader van de relaties tussen de gebruiker van het certificaat, klant van BNP Paribas Fortis, en BNP Paribas Fortis.

IX.F.5. Andere deelnemers

Er worden hierover geen specifieke eisen gesteld in het kader van dit CP.

IX.G. Waarborglimiet

De aansprakelijkheid van BNP Paribas Fortis tegenover de gebruiker van het certificaat, klant van BNP Paribas Fortis, wordt vermeld en beperkt in de algemene voorwaarden die van toepassing zijn op het kanaal van BNP Paribas Fortis waarin het certificaat wordt gebruikt.

IX.H. Aansprakelijkheidslimiet

De aansprakelijkheid van BNP Paribas Fortis tegenover de gebruiker van het certificaat, klant van BNP Paribas Fortis, wordt vermeld en beperkt in de algemene voorwaarden die van toepassing zijn op het kanaal van BNP Paribas Fortis waarin het certificaat wordt gebruikt.

IX.I. Vergoedingen

De financiële aansprakelijkheid van BNP Paribas Fortis tegenover de gebruiker van het certificaat, klant van BNP Paribas Fortis, wordt vermeld en beperkt in de algemene voorwaarden die van toepassing zijn op het kanaal van BNP Paribas Fortis waarin het certificaat wordt gebruikt.

IX.J. Duur en vervroegde beëindiging van de geldigheid van het CP

IX.J.1. Geldigheidsduur

Het CP van de CA moet minstens van toepassing blijven tot het einde van de levensduur van het laatste

certificaat dat op grond van dit CP werd uitgegeven.

IX.J.2. Gevolgen van het einde van de geldigheid en van toepassing blijvende bepalingen

Er worden hierover geen specifieke eisen gesteld in het kader van dit CP.

IX.K. Individuele kennisgevingen en communicatie tussen de deelnemers

Er worden hierover geen specifieke eisen gesteld in het kader van dit CP.

IX.L. Wijzigingen in het CP

IX.L.1. Wijzigingsprocedures

Grote wijzigingen in dit CP moeten worden voorgelegd aan een Policy Management Authority (PMA) om de aangebrachte wijzigingen goed te keuren vóór de publicatie van de nieuwe versie van het CP.

Kleinere wijzigingen (druk- of typfouten enz.) vereisen geen formele goedkeuring van de PMA vóór de publicatie van de nieuwe versie van het CP.

IX.L.2. Mechanisme en periode voor informatie over de wijzigingen

Er is geen mechanisme ingesteld voor het verstrekken van informatie over de aangebrachte wijzigingen.

IX.L.3. Omstandigheden waarin de OID moet worden veranderd

De OID van het CP moet worden veranderd bij grote en door de PMA goedgekeurde wijzigingen in het CP.

In dat geval wordt het laatste cijfer van de OID veranderd om de grote wijzigingen te weerspiegelen.

IX.M. Bevoegde rechtbanken

Toepassing van de geldende wetgeving en regelgeving op het Belgische grondgebied.

IX.N. Conformiteit met de wetgeving en regelgeving

Toepassing van de geldende wetgeving en regelgeving op het Belgische grondgebied.

IX.O. Diverse bepalingen

Er worden hierover geen specifieke eisen gesteld in het kader van dit CP.

IX.P. Andere bepalingen

Er worden hierover geen specifieke eisen gesteld in het kader van dit CP.

X. Bijlage 2 – Als referentie aangehaalde documenten

X.A. Regelgeving

Niet van toepassing.

X.B. Technische documenten

Referentie	Voorwerp van het document
FIPS140-2_LEVEL3_CERT	Kwalificatiecertificaat FIPS 140-2 level 3 van de cryptobox nShield (firmware 2.50.16)

Alle gedetailleerde procedures betreffende dit CP worden beschreven in de bijlagen bij de CPS, die op verzoek kan worden geraadpleegd (zie hoofdstuk I.E.2).

XI. Bijlage 3 – Veiligheidseisen van de versleutelingsmodule van de CA's

XI.A. Eisen in verband met de veiligheidsdoelstellingen

De versleutelingsmodule die door de PKI van de groep BNP Paribas wordt gebruikt om haar handtekeningsleutels aan te maken en te gebruiken (voor de aanmaak van elektronische certificaten, CRL's) en om de sleutelparen van de houders aan te maken, moet voldoen aan de volgende veiligheidseisen:

- de vertrouwelijkheid en de integriteit van de private handtekeningsleutels van de CA waarborgen tijdens hun volledige levenscyclus en hun veilige vernietiging garanderen aan het einde van hun levensduur;
- in staat zijn om de gebruikers te identificeren en te authenticeren;
- de toegang tot haar diensten beperken naargelang de gebruiker en de rol die hem werd toevertrouwd;
- in staat zijn om een reeks testen uit te voeren om na te gaan of de module correct werkt en overschakelen naar een veilige status als er een fout wordt gedetecteerd;
- de mogelijkheid bieden om een beveiligde elektronische handtekening aan te maken om de door de CA aangemaakte certificaten te ondertekenen, die de private sleutels van de CA niet onthult en die niet kan worden vervalst zonder kennis van die private sleutels;
- auditregistraties aanmaken voor elke wijziging met betrekking tot de veiligheid;
- de vertrouwelijkheid en de integriteit van de opgeslagen gegevens waarborgen en ten minste een dubbele controle van de back-up- en herstelverrichtingen eisen.

XI.B. Eisen voor de kwalificatie

De versleutelingsmodule die door de PKI van de groep BNP Paribas wordt gebruikt, is niet gekwalificeerd volgens het proces dat wordt beschreven in de Référentiel Général de Sécurité van de Franse administratie.