Certificate Policy BNP Paribas

Certificate Authority

BNP Paribas Group PDF Certification Authority

BNP Paribas Group Level 2 Certification Authority

itg

Herziening		
Naam	Functie	Datum

Goedkeuring		
Naam	Functie	Datum

Versiebeheer			
Versie	Datum	Auteur	Wijzigingen
0.1	18/11/2014	Morpho DSA	Initialisatie document
0.2	29/06/2015	Morpho DSA	Bijwerking
0.3	13/07/2015	Morpho DSA	Bijwerking
0.5	19/01/2016	Cédric SZANIEC	Afwerking van de globale herlezing van de documenten: versie vóór voltooiing door de verschillende contributors
0.6	06/04/2016	Cédric SZANIEC	Samenvoeging van de feedback van de verschillende contributors
0.7	03/05/2016	Cédric SZANIEC	Invoeging van de laatste feedback na de pre-audit
1.0	09/05/2016	Cédric SZANIEC	Versie goedgekeurd door de PMA
1.1	21/06/2016	Cédric SZANIEC	Invoeging van de opmerkingen uit fase 1 van de audit ETSI TS 102 042 : • Toevoegen van V.G.4, IX • Wijzigen van I.A, I.E.4, IV.D.3, IV.I.7, IV.I.8, V.H Correctie van een typfout van III.A.3, IV.J.2, IV.L, VI.B.3
2.0	14/09/2016	Cédric SZANIEC	Correctie van een deel van de afwijkingen van de audit ETSI TS 102 042: • Verandering van OID • Wijziging van I.B, IX.C.1

Inhoudstafel

I. Inleiding

I.A. Algemene presentatie

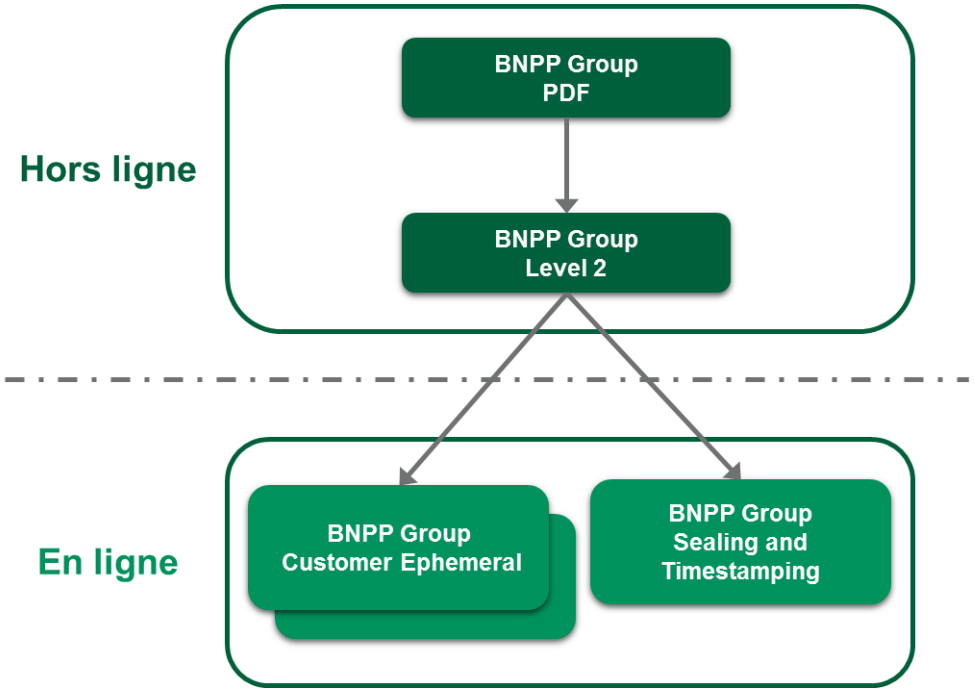
Dit document vormt het Certificate policy (CP) van de Certificate Authority (CA) root van BNP Paribas genaamd BNP Paribas Group PDF Certification Authority (« BNPP PDF CA » in de rest van het document) en de tussenliggende CA genaamd BNP Paribas Group Level 2 Certification Authority (« BNPP LEVEL2 CA » in de rest van het document).

in het kader van de uitgifte van elektronische certificaten voor CA van een lager niveau van de keymanagement infrastruktuur.

Dit document beschrijft welk eisenniveau de Certificate Authority « BNPP PDF CA » en « BNPP LEVEL2 CA » willen naleven en in stand houden bij de uitgifte, het beheer van de levenscyclus en de publicatie van de certificaten.

Het is gebaseerd, als een documentaire kader, op de aanbevelingen van de ETSI TS 102 042.

Dit Certificate policy voldoet aan de eisen van de 'Normalized Certificate Policy' (NCP) zoals bepaald in de norm ETSI TS 102 042. Dit is de NCP OID: 0.4.0.2042.1.1.



I.B. Identification du document

Benaming van het document « Certificate Policy – Root en intermediate autoriteit van de BNP Paribas PKI».

OID-nummer van dit Certificate policy:

- BNPP PDF CA : 1.2.250.1.62.10.1.1.1.1
- BNPP LEVEL2 CA : 1.2.250.1.62.10.2.1.1.1

Neerlegging van de OID-tak van BNP Paribas : {iso(1) member-body(2) fr(250) type-org(1) BNP Paribas(62)} Signel (10) Autorités BNPP PDF & LEVEL2 CA (1 ou 2) Politique de Certification(1) Gabarit de Certificat(1) Version(1)

Geldig voor de certificaten uitgegeven vanaf 08 september 2015.

I.C. Entiteiten die interveniëren in de PKI

I.C.1. Certificate Authority

De Certificate Authority « BNPP PDF CA » en « BNPP LEVEL2 CA » zijn 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).

De diensten "BNPP PDF CA" en "BNPP LEVEL2 CA" zijn het resultaat van functies die overeenkomen met de verschillende stadia van de levenscyclus van sleutelparen en certificaten (zie hieronder)

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.

Alle functies die de PKI van BNP Paribas (als technische dienst) verzorgt, worden uitgevoerd door de informaticadienst van Safran I&S.

De verklaring met betrekking tot de certificatiepraktijk (Certificate Practice Statement of CPS) zoals toegepast door de in dit document opgenomen autoriteiten beschrijft de operationele organisatie van de PKI en de rolverdeling tussen de verschillende componenten volgens de functionele organisatie en de definitie van de in dit beleid beschreven rollen (zie hoofdstuk **Error! Reference source not found.**).

a) Offline Certificate Authority

De autoriteiten "BNPP PDF CA" en " BNPP LEVEL2 CA " zijn een PKI component die over een platform beschikken die hem toelaten certificaten voor een lager niveau CA uit te geven en te beheren.

a) Online Certificate Authority

Het gaat om certificaat autoriteiten van het laagste niveau van business die gekoppeld zijn aan de autoriteit « BNPP LEVEL2 CA ».

I.C.2. Certificaathouders

a) CA « BNPP PDF CA »

In het kader van de huidige policy is de certificaathouder de CA « BNPP LEVEL2 CA ».

b) CA « BNPP LEVEL2 CA »

In het kader van de huidige policy is de certificaathouder een certificaatautoriteit van het laagste niveau van de BNP Paribas PKI, ook genoemd « **online autoriteit** ».

I.C.3. Certificaatoperator

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

De rol van certificaatoperator wordt opgenomen door Safran I&S, dat wordt bijgestaan door zijn partner Colt voor de rol van host. Alle functies die niet rechtstreeks worden verzorgd door Safran I&S, worden overgenomen door Colt, waarvan de verantwoordelijkheden tegenover Safran I&S contractueel worden beschreven. Alle functies onder de verantwoordelijkheid van Colt worden gedocumenteerd door deze onderneming. Sommige informatie is vertrouwelijk en voor de verspreiding van deze informatie is de voorafgaande goedkeuring van de stakeholders vereist.

I.C.4. Certificaatgebruikers

In de huidige policy die certificaten van certificaatautoriteiten behandelt, kan een certificaatgebruiker zijn:

- Een application service die de certificaat autoriteiten "BNPP PDF CA" en " BNPP LEVEL2 CA" erkent en op basis van een controle-apparaat het geleverde certificaat controleert en de certificaatketting van een houder van het certificaat uitgegeven door de instantie.
- Elke klant van BNPP die wenst de certificaat keten van de autoriteit(en) te controleren die zijn certificaat uitgegeven heeft.

I.D. Gebruik van de certificaten

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

Deze policy richt zich op de sleutelparen en certificaten van de categorieën houders die zijn vastgesteld in hoofdstuk I.C.2 zodat deze houders kunnen:

- Certificaten tekenen met hun Certificate Authority certificaat ten behoeve van hun eigen houders

- Intrekkingslijsten (CRL's) tekenen

I.D.2. Sleutelparen en certificaten van de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA »

De autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA » genereren en tekenen verschillende types objecten: certificaten en intrekkingslijsten (CRL's).

Om deze objecten te ondertekenen, hebben ze elk een uniek sleutelpaar. Dit sleutelpaar en het bijbehorende certificaat worden niet gebruikt voor encryptie doeleinden of voor authenticatie doeleinden.

I.E. Beheer van het Certificate policy

I.E.1. Entiteit die het Certificate policy beheert

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

I.E.2. Contactpersoon

Voor alle vragen over dit Certificate policy moet de klant contact opnemen met zijn gebruikelijke adviseur of de kantoordirecteur (niveau 1), via het postadres van zijn kantoor, dat hij makkelijk kan terugvinden op het internet, met name via zijn beveiligde ruimte.

Als zijn adviseur niet beschikbaar is, kan de klant ook contact opnemen met het klantenrelatiecentrum (Centre de Relation Client of CRC) op het nummer 0 820 820 001 (0,12 euro/min + gesprekskosten).

Als de adviseur (kantoor of CRC) en/of de kantoordirecteur geen antwoord kunnen geven of als de klant geen voldoening krijgt, wordt de klacht ter behandeling doorgegeven aan de core business Klachten van de betrokken regionale directie (niveau 2).

Als de klant meent dat het antwoord/de behandeling nog altijd niet toereikend is, kan hij contact opnemen met de Bemiddelingsdienst Banken (niveau 3).

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
- **CRL** : Liste de Certificats Révoqués
- **DN** : Distinguished Name
- **DPC** : Déclaration des Pratiques de Certification
- **IGC** : Infrastructure de Gestion de Clés
- **OID** : Object Identifier
- **PC** : Politique de Certification
- **RGS** : Référentiel Général de Sécurité
- **RSA** : Rivest Shamir Adleman
- **URL** : Uniform Resource Locator

Public Key Infrastructure (PKI ou IGC)	Geheel van fysieke componenten, procedures en software om de levenscyclus van de certificaten te beheren en authenticatie-, versleutelings- en handtekeningdiensten aan te bieden.
Certificat	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.
Autorité de Certification	Dienst die is belast met de ondertekening, de uitgifte en het onderhoud van de certificaten van een public key infrastructure,

(AC ou CA)	overeenkomstig een Certificate policy. Softwarediensten voor het beheer van de certificaten uitgegeven door de Certificate Authority van de certificaathouder.
Politique de certification (PC)	Een reeks regels en eisen die een Certificate Authority moet naleven bij het organiseren en het verstrekken van haar diensten.
Déclaration des pratiques de certification (PC)	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 het Certificate policy dat zij moet naleven.
Liste de révocation des Certificats (CRL ou LCR)	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.
Bi-clé	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 het 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 richten de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 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 autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA » publiceren de volgende informatie voor de certificaathouders en -gebruikers:

- dit Certificate policy;
- de lijsten met ingetrokken certificaten;
- de geldige certificaten van de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA ».

ITP ITG houdt de verschillende vereiste formulieren voor het beheer van de certificaten (registratieaanvraag, intrekkingsaanvraag enz.) ter beschikking van de entiteiten.

II.C. Publicatietermijnen en -frequenties

De publicatietermijnen en -frequenties zijn afhankelijk van de betreffende 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 root CA altijd coherent blijven.
- Voor informatie over de status van de certificaten verwijzen we naar § **Error! Reference source not found.**.
- 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 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).

Merk op dat het verlies van integriteit van informatie (aanwezigheid van de informatie en inhoudelijke integriteit) wordt beschouwd als onbeschikbaarheid van deze informatie; de bovenstaande eisen zijn dan van toepassing op dezelfde manier.

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 structuur van de DN bevat de gebruiksnaam van het certificaat in de PKI van BNP Paribas. De contrôle van de informatie gebeurt tijdens de Key Ceremony door de technische operatoren van de PKI.

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

Naast de hierboven beschreven regels zijn er geen andere eisen vastgelegd.

III.A.5. Uniciteit van namen

Om de unieke identificatie van de houder in de PKI van BNP Paribas te garanderen en elke dubbelzinnigheid te vermijden, kan in het veld 'subject' van elk houdercertificaat een unieke identificatie voor het gebruik van het certificaat in de PKI worden vermeld.

De uniciteit van een certificaat is gebaseerd op het unieke karakter van het serienummer gedefinieerd door de CA. Er moet echter vermeden worden dat er ambiguïteit kan zijn omtrent het bezit van een certificaat door de uniciteit van eenzelfde naam binnen dezelfde CA te garanderen.

Die uniciteit wordt gewaarborgd door de eis die in alinea **Error! Reference source not found.** wordt beschreven.

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.

III.B. Oorspronkelijke goedkeuring van de identiteit

De identificatie van de online certificaatautoriteiten is beschreven in de overeenkomstige CPS.

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

a) « BNPP PDF CA »

Waneer het zijn sleutelpaar genereert, genereert het eveneens een zelfgetekend certificaat.

b) « BNPP LEVEL2 CA »

Waneer het zijn sleutelpaar genereert, moet het aan de root autoriteit een bewijs van bezit leveren van zijn privésleutel die overeenkomt met de publieke sleutel vervat in de certificaataanvraag.

c) Voor de online autoriteiten

Waneer ze hun sleutelpaar genereren, moeten ze aan de autoriteit « BNPP LEVEL2 CA » een bewijs van bezit leveren van zijn privésleutel die overeenkomt met de publieke sleutel vervat in de certificaataanvraag.

Dit bewijs is technisch geleverd door het doorgeven aan de autoriteit « BNPP LEVEL2 CA » van een certificate request of CSR (Certificate Signing Request), in het formaat PKCS#10.

III.B.2. Goedkeuring van de identiteit van een organisme

Cf. §III.B.3.

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

De validatie gebeurt intern in BNP Paribas en komt van de directie van ITP ITG.

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

Niet van toepassing.

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

Deze stap wordt uitgevoerd tijdens een Key Ceremony waargenomen door een BNP Paribas Security Officer.

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. Identification et validation pour un renouvellement après révocation

Als de privésleutel van een certificaatautoriteit gecompromitteerd is, is er een goedkeuring nodig van de ITP ITG directie om een nieuw sleutelpaar te genereren.

Als het certificaat van een van de CA's ingetrokken is dan mag er geen certificaatvernieuwing plaatsvinden. Dan moet de CA nieuwe sleutels genereren.

III.D. Identificatie en goedkeuring van een intrekkingsaanvraag

De goedkeuring van een intrekkingsaanvraag van een Certificate Authority komt slechts uitzonderlijk voor.

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

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

IV. Operationele eisen voor de levenscyclus van de certificaten

IV.A. Certificaataanvraag

IV.A.1. Herkomst van een certificaataanvraag

Een certificaat kan enkel worden aangevraagd door een persoon par une personnegemachtigd door ITP ITG.

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

In de certificaataanvraag moet minstens de volgende informatie worden vermeld (zie hoofdstuk **Error! Reference source not found.**):

- te certificeren gegevens, inclusief de DN;
- de publieke sleutel;
- het bewijs voor het bezit van de private sleutel.
- Identificatiegegevens van de betreffende certificatie autoriteit.

IV.B. Behandeling van een certificaataanvraag

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

De identiteit van de aanvrager wordt gecontroleerd overeenkomstig de eisen in hoofdstuk **Error! Reference source not found.**.

Een getuige, a minima, bevestigt de conformiteit van de aanvraag voor de aanmaak van elk autoriteitcertificaat van de PKI van BNP Paribas.

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

Deze krijgt concreet vorm door een proces verbaal van de Key Ceremony.

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

De behandelingstermijn is variabel want hij is afhankelijk van het erk dat nodig is om de ontvankelijkheid van de aanvraag te realiseren.

De duurtijd van de opstelling van het certificaat is afhankelijk van het verloop van de key ceremony

IV.C. Aflevering van het certificaat

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

Na de authenticatie van de herkomst en de controle van de integriteit van de aanvraag start de autoriteit « BNPP PDF CA » en « BNPP LEVEL2 CA » in haar hoedanigheid van technische dienst met de processen voor de aanmaak van het certificaat.

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

Na de ceremonie, als er geen afwijkingen werden gemeld op het certificaat, wordt deze officieel overhandigd aan ITG ITP, in de vorm van een bestand op een portable mediadrager.

IV.D. Aanvaarding van het certificaat

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

ITP ITG aanvaardt het certificaat formeel dat geleverd is tijdens de Key Ceremony door het ceremonieregister te tekenen. Geen bezwaar kan na de ceremonie worden ontvangen om de acceptatie van het certificaat te annuleren.

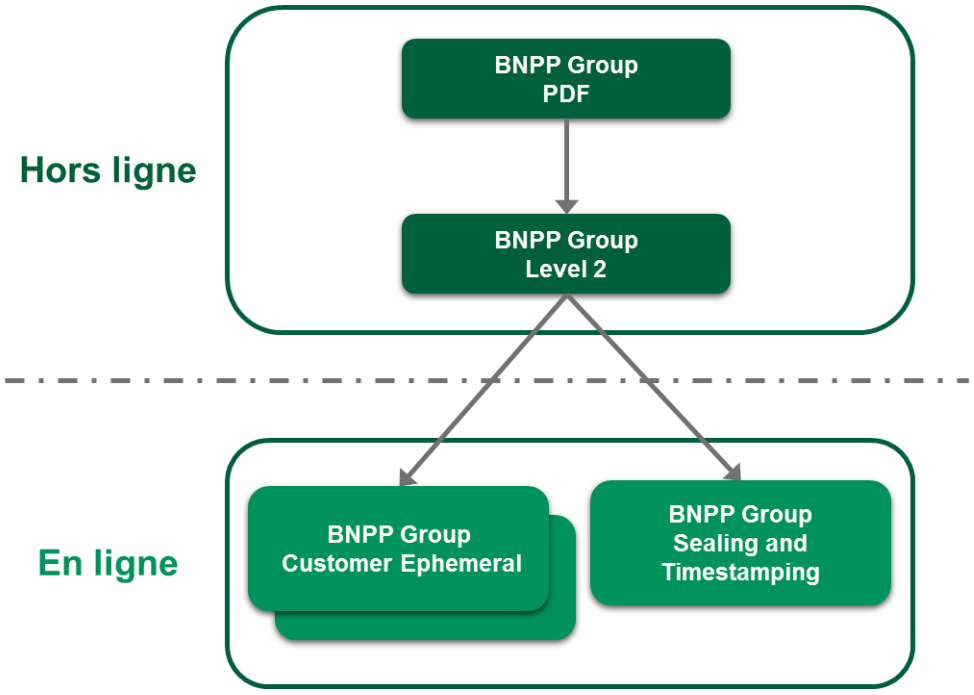
IV.D.2. Publicatie van het certificaat

Deze informatie moet toegankelijk zijn vanaf het internet.

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

La notification de la délivrance du certificat s'effectue durant la cérémonie des clés.

IV.E. Gebruik van het sleutelpaar en het certificaat



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

Dans la suite du document, l'autorité de certification BNPP Group Customer Epheremal sera nommée « BNPP Instant CA » et l'autorité de certification BNPP Group Sealing and Timestamping sera nommée « BNPP Service CA ».

L'utilisation de la clé privée est limitée à :

Het gebruik van de private sleutels van de autoriteiten "BNPP PDF CA" en "BNPP LEVEL2 CA" en de bijbehorende certificaten is strikt beperkt tot de ondertekening van CA-certificaten en de ondertekening van de lijst van ingetrokken certificaten.

Het toegestane gebruik van het sleutelpaar en bijbehorende certificaat wordt ook aangegeven in het certificaat zelf, met behulp van uitbreidingen op de belangrijkste gebruik.

In de rest van het document, zal de CA BNP Paribas Group Customer Epheremal worden genoemd "BNPP Instant CA" en CA BNPP Group Sealing and Timestamping zal worden genoemd "BNPP CA Service CA".

Het gebruik van de private sleutel is beperkt:

a) Voor de certificate authority « BNPP Instant CA » :

- De ondertekening van handtekeningscertificaten voor BNP Paribas klanten
- De ondertekening van de lijst van ingetrokken certificaten.

b) Voor de certificate authority « BNPP Service CA » :

- De ondertekening van handtekeningscertificaten in naam van BNP Paribas of van haar dochterondernemingen.
- De ondertekening van timestamping certificaten in nam van BNP Paribas.
- De ondertekening van de lijst van ingetrokken certificaten.

IV.E.2. Utilisation de la clé privée et du certificat par l'utilisateur du certificat

Les certificats délivrés par les autorités « BNPP PDF CA » en « BNPP LEVEL2 CA » ne peuvent être utilisés par un utilisateur qu'à des fins de validation d'une chaîne de confiance comprenant le certificat de celle-ci.

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

De certificaten geleverd door de autoriteiten "BNPP PDF CA" en "BNPP LEVEL2 CA" kunnen uitsluitend worden gebruikt door een gebruiker voor de validatie van een vertrouwde keten die het certificaat zelf bevat.

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

IV.G.1. Mogelijke oorzaken van een verandering van een sleutelpaar

De sleutelparen moeten worden veranderd:

- om de recentste versleutelingsontwikkelingen te volgen, en in het bijzonder de aanbevelingen van het Franse ANSSI, en cryptoaanvallen zo veel mogelijk te vermijden;
- als het certificaat van een van de certificaatautoriteiten vervalt;
- bij (vermoedelijke) schending, diefstal of verlies van de middelen voor de reconstructie van de private sleutel van een van de certificaatautoriteiten.

In al die gevallen kan voor elke PKI van BNP Paribas een nieuw autoriteitcertificaat worden afgeleverd.

Ten slotte moet bij een verandering van een sleutelpaar het certificaat dat met het oude sleutelpaar overeenstemt, worden ingetrokken (zie §**Error! Reference source not found.**).

IV.G.1. Herkomst van een aanvraag van een nieuw certificaat

Een nieuw certificaat wordt aangevraagd onder dezelfde voorwaarden als in alinea IV.A.

IV.G.2. Procedure voor de behandeling van een aanvraag voor een nieuw certificaat

De behandeling van een certificaataanvraag na de verandering van een sleutelpaar is hetzelfde als de behandeling beschreven in alinea. **Error! Reference source not found.**.

IV.G.3. Kennisgeving aan de houder van de opstelling van het nieuwe certificaat

Zie hoofdstuk IV.C.2.

IV.G.4. Proces voor de aanvaarding van het nieuwe certificaat

Zie hoofdstuk IV.D.

IV.G.5. Publicatie van het nieuwe certificaat

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

IV.G.6. Kennisgeving van de aflevering van een nieuw certificaat

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

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, zie § **Error! Reference source not found.**).

In dit beleid zijn geen certificaatwijzigingen toegestaan.

IV.I. Intrekking en opschorting van de certificaten

IV.I.1. Mogelijke oorzaken van een intrekking

Voor een online en offline certificaatautoriteit, zijn de oorzaken van intrekking de volgende:

- stopzetting van de handelsactiviteit gekoppeld aan de Certificate Authority;
- (vermoedelijke) schending, diefstal of verlies van de middelen voor de reconstructie van de private sleutel;
- niet-conformiteit vastgesteld tijdens een audit.

IV.I.2. Herkomst van een intrekkingsaanvraag

Alleen ITP ITG is gemachtigd om een intrekkingsaanvraag in te dienen..

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

De intrekking van een van de certificaten moet gebeuren via een sleutelceremonie.

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

Bij een (vermoedelijke) schending van de private sleutel van een online of offline Certificate Authority vraagt ITP ITG onmiddellijk om het certificaat in te trekken.

IV.I.5. Behandelingstermijn van een intrekkingsaanvraag

Intrekkingsaanvragen moeten worden behandeld bij ontvangst door de overeenkomstige autoriteit tijdens de Key Ceremony.

De intrekking wordt binnen 24 uur na ontvangst van de aanvraag behandeld.

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

Niet van toepassing.

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

De frequentie van de publicatie van de CRL van de offline autoriteiten is 1 jaar. De CRL van de offline autoriteiten overlapt over een periode van één maand: de volgende CRL heeft een vervaldatum die kleiner is dan een maand voor de vervaldatum van de huidige CRL.

In het uitzonderlijke geval van een herroeping, zal de CRL onmiddellijk worden bijgewerkt (cf. § **Error! Reference source not found.**).

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

Een CRL moet binnen 8 uur 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, ongeacht van de publikatie op ARL Internet en van de certificaten (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

Als er andere middelen voorhanden zijn, zal dat in de CPS staan.

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

Intrekking ten gevolge van een compromis van de private sleutel moet duidelijk verspreid worden als informatie in ieder geval op de website van BNP Paribas.

IV.I.13. Mogelijke oorzaken van een opschorting

De opschortng van certificaten is niet toegelaten in de huidige CP.

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

IV.J.1. Operationele kenmerken

De functie voor informatie over de status van de certificaten stelt de certificaatgebruikers een mechanisme voor de vrije raadpleging van CRL's ter beschikking.

De ARL's van de rootautoriteit zijn in formaat V2, in http toegankelijk via de URL: **http://bnpp.digitaltrust.morpho.com/crl/bnpp-sealing-and-timestamping-ca.crl**

- « BNPP PDF CA » :
  http://bnpp.digitaltrust.morpho.com/crl/bnpp-pdf-ca.crl
- « BNPP LEVEL2 CA » :
  http://bnpp.digitaltrust.morpho.com/crl/bnpp-level2-ca.crl

Die informatie is toegankelijk via het internet.

IV.J.2. Beschikbaarheid van de functie

Informatie over de status van de certificaten is beschikbaar gesteld door de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA » met een maximale onbeschikbaarheid zoals beschreven in §II.C.

Het beschikbaarheidspercentage is minimum 99,7%, 24/7.

IV.K. Einde van de relatie met de houder

Zie hoofdstuk IV.I voor de mogelijke oorzaken van een intrekking.

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 offline autoriteiten (BNPP PDF CA & BNPP Level 2 CA) moeten naleven. 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

Niet van toepassing aangezien de CA offline zijn.

V.A.3. Stroomvoorziening en klimaatregeling

Niet van toepassing aangezien de CA offline zijn.

V.A.4. Kwetsbaarheid voor waterschade

Niet van toepassing aangezien de CA offline zijn.

V.A.5. Brandpreventie en -bescherming

Niet van toepassing aangezien de CA offline zijn.

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 CPS identificeert de opslagmogelijkheden.

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 het 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 het 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.
- **Porteurs de secret:**
    - De porteur de secret beheerder maakt de beveiligingscontext van de toegang tot de behuizing;
    - De porteur de secret operator neemt deel aan de creatie en activatie van het sleutelpaar van de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA » in de veiligheidscontext van de porteur de secret beheerder.

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.

De CPS van de rootautoriteit preciseert de activiteiten waarvoor de tussenkomst van verschillende mensen nodig is en wat de beperkingen zijn die deze mensen moeten respecteren (posities in de organisatie, de hiërarchische structuur, etc.).

Erkend wordt dat dezelfde persoon meerdere rollen kan vervullen. De verdeling is gedefinieerd in de CPS.

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.

De porteurs de secret

De porteurs de secret houden nooit de minimale quorum van hetzelfde geheim.

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 (CO) 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.

Relevante documenten betekent:

- het Certificate policy;
- de verklaring met betrekking tot de certificatiepraktijk;
- de interne procedures;
- de technische documenten met betrekking tot de gebruikte hardware en software.

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 § 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 BNP Paribas houdt logbestanden bij voor de offline certificaatautoriteiten :

- PKI applikatieve gebeurtenissen:
  - ontvangst van een certificaataanvraag (eerste aanvraag en vervanging);
  - goedkeuring/afwijzing van een certificaataanvraag;
  - gebeurtenissen verbonden aan de handtekeningsleutels en de certificaten van de CA (aanmaak (sleutelceremonie), bewaring, herstel, intrekking, vernieuwing, vernietiging enz.);
  - aanmaak van de certificaten van de houders;
  - ontvangst van een intrekkingsaanvraag;
  - goedkeuring/afwijzing van een intrekkingsaanvraag;
  - aanmaak en publicatie van CRL's.

- Andere gebeurtenissen:
  - de fysieke toegangen;
  - het onderhoud en de wijzigingen in de configuratie van de systemen;
  - de veranderingen in het personeel;
  - Publicities en bijwerkingen in verband met de autoriteit (PC, certificaatautoriteiten, voorwaarden, etc.).

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

- Bestemmeling van de operatie
- naam van de uitvoerder of het aanspreekpunt van het systeem dat de gebeurtenis in gang zet;
- naam van de aanwezigen (in het geval van een operatie waarbij meerdere personen nodig zijn)
- Reden van de gebeurtenis
- Alle informatie mbt het karakteriseren van de gebeurtenis (bijvoorbeeld voor het genereren van een certificaat, het serienummer van het certificaat)

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

De inhoud van de gebeurtenissenlogboeken moet regelmatig worden geanalyseerd door de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA » bij elk certificaathandtekening of CRL.

V.D.3. Bewaringsperiode van de gebeurtenissenlogboeken

De gebeurtenissenlogboeken worden bewaard tot het einde van de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA ».

V.D.4. Bescherming van de gebeurtenissenlogboeken

De logging is ontworpen en geïmplementeerd om zo de risico's van ontwijking, wijziging of vernietiging van gebeurtenislogs te beperken.

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

De PKI van 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.6. Verzamelsysteem van de gebeurtenissenlogboeken

De PKI van 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

Zie het overeenkomstige hoofdstuk in de CPS.

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.

V.E. Archivering van de gegevens

V.E.1. Te archiveren gegevenstypes

Procedures en instrumenten laten toe om de volgende gegevens te archiveren:

- Certificaten van de offline autoriteiten
- Certificaat van de online autoriteiten, geldig en ingetrokken
- Event logs, zie §V.D
- Software en configuratie-bestanden voor de verschillende componenten
- Alle nuttige elementen voor registratie of intrekking:
    - Receipts
    - intrekkingsaanvragen en hun resultaten
- Key Ceremony Records
- Scripts van de ceremonies
- Revocation Lists

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

Zie het overeenkomstige hoofdstuk in de CPS.

V.E.3. Bewaringsperiode van het archief

De archieven worden bewaard tot het einde van de levenscyclus van de BNP Paribas PKI.

Op dezelfde manier worden de papiergegevens bewaard tot het einde van de levenscyclus van de PKI.

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

Zie het overeenkomstige hoofdstuk in de CPS.

V.E.7. Verzamelsysteem van het archief

Zie het overeenkomstige hoofdstuk in de CPS.

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

Het archief wordt beheerd door de PKI van 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 'BNPP Service 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 'BNPP Service 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.

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

In geval van corruptie van IT-middelen tijdens de sleutel ceremonie wordt deze geannuleerd en verplaatst naar een zo snel mogelijk tijdstip.

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, zie § **Error! Reference source not found.**).

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

Bij schending van een algoritme dat is gebruikt in een autoriteitcertificaat: zie het overeenkomstige hoofdstuk in het CP PDF Level 2.

Bij schending van een algoritme dat betrekking heeft op een (tijd)stempelcertificaat, wordt het bijbehorende certificaat ingetrokken (zie § IV.I.5, ifv uitstel van realisatie van Key Ceremony) en wordt er een nieuw certificaat aangemaakt dat het geschonden algoritme niet gebruikt (zie § IV.A).

V.G.5. Bedrijfscontinuïteitsmogelijkheden na schade

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

Voor de autoriteit « BNPP PDF CA » en « BNPP LEVEL2 CA » 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 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.

De stopzetting van de activiteit in deze paragraaf geldt slechts voor de ACR "BNPP PDF CA". Als de ACR ophoudt, zie § V.H.2.

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;
- Archieven overdragen aan de AA;

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 ACR 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 ACR 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

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

De handtekeningsleutels van de autoriteit « BNPP PDF CA » en « BNPP LEVEL2 CA » worden aangemaakt en gebruikt in een cryptobox waarvan de kenmerken worden beschreven in de CPS.

De handtekeningsleutels van de autoriteit « BNPP PDF CA » en « BNPP LEVEL2 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 « BNPP PDF CA » en « BNPP LEVEL2 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 'BNPP Service 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.

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

Private sleutels van de autoriteiten "BNPP PDF CA" en "BNPP LEVEL2 CA" worden uitgezonden in de vorm van gedeelde geheimen tussen verschillende vervoerders BNPP.

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

a) « BNPP PDF CA »

De wijzen van overdracht van de publieke sleutel (zelf-ondertekend certificaat, PKCS # 10, ...) worden gedefinieerd in de certificaataanvraag procedure van paragraaf IV.B.

b) « BNPP LEVEL2 CA »

De wijzen van overdracht van de publieke sleutel (certificaat ondertekend door **« BNPP PDF CA »**,, PKCS # 10, ...) worden gedefinieerd in de certificaataanvraag procedure van paragraaf IV.B.

c) Online certificaat authoriteiten

De wijzen van overdracht van de publieke sleutel (certificaat ondertekend door **« BNPP LEVEL2 CA »**,, PKCS # 10, ...) worden gedefinieerd in de certificaataanvraag procedure van paragraaf IV.B.

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 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

De levensduur van de sleutels is 23 jaar.

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.

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

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

Private sleutels van het PKI-certificaat autoriteiten BNP Paribas (offline of online) zijn beschermd door een cryptografische doos waarvan de weerstand niveau wordt geëvalueerd FIPS 140-2 level 3.

De behuizing die gebruikt wordt door CA "BNPP PDF CA" en "BNPP LEVEL2 CA" is niet gekwalificeerd door ANSSI.

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

De controle van de prviate keys van de CA moet verzekerd worden door vertrouwd personeel (PKI porteurs de secret) en door middel van een instrument ter uitvoering van geheimen delen (systemen waarbij n exploitanten van m moeten authenticeren, met n ten minste 2).

De directie van ITP ITG duidt deze porteurs de secret aan.

VI.B.3. Escrow van de private sleutel

De private sleutels (tijdstempel en handtekeningstempel) van alle BNP Paribas PKI autoriteiten worden in geen geval in escrow gegeven.

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

De back-up van de sleutels verbonden aan de autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA », wordt gemaakt door gebruik te maken van de specificaties van de cryptobox.

Het proces wordt beschreven in de CPS.

VI.B.5. Archivering van de private sleutel

De private sleutels van alle BNP Paribas PKI autoriteiten worden in geen geval gearchiveerd.

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

Zie VI.B.4.

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

Private sleutels van de PKI autoriteit van BNP Paribas (root of ondergeschikte) worden opgeslagen tijdens hun activering, in een cryptografische module minstens voldoet aan de eisen van hoofdstuk XI hieronder.

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

De activering van de private sleutel van alle CA BNP Paribas PKI in een cryptografische module moet worden geregeld via de activering van gegevens en moet ten minste n van m personen betrekken genoemd in overeenkomstige vertrouwensrollen.

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

Het uitschakelen van private sleutels van een CA BNP Paribas PKI in een cryptografische module dient automatisch te geschieden zodra de moduleomgeving verandert: stoppen of uitschakeling van de module, ontkoppeling van de technische operator van de PKI, etc.

Deactiveren van de private sleutel van een CA BNP Paribas PKI gebruikt in een ceremonie om de sleutels en het genereren van sleutelpaar en certificaat wordt onmiddellijk uitgevoerd na het gebruik van de toets.

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

De werkwijze van de vernietiging van de private sleutel van een CA voor de BNP Paribas PKI moet toestaan te beantwoorden aan de in hoofdstuk XI gestelde eisen.

Op het levenseinde van een CA BNP Paribas PKI, normaal of geanticipeerd (intrekking), wordt deze sleutel systematisch vernietigd, evenals alle kopieën en alle elementen die zouden toelaten om hem te reconstrueren.

Dit wordt alleen op verzoek van de directie van ITP ITG uitgevoerd.

VI.B.11. Veiligheidsevaluatieniveau van de versleutelingsmodule

Cryptografische modules van een CA BNP Paribas PKI worden geëvalueerd op het niveau dat overeenkomt met het beoogde gebruik, zoals omschreven in hoofdstuk XI hieronder.

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

VI.C.1. Archivering van de publieke sleutels

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

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

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

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 zjin gekend enkel door de verantwoordelijkengeïdentificeerd in het kader van de hen toevertrouwde rollen (cf. hoofdstuk V.B.1).

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 BNP Paribas, worden beschermd tot de uitgifte aan de ontvanger.

De ontvanger van de bepaalde actie stuurt deze naar de boot manager, die vervolgens de verantwoordelijkheid heeft de vertrouwelijkheid, integriteit en beschikbaarheid erover te garanderen.

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

Zie het overeenkomstige hoofdstuk in de CPS.

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

Niet van toepassing.

VI.E. Veiligheidsmaatregelen voor de informaticasystemen

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

Zie het overeenkomstige hoofdstuk in de CPS.

VI.E.2. Kwalificatieniveau van de informaticasystemen

De versleutelingsmodule die wordt gebruikt door de PKI van 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 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 autoriteiten « BNPP PDF CA » en « BNPP LEVEL2 CA » zijn offline.

VI.A. Tijdstempel/dateringssysteem

Er is geen tijd stempel in de PKI, maar een datering-systeem waarvan de omschrijving wordt gegeven in de CPS.

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 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 autoriteit 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 volgende alinea.

VII.A.3. Extensies van het certificaat

De certificaten die worden uitgegeven door de offline autoriteiten van de PKI van BNP Paribas, 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
Key Usage	O	Beschrijving van het toegestane gebruik van de private sleutel: digitalSignature
Certificate Policies	N	OID van het CP dat van toepassing is op het certificaat 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
Certificate Policy	N	Het adres waar alle CP zijn gepubliceerd
CRL Distribution Points	O	De adressen waar de CRL wordt afgegeven door de autoriteit die het certificaat heeft afgegeven, behalve voor "BNPP PDF CA"

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 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 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 BNP Paribas voldoen aan de norm X.500, zoals beschreven in hoofdstuk III.A van dit document.

VII.A.6. OID van het Certificate policy

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

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 het 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 CRLX.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 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-inputextensie

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
Reason Code	Identificeert de oorzaak van de intrekking van het certificaat. De waarde voor elke intrekking is 'unspecified' en wordt dus niet vermeld.

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 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 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

Niet van toepassing.

IX.B. Financiële aansprakelijkheid

Niet van toepassing voor offline certificaatautoriteiten.

IX.C. Vertrouwelijkheid van de professionele gegevens

IX.C.1. Scope van de vertrouwelijke gegevens

Minstens de volgende gegevens worden als vertrouwelijk beschouwd:

- het niet-publieke deel van de CPS voor dit CP;
- de private sleutels van de componenten en de houders van certificaten van de PKI van BNP Paribas;
- de activeringsgegevens gekoppeld aan de private sleutels van de autoriteiten van de PKI van BNP Paribas;
- alle geheime codes van de PKI van BNP Paribas;
- de gebeurtenissenlogboeken van de componenten van de PKI van BNP Paribas;
- het registratiedossier van de houders;
- het verslag van de sleutelceremonie.

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 is er als autoriteit toe gehouden om de geldende wetgeving en regelgeving op het Franse grondgebied na te leven.

IX.D. Bescherming van de persoonsgegevens

BNP Paribas leeft de regelgeving over de persoonsgegevens na, zowel voor de verzameling als voor het gebruik van de persoonsgegevens.

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

Er wordt overeengekomen dat de persoonsgegevens door de componenten van de PKI van BNP Paribas worden verzameld en gebruikt met strikte naleving van de geldende wetgeving en regelgeving op het Franse grondgebied, en in het bijzonder de wet [CNIL].

IX.D.2. Persoonsgegevens

Minstens de volgende gegevens worden als persoonlijk beschouwd:

- de registratiedossiers van de verschillende rollen (aanspreekpunten, certificaatbeheerder enz.).

IX.D.3. Niet-persoonsgegevens

Er worden hierover geen specifieke eisen gesteld.

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

Zie geldende wetgeving en regelgeving op het Franse grondgebied.

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

Overeenkomstig de geldende wetgeving en regelgeving op het Franse grondgebied mogen de aan de CA meegedeelde persoonsgegevens noch worden verspreid noch worden overgedragen aan derden, behalve in de volgende gevallen: voorafgaande toestemming, rechterlijke beslissing of andere wettelijke machtiging.

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

Zie geldende wetgeving en regelgeving op het Franse grondgebied.

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

Zie geldende wetgeving en regelgeving op het Franse grondgebied.

IX.E. Intellectuele en industriële eigendomsrechten

Toepassing van de geldende wetgeving en regelgeving op het Franse 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 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

De CA moet garanderen dat haar CPS coherent is en blijft met haar CP.

IX.F.2. Registratiedienst

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

IX.F.3. Certificaathouders

In het geval van autoriteitcertificaten hebben de certificaathouders de volgende verplichtingen:

- juiste en bijgewerkte informatie meedelen bij de aanvraag of de vernieuwing van het certificaat;
- de private sleutel van het certificaat waarvoor zij verantwoordelijk zijn, beschermen met aan hun omgeving aangepaste middelen;
- de activeringsgegevens van die private sleutel beschermen en ze eventueel gebruiken;
- de gebruiksvoorwaarden van de private sleutel en het overeenkomstige certificaat naleven;
- de CA op de hoogte brengen van elke wijziging in de informatie in het elektronisch certificaat;
- onverwijld een intrekkingsaanvraag indienen voor het elektronisch certificaat waarvoor zij verantwoordelijk zijn bij de RA of de CA bij (vermoedelijke) schending van de overeenkomstige private sleutel (of activeringsgegevens).

IX.F.4. Certificaatgebruikers

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

IX.F.5. Andere deelnemers

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

IX.G. Waarborglimiet

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

IX.H. Aansprakelijkheidslimiet

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

IX.I. Vergoedingen

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

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. Effekt van de beëindiging van de geldigheid en overblijvende toepasbare clausules

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

IX.K. Individuele kennisgevingen en communicatie tussen de deelnemers

Er worden hierover geen 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 Franse grondgebied.

IX.N. Conformiteit met de wetgeving en regelgeving

Toepassing van de geldende wetgeving en regelgeving op het Franse 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 FIP 140-2 level 3 van de cryptobox Thales nShield

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 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 BNP Paribas wordt gebruikt, is niet gekwalificeerd volgens het proces dat wordt beschreven in de Référentiel Général de Sécurité van de Franse administratie.