Certificate policy BNP Paribas

Certificate Authority

BNP Paribas Group Sealing and Timestamping CA

itg

Herziening		
Naam	Functie	Datum

Goedkeuring		
Naam	Functie	Datum

Follow-up van de versies

Versie	Datum	Auteur	Aard van de wijzigingen
0.1	06.07.2015	Morpho DSA	Redactie van het document
0.2	17.07.2015	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: • Toevoeging van V.G.4, IX • Wijziging van I.A, I.E.4, IV.B.3, V.H • Onderscheid tussen certificaathouders en -autoriteiten bij VI.B • Correctie van een drukfout bij III.A.3, IV.J.2 • Correctie van IV.C.2, IV.D.2, IV.D.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, IX.J, VI.B.8 en VI.B.9

Inhoud

I. Inleiding

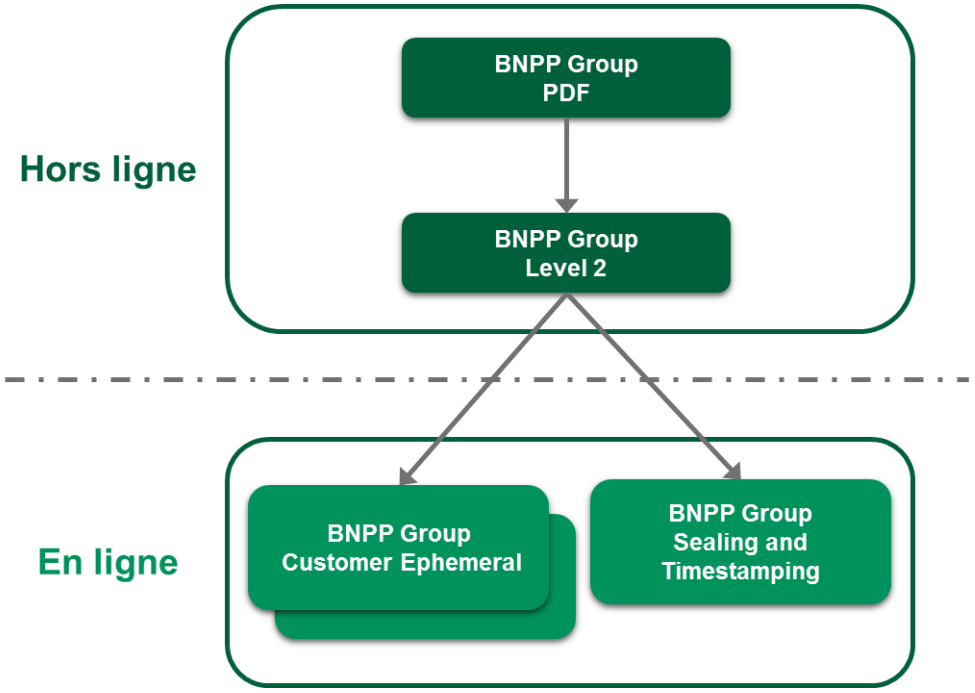
I.A. Algemene presentatie

Dit document vormt het Certificate policy (CP) van de Certificate Authority 'BNP Paribas Group Sealing and Timestamping CA' ('BNPP Service CA' in de rest van het document) in het kader van de uitgifte van elektronische certificaten voor klanten van BNP Paribas, om te gebruiken als handtekening van een entiteit (ook handtekeningstempel genoemd), en voor BNP Paribas, om te gebruiken als tijdstempel.

Dit document beschrijft welk eisenniveau de Certificate Authority wil naleven en in stand houden bij de uitgifte, het beheer van de levenscyclus en de publicatie van de certificaten.

Het is louter een documentair referentiekader en berust op de aanbevelingen van het Franse Agence nationale de la sécurité des systèmes d'information (ANSSI), de Franse Direction générale de la modernisation de l'État (DGME) en het Europees Telecommunicatie en Standaardisatie Instituut (ETSI).

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. Identificatie van het document

Benaming van het document: 'Certificate policy – Certificate Authority voor entiteiten van BNP Paribas'.

OID-nummer van dit Certificate policy:

- Entiteitcertificaat of serverstempel: 1.2.250.1.62.10.5.1.1.1
- Tijdstempel: 1.2.250.1.62.10.5.1.2.1

Neerlegging van de OID-tak van BNP Paribas: {iso(1) member-body(2) fr(250) type-org(1) BNP Paribas(62)} Signel(10) 'BNPP Service CA'(5) Certificate policy(1) Certificaatmodel(1 of 2) Versie(1).

Geldig voor de certificaten uitgegeven vanaf 23 september 2016.

I.C. Entiteiten die interveniëren in de PKI

I.C.1. Certificate Authority

De Certificate Authority 'BNPP Service 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.

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.

I.C.2. Registratieautoriteit (RA)

De RA heeft de opdracht om de identiteit van de toekomstige certificaathouder en de vereisten voor het gebruik van het aan de houder afgeleverde certificaat te controleren in overeenstemming met het Certificate policy. De RA moet worden erkend door de CA van de PKI waarvoor ze certificaat- en intrekkingsaanvragen uitgeeft.

I.C.3. Certificaathouders

Een certificaathouder is:

- ofwel een toepassing van de klant van BNP Paribas die uitsluitend wordt gebruikt voor de ondertekening van documenten in naam van die klant;
- ofwel een tijdstempeleenheid ingesteld door BNP Paribas. Een tijdstempeleenheid is een hardware- en softwaregeheel dat tijdswaarmerken aanmaakt die worden gekenmerkt door een ID van de tijdstempeleenheid zoals toegekend door de tijdstempelautoriteit van BNP Paribas en een unieke handtekeningsleutel met tijdswaarmerken.

I.C.4. 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.5. Certificaatgebruikers

De gebruikers zijn de entiteiten van BNP Paribas die ondertekende documenten uitgeven in hun hoedanigheid van rechtspersoon.

Daarnaast worden de certificaten gebruikt voor de uitgifte van tijdswaarmerken.

I.C.6. Andere deelnemers

a) Voor een entiteitcertificaat van BNP Paribas

De certificaatbeheerder staat rechtstreeks in contact met de vragende entiteit. Hij verricht voor de entiteit een aantal controles betreffende de identiteit en, eventueel, de gegevenskenmerken van de houders van de entiteit.

De aanvragende entiteit moet voor elke entiteit een of twee aanspreekpunten aanstellen die zijn gemachtigd om contact op te nemen met de certificaatbeheerder voor de aanvraag van een handtekeningcertificaat voor de entiteit.

b) Voor een tijdstempelcertificaat van BNP Paribas

De certificaatbeheerder van BNP Paribas controleert of de certificaataanvragen van de tijdstempeleenheden coherent zijn.

I.D. Gebruik van de certificaten

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

a) Voor een entiteitcertificaat van BNP Paribas

De houders maken alleen elektronische handtekeningen aan voor het gebruik dat contractueel werd bepaald tussen de partijen, en maken daarbij gebruik van de producten van Safran I&S.

Het handtekening- en handtekeningcontrolebeleid kan worden geraadpleegd op het volgende adres:

http://bnpp.digitaltrust.morpho.com/psv.html

b) Voor een tijdstempelcertificaat van BNP Paribas

De houders maken alleen tijdswaarmerken aan overeenkomstig RFC 3161.

Het tijdstempelbeleid voor deze certificaten kan worden geraadpleegd op het volgende adres:

http://bnpp.digitaltrust.morpho.com/ph.html

I.D.2. Sleutelparen en certificaten van de autoriteit 'BNPP Service CA'

De autoriteit 'BNPP Service CA' geeft alleen zogenaamde handtekeningcertificaten voor entiteiten uit (ook stempels genoemd) voor klanten van BNP Paribas of tijdstempelcertificaten voor BNP Paribas en CRL's.

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
- **ANSSI :** Agence nationale de la sécurité des systèmes d'information
- **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	Geheel van fysieke componenten, procedures en software om de

(PKI ou IGC)	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 (AC ou 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.
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 richt de autoriteit 'BNPP Service 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 'BNPP Service CA' publiceert de volgende informatie voor de certificaathouders en -gebruikers:

- dit Certificate policy;
- de lijsten met ingetrokken certificaten;
- de geldige certificaten van de autoriteiten 'BNPP Service 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

- 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 tijdelijke 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 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 structuur van de DN bevat de gebruiksnaam van het certificaat in de PKI van BNP Paribas. De technische operatoren van de PKI controleren de informatie.

Voor de serverstempel moet de klant van BNP Paribas in het veld CN (Common Name) van zijn aanvraag een betekenisvolle naam vermelden die verband houdt met zijn toepassingsdienst, en dus bijvoorbeeld een keuze maken uit de volgende mogelijkheden:

- zijn handelsnaam;
- de naam van een van zijn dochtermaatschappijen;
- de naam van een van zijn commerciële aanbiedingen.

Als de voorgestelde naam dubbelzinnig of betwistbaar is, bijvoorbeeld een bestaand gedeponeerd handelsmerk, dan moet de naam worden voorafgegaan door de handelsnaam van de klant.

Elke tijdstempeleenheid wordt 'Timestamp Unit' genoemd, met als achtervoegsel een oplopend nummer dat door BNP Paribas wordt beheerd.

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.

Die uniciteit wordt gewaarborgd door de eis die in alinea III.A.2 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

ITP ITG is de enige entiteit die is gemachtigd om de aanmaak van een entiteit- of tijdstempelcertificaat aan te vragen.

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

De aanvraag van een certificaat in het formaat PKCS #10 aangemaakt door de technische RA wordt ondertekend op basis van de bijbehorende private sleutel, terwijl het sleutelpaar wordt aangemaakt door de HSM van de technische RA.

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

Elke entiteit moet minstens één aanspreekpunt aanstellen (zoals vermeld in § I.C.6) om een handtekeningcertificaat voor de entiteit te kunnen verkrijgen.

Het aanspreekpunt moet de goedkeuring van zijn management krijgen en mag alleen een interne medewerker van de groep BNPP zijn. De contactgegevens van het aanspreekpunt (naam, voornaam, e-mail, UID) en de hiërarchische goedkeuring van zijn statuut moeten aan het team van SIGNEL worden meegedeeld zodat zij de rechtmatigheid van de aan hen gerichte aanvragen kunnen valideren.

Ten slotte is de entiteit verantwoordelijk voor het up-to-date houden van de lijst met haar aanspreekpunten. Zo moet ze communiceren over het vertrek (bv. mobiliteit, langdurige afwezigheid) van de medewerker-aanspreekpunt om zijn machtigingen in te trekken.

De aanvraag van een handtekeningcertificaat voor de entiteit moet worden goedgekeurd door de CISO (Chief Information Security Officer) van de betrokken entiteit zodat de certificaatbeheerder de aanvraag kan indienen bij de beheerder van de PKI.

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

a) Voor een entiteitcertificaat voor een klant van BNP Paribas

Alleen de certificaatbeheerder is gemachtigd om de aanmaak van een entiteitcertificaat aan te vragen.

b) Voor een tijdstempelcertificaat van BNP Paribas

Alleen de certificaatbeheerder is gemachtigd om de aanmaak van een tijdstempelcertificaat aan te vragen.

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

Niet van toepassing.

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

a) Voor een entiteitcertificaat voor een klant van BNP Paribas

De certificaatbeheerder mag zijn aanvraag pas indienen nadat het (de) aanspreekpunt(en) een aanvraag heeft (hebben) ingediend overeenkomstig § III.B.2.

b) Voor een tijdstempelcertificaat van BNP Paribas

De goedkeuring van de aanvrager wordt bevestigd bij de ondertekening van het formulier voor de aanvraag van het tijdstempelcertificaat.

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.

Voor een verandering van sleutelpaar verwijzen we naar § IV.G.

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

Bij een certificaatintrekking wegens (vermoedelijke) schending, verlies of diefstal van de sleutel, moeten nieuwe sleutels worden aangemaakt. Dan moet dezelfde authenticatieprocedure worden gevolgd als bij een eerste registratie overeenkomstig § III.B.3.

Als het certificaat om een andere reden wordt ingetrokken (wijziging van de informatie in het certificaat, intrekking van de Certificate Authority enz.) moeten ook nieuwe sleutels worden aangemaakt. De authenticatie van de gebruiker verloopt volgens dezelfde procedure als bij de eerste certificaataanvraag.

III.D. Identificatie en goedkeuring van een intrekkingsaanvraag

a) Voor een Certificate Authority

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.

b) Voor de eindentiteit

Een certificaat uitgegeven door de autoriteit 'BNPP Service CA' wordt ingetrokken via een formulier door:

- voor een entiteitcertificaat:
  - de certificaatbeheerder na een bijzondere gebeurtenis;
  - de operator van de PKI bij contractbreuk;
- voor een tijdstempelcertificaat: de certificaatbeheerder na een bijzondere gebeurtenis.

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 de certificaatbeheerder in het kader van de handelsactiviteit van de vennootschap.

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

In de certificaataanvraag moet minstens de volgende informatie worden vermeld (zie hoofdstuk III.B):

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

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 III.B.

De certificaatbeheerder bevestigt de conformiteit van de aanvraag voor de aanmaak van elk entiteitcertificaat.

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

De aanvaarding krijgt concreet vorm door de installatie van het certificaat op de handtekening- of tijdstempelservers van BNP Paribas.

De afwijzing krijgt concreet vorm door een elektronisch bericht waarin de reden voor de weigering wordt vermeld.

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

De maximale behandelingstermijn is 24 uur na ontvangst en goedkeuring 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 de authenticatie van de herkomst en de controle van de integriteit van de aanvraag start de autoriteit 'BNPP Service 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

De beheerder van de PKI brengt de certificaatbeheerder op de hoogte van het goede verloop van de verrichting.

IV.D. Aanvaarding van het certificaat

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

ITP ITG aanvaardt het certificaat formeel door de overeenstemming van het certificaat met het aanvraagformulier te controleren.

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

a) Voor een entiteitcertificaat van BNP Paribas

Het gebruik van de private sleutel van BNP Paribas voor een entiteit is strikt beperkt tot de ondertekening van documenten.

Het toegestane gebruik van het sleutelpaar en het bijbehorende certificaat staat trouwens vermeld in het certificaat zelf, via de extensies over het gebruik van de sleutels.

b) Voor een tijdstempelcertificaat van BNP Paribas:

Het gebruik van de private sleutel door een tijdstempeleenheid is strikt beperkt tot de aanmaak van tijdstempelwaarmerken overeenkomstig RFC 3161.

Het toegestane gebruik van het sleutelpaar en het bijbehorende certificaat staat trouwens vermeld in het certificaat zelf, via de extensies over het gebruik van de sleutels.

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

De certificaatgebruikers moeten het toegestane gebruik van de certificaten strikt naleven. Anders worden zij aansprakelijk gesteld.

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 de autoriteit 'BNPP Service CA' vervalt;

- bij (vermoedelijke) schending, diefstal of verlies van de middelen voor de reconstructie van de private sleutel van de autoriteit 'BNPP Service CA'.

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 § IV.I).

IV.G.2. Herkomst van een aanvraag van een nieuw certificaat

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

IV.G.3. 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 IV.B.

IV.G.4. Kennisgeving aan de houder van de opstelling van het nieuwe certificaat

Zie hoofdstuk IV.C.2.

IV.G.5. Proces voor de aanvaarding van het nieuwe certificaat

Zie hoofdstuk IV.D.1.

IV.G.6. Publicatie van het nieuwe certificaat

Zie hoofdstuk IV.D.2.

IV.G.7. Kennisgeving van de aflevering van een nieuw certificaat

Zie hoofdstuk IV.D.3.

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 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

Voor de eindcertificaten uitgegeven door de autoriteit 'BNPP Service CA' zijn dit de intrekkingsoorzaken:

- 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.

De certificaatbeheerder kan in het daartoe bestemde formulier de reden van de intrekkingsaanvraag verduidelijken:

- verlies;
- schending;
- disfunctie;
- stopzetting van de inproductiename.

IV.I.2. Herkomst van een intrekkingsaanvraag

Alleen de certificaatbeheerder is gemachtigd om een intrekkingsaanvraag in te dienen.

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

Een entiteit- of tijdstempelcertificaat van BNP Paribas wordt ingetrokken door de beheerteams van Safran I&S onder toezicht van ITP ITG.

Bij de intrekking van een van de certificaten in de certificaatketen via een sleutelceremonie brengt BNP Paribas al haar klanten zo snel mogelijk en via alle kanalen (en indien mogelijk op voorhand) op de hoogte.

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

Bij een (vermoedelijke) schending van de private sleutel van een Certificate Authority, de handtekeningdienst of de tijdstempeldienst van BNP Paribas vraagt ITP ITG na bevestiging van het risico om het certificaat in te trekken.

IV.I.5. Behandelingstermijn van een intrekkingsaanvraag

Intrekkingsaanvragen moeten worden behandeld bij ontvangst door de overeenkomstige autoriteit.

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

Om de 24 uur en meteen na de intrekking van een certificaat 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.

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

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

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

Die informatie is toegankelijk via het internet.

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.J.3. Optionele systemen

Niet van toepassing.

IV.K. Einde van de relatie met de houder

Als er om de een of andere reden een einde komt aan de relatie tussen de CA en de houder vóór het verstrijken van de geldigheid van het certificaat moet het certificaat worden ingetrokken.

Zie hoofdstuk IV.I.1 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 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 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.

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 (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 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 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;
- 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 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 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 BNP Paribas wordt er een back-up van de gebeurtenissenlogboeken gemaakt.

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

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

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.

Ook de papieren gegevens worden vijf 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 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.

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 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) 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 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 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

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

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 'BNPP Service CA' worden aangemaakt en gebruikt in een cryptobox waarvan de kenmerken worden beschreven in de CPS.

De handtekeningsleutels van de autoriteit 'BNPP Service 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 Service 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.

b) Sleutels van de houders

De sleutels van entiteit- en tijdstempelcertificaten worden door het personeel van Safran I&S aangemaakt op versleutelingsmiddelen (HSM) met inachtneming van een specifieke daartoe bestemde procedure. Die door auditors gecontroleerde methodologie maakt het mogelijk om de vertrouwelijkheid en de integriteit van de sleutels te garanderen.

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 sleutels worden aangemaakt op een versleutelingsmiddel (HSM) zodat de sleutels nooit uit het middel weggaan en de vertrouwelijkheid en de integriteit dus beschermd blijven.

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. 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.

De overdrachtvormen van de publieke sleutel (certificaat ondertekend door de CA 'BNPP Service CA' PKCS #10 enz.) worden bepaald in de procedure voor de aanvraag van een certificaat zoals vermeld in alinea 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 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 § 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.

Voor de certificaten van de houders, zie § I.D.1.

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 (tijdstempel en handtekeningstempel) worden in geen geval 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 back-up van de sleutels verbonden aan de (tijd)stempelcertificaten die door de handtekeningdiensten van BNP Paribas worden gebruikt, 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

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 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 XIhierna 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

Niet van toepassing.

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

Niet van toepassing.

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

De sleutels worden vernietigd wanneer het certificaat dat aan de sleutelparen is gekoppeld, is vervallen.

VI.B.11. Veiligheidsevaluatieniveau van de versleutelingsmodule

a) Autoriteitsleutels

De versleutelingsmodules van een CA van de PKI van BNP Paribas worden geëvalueerd op een niveau dat overeenstemt met het beoogde gebruik, zoals beschreven in § 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 BNP Paribas worden gearchiveerd in het kader van de archivering van de overeenkomstige certificaten.

b) 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 eindcertificaat:

- Voor het tijdstempelcertificaat van een eenheid: 12,5 jaar;
- voor het stempelcertificaat: 3 jaar.

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 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 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 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 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 Certificate Authority 'BNPP Service CA' 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

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.

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.B.3. 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. 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

Bij afwijkingen tussen gekochte/gebruikte licenties in het nadeel van de dienstverlener kunnen wij aangeven dat BNPP daadwerkelijk en overeenkomstig het ondertekende contract met de dienstverlener financieel aansprakelijk blijft en de situatie zo snel mogelijk in orde moet brengen. De dienstverlener mag echter een schadeloosstelling eisen.

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

IX.F.3. Certificaathouders

Voor entiteit- of tijdstempelcertificaten 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.1.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.