



**Registratiebeleid en Verklaring**  
**Registratiepraktijken BNP Paribas Fortis**  
Registratieautoriteit  
Van de certificaatautoriteit LuxTrust Corporate CA

itg



Herziening		
Naam	Functie	Datum

Validatie		
Naam	Functie	Datum
PMA	Governance-instantie	21/12/21

Follow-up van de versies			
Versie	Datum	Auteur	Aard van de wijzigingen
0.4.1	23/09/2020	Sealweb	Redactie van het document
0.4.2	21/10/2020	Sealweb	Afronding van het document voor validatie
0.4.3	07/11/2020	Sealweb	Rekening houden met de laatste opmerkingen van Worldline
0.4.4	19.11.2020	Sealweb	Rekening houden met de feedback van Fortis
1.0.0	13/10/2021	ITA	Interne herziening, rekening houdend met de opmerkingen van Legal BNP Paribas Fortis <ul style="list-style-type: none"> <li>Wijziging van I.A, 1.E.4, V.E.3, V.D.3</li> </ul>
1.1	28/10/2021	ITA	Rekening houden met de opmerking van de juridische afdeling van BNP Paribas Fortis naar aanleiding van de PMA: <ul style="list-style-type: none"> <li>Wijziging V.E.3</li> </ul>
1.2	15/12/2021	MBA	Rekening houden met de opmerking van de interne audit van SealWeb <ul style="list-style-type: none"> <li>Wijziging van hoofdstuk IV.C.2</li> </ul> [Gevalideerd door de PMA van 21 december 2021]
1.3	9/09/2022	GFE	Wijziging volgt op: <ul style="list-style-type: none"> <li>nieuwe kanalen: EBA, EBBM</li> <li>nieuw token: Easy PIN (Gemalto) in EBA, EBBM</li> <li>itsme autorisatiemiddel</li> <li>wijziging in veld OF van het certificaat</li> <li>onderscheid scherm layout Web &amp; Mobile</li> </ul>
1.4	01/04/2023	RZE	Update voor de overdracht van de activiteit van Worldline naar Worldline France bij de migratie van de PKI "Mediacert Root CA 2018" (en AC 2019) naar "Mediacert Root CA 2021" Update obv de opmerkingen van Worldline en de wijziging in de OID's van Mediacert's 2021 CA OTU (inwerkingtreding op 17 februari 2022 voor Worldline France/Mediacert): wijziging van 1.2.250.1.111.20.5.5 naar 1.2.250.1.111.20.5.6
Versies vanaf migratie naar LuxTrust			
2.0	20/03/2024	SEALED	Document update in context van de migratie naar LuxTrust Corporate CA
2.1	10/04/2024	YNU & GFE	Review
2.3	15/04/2024	SEALED	Laatste review voor integratie feedback van YNU & GFE
2.4	30/04/2024	SEALED	Update V.B.1 roles
2.5	20/05/2025	SEALED	Update V.B.1 roles: add "Registration operator"
2.6	10/10/2025	GFE	Update XI.A: add "Isakey"

## Inhoudsopgave

I.	Inleiding .....	6
I.A.	Algemene presentatie .....	6
I.B.	Identificatie van het document .....	6
I.C.	Entiteiten die interveniëren in de PKI .....	7
I.D.	Gebruik van de certificaten .....	11
I.E.	Beheer van het beleid van dit RP and RPS.....	11
I.F.	Definities en afkortingen .....	12
II.	Verantwoordelijkheden in verband met de terbeschikkingstelling van de te publiceren informatie .....	15
II.A.	Entiteiten belast met de terbeschikkingstelling van de informatie .....	15
II.B.	Te publiceren informatie .....	15
II.C.	Publicatietermijnen en -frequenties .....	16
II.D.	Controle op de toegang tot de gepubliceerde informatie .....	16
III.	Identificatie en authenticatie .....	16
III.A.	Naamgeving.....	16
III.B.	Oorspronkelijke goedkeuring van de identiteit.....	18
III.C.	Goedkeuring van de autoriteit van de aanvrager .....	19
III.D.	Identificatie en goedkeuring van een aanvraag voor de vernieuwing van de sleutels .....	20
III.E.	Identificatie en goedkeuring van een intrekkingaanvraag .....	20
IV.	Operationele eisen voor de levenscyclus van de certificaten .....	20
IV.A.	Herkomst van een certificaataanvraag .....	20
IV.B.	Proces en verantwoordelijkheden voor de opstelling van een certificaataanvraag.....	20
IV.C.	Behandeling van een certificaataanvraag .....	20
IV.D.	Aflevering van het certificaat.....	21
IV.E.	Aanvaarding van het certificaat .....	21
IV.F.	Gebruik van het sleutelbaar en het certificaat .....	22
IV.G.	Vernieuwing van een certificaat.....	22
IV.H.	Aflevering van een nieuw certificaat na een verandering van het sleutelbaar .....	22
IV.I.	Wijziging van het certificaat .....	23
IV.J.	Intrekking en opschorting van de certificaten .....	23
IV.K.	Functie voor informatie over de status van de certificaten .....	24
V.	Niet-technische veiligheidsmaatregelen.....	24
V.A.	Fysieke veiligheidsmaatregelen .....	24

V.B.	Veiligheidsmaatregelen voor de procedures .....	24
V.C.	Veiligheidsmaatregelen tegenover het personeel .....	25
V.D.	Procedures voor de verzameling van auditgegevens .....	27
V.E.	Archivering van de gegevens .....	28
V.F.	Verandering van sleutel van de autoriteit .....	29
V.G.	Hervatting na schending en schade .....	30
V.H.	Einde levensduur RA .....	30
VI.	Technische veiligheidsmaatregelen .....	30
VI.A.	Aanmaak en installatie van sleutelparen .....	30
VI.B.	Veiligheidsmaatregelen voor de bescherming van de private sleutels en voor de versleutelingsmodules.....	31
VI.C.	Andere aspecten van het beheer van de sleutelparen .....	32
VI.D.	Activeringsgegevens.....	32
VI.E.	Veiligheidsmaatregelen voor de informaticasystemen .....	33
VI.F.	Veiligheidsmaatregelen voor de ontwikkeling van de systemen .....	33
VI.G.	Veiligheidsmaatregelen voor het netwerk.....	33
VI.H.	Tijdstempel/dateringssysteem .....	33
VII.	Profielen van de certificaten, OCSP en CRL's .....	34
VIII.	Conformiteitsaudit en andere evaluaties .....	34
VIII.A.	Frequentie en/of omstandigheden van de evaluaties.....	34
VIII.B.	Identiteit/kwalificaties van de evaluators .....	34
VIII.C.	Relaties tussen evaluators en geëvalueerde entiteiten .....	34
VIII.D.	Onderwerpen die in de evaluaties aan bod komen .....	34
VIII.E.	Ondernomen acties op grond van de conclusies van de evaluaties .....	34
VIII.F.	Mededeling van de resultaten.....	34
IX.	Andere kwesties in verband met het metier en de wetgeving.....	35
IX.A.	Tarieven.....	35
IX.B.	Financiële aansprakelijkheid.....	35
IX.C.	Vertrouwelijkheid van de professionele gegevens .....	35
IX.D.	Bescherming van de persoonsgegevens .....	35
IX.E.	Intellectuele en industriële eigendomsrechten .....	36
IX.F.	Contractuele interpretaties en waarborgen .....	36
IX.G.	Certificaatgebruikers .....	37
IX.H.	Andere deelnemers .....	37
IX.I.	Waarborglimiet.....	37

IX.J.	Aansprakelijkheidslimiet .....	37
IX.K.	Schadevergoeding .....	37
IX.L.	Duur en vervroegde beëindiging van de geldigheid van het PE .....	37
IX.M.	Wijzigingen in het PE .....	38
IX.N.	Bepalingen betreffende conflictoplossing .....	38
IX.O.	Bevoegde rechtbanken .....	38
IX.P.	Conformiteit met de wetgeving en regelgeving .....	38
IX.Q.	Diverse bepalingen .....	38
IX.R.	Andere bepalingen .....	38
X.	Bijlage – Referentiedocumenten .....	38
X.A.	Regelgeving .....	38
X.B.	Technische documenten .....	39
XI.	Bijlage: Registratieprocedures – authenticatie en toelating aanvaard onder dit RB .....	39
XI.A.	Procedure op basis van EMV-kaart voor retailklant .....	40

## I. Inleiding

### I.A. Algemene presentatie

Dit document beschrijft het Registratiebeleid (RP) en de Verklaring Registratiepraktijken (RPS) die van toepassing zijn op de klantencertificaten van de Fortis-entiteit van BNP Paribas.

- **uitgegeven door de certificatie-autoriteit 'LuxTrust Corporate CA' ('CA' verder in dit document) die optreedt als verlener van certificatiediensten,**
- **om tegemoet te komen aan de vertrouwensbehoeften van zakelijke toepassingen (in het bijzonder in het geval van gedematerialiseerde banktoepassingen).**

Dit Registratiebeleid en de Verklaring Registratiepraktijken (hierna 'RP' en 'RPS' genoemd) heeft betrekking op de uitgifte van certificaten voor elektronische handtekeningen van documenten in PDF-, XML- (XAdES, XML-dig) of CMS-formaat.

De autoriteit 'CA' geeft certificaten uit de klanten van BNP Paribas Fortis, gebruikers van persoonlijke certificaten.

De RP en RPS maken deel uit van een proces voor de certificatie van de conformiteit van de registratievereisten en -praktijken met de Europese norm ETSI EN 319 411-1 niveau NCP+ met als doel:

- **De verbintenissen van de registratieautoriteit 'FORTIS RA' met betrekking tot de bepaling van de uitgifte-regels en het beheer van de certificaten uitgegeven door de CA, alsook de toepassing ervan**
- **De gebruiksvoorwaarden van de certificaten uitgegeven door de CA uitgegeven voor rekening van BNP Paribas FORTIS, geregistreerd en aangevraagd door de 'FORTIS RA'.**

De RP en RPS voldoen aan de eisen van de « Extended Normalized Certificate Policy » (NCP+) zoals bepaald in de norm ETSI EN 319 411-1. Dit is de OID NCP+: 0.4.0.2042.1.2.

Het gaat ook om:

- **Te voldoen aan de registratievereisten opgelegd aan RA LuxTrust (OID 1.3.171.1.1.10) zoals beschreven in de LuxTrust Corporate CA (CP) geïdentificeerd onder OID 1.3.171.1.1.1.10.4.5 en conform aan standaard EN 319 411-1/NCP<sup>1</sup>**
- **Te voldoen aan de registratievereisten van het programma Adobe AATL**

### I.B. Identificatie van het document

Deze RP en RPS worden geïdentificeerd aan de hand van de Object ID (OID, footer op elke pagina van dit document). Het kan ook worden geïdentificeerd aan de hand van specifiekere elementen zoals de naam, het versienummer en de bijwerkingsdatum.

OID van dit registratiebeleid

1.3.171.1.1.10

<sup>1</sup> Beschikbaar op: <https://www.luxtrust.com/fr/repository>

## **I.C. Entiteiten die interveniëren in de PKI**

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

- **Certificaatautoriteit (CA)**
- **Registratieautoriteit (RA)**
- **Certificaathouders**
- **Gebruikende applicatie (applicatie voor de ondertekening van documenten die BNP Paribas Fortis ter beschikking stelt van haar klanten)**
- **PMA (Policy Management Authority): governance-instantie van de handtekeningdienst van BNP Paribas en van AE Fortis.**

Het gebruik zoals bepaald in het PE vereist geen escrowfuncties.

'CA' verwijst naar een Certificaatbeheerder voor het beheer van zijn PKI, met name als interface met de Operator.

In het kader van de functies voor de levering van certificatediensten 'CA' die ze rechtstreeks uitvoert, is 'CA' een externe dienst van BNP Paribas. In het kader van de gebruiken delegeert ze echter een aantal verantwoordelijkheden aan BNP Paribas Fortis. In het bijzonder verbindt BNP Paribas Fortis, wettelijke entiteit in de zin van de Belgische wetgeving, zich ertoe de volgende vereisten na te leven:

- **Een contractuele relatie die wordt of zal worden onderhouden met de eindklanten waarvoor zij de volgende taken vervult:**
  - o **De uitgifte en het beheer van de certificaten op basis van de openbare sleutelinfrastructuur (PKI) van 'CA'.**
  - o **de bepaling, voor de perimeter van de voor BNP Paribas uitgegeven certificaten, van de regels voor de registratie van de houders met het oog op de uitgifte van de certificaten uitgegeven door de CA en de correcte toepassing ervan;**
  - o **De bepaling van de gebruiksvoorwaarden van de certificaten uitgegeven door de CA voor rekening van BNP Paribas Fortis**

### **I.C.1. Certificaatautoriteit**

De certificaatautoriteit '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).

Het geheel van de functies die door de PKI worden uitgeoefend, is beschreven in de CP van de CA.

### **I.C.2. Registratieautoriteit (RA)**

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

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

Ze moet de procedures voor de identificatie van natuurlijke personen toepassen om certificaten uit te geven

volgens een procedure die in overeenstemming is met:

- **de Belgische bankregelgeving, en met name de regelgeving ter voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme (Wet van 18 september 2017 ter voorkoming van het witwassen van geld en de financiering van terrorisme en en tot beperking van het gebruik van contanten;**
- **Registratie verplichtingen opgelegd door RA LuxTrust;**
- **Registratie verplichtingen opgelegd door Adobe AATL.**

De registratieprocedure voor de certificaten uitgegeven door de CA voor BNP Paribas Fortis verloopt in twee stappen, zoals hierna beschreven. De eerste stap wordt slechts eenmaal uitgevoerd en is een voorwaarde voor de volgende stap.

### 1) **Stap 1: Registratie**

Deze eerste stap wordt slechts eenmaal uitgevoerd wanneer de natuurlijke persoon een relatie aangaat met de bank.

Hij bestaat uit 3 elementen:

- **Stap REG 1.1** De samenstelling van een identiteitsdossier van de natuurlijke persoon en de bewaring van de door hem verstrekte identiteitsbewijzen (vereiste **REG1** zoals geïdentificeerd in document [1]). Deze documenten worden elektronisch gearhiveerd. De geldigheid ervan wordt in de loop van de tijd behouden in overeenstemming met de Belgische bankreglementering. Alle bewijzen van identiteitsdocumenten worden bewaard in het bankarchief, dat ter beschikking wordt gesteld van alle bankkantoren BNP Paribas Fortis
- **Stap REG 1.2** De controle of de in 1.1 verzamelde identiteitsgegevens wel degelijk toebehoren aan de persoon die zich aanmeldt als klant van de bank of volmachthebber (vereiste **REG2** zoals geïdentificeerd in document [1]). De controle van de identiteitsgegevens op basis van bewijsstukken overeenkomstig de regelgeving die van toepassing is op kredietinstellingen. Hij wordt uitgevoerd tijdens een face-to-facegesprek of gelijkwaardig met een van de middelen beschreven in III.B.3 Wanneer de identificatiegegevens worden gecontroleerd, tijdens het face-to-facegesprek met de klant, wordt een acceptatieproces opgestart om klant of gevolmachtigde van de bank te worden.
- **Stap REG 1.3** De toewijzing of identificatie van een sterk authenticatiemiddel dat de persoon zal gebruiken om zich te authenticeren (**AUTH**) en/of zijn toestemming te geven (**SAS**) tijdens zijn volgende contacten met de gebruikende applicatie (vereiste **REG2** zoals geïdentificeerd in document [1]).  
Het moet gaan om een authenticatiesysteem (**AUTH**) dat gebruikmaakt van de door de bank erkende authenticatiemethodes met een hoog niveau van zekerheid over de identiteit van de persoon.

Document [4] definieert de vereisten voor authenticatie (**AUTH**) en/of zijn toestemming te geven (**SAS**), identificeert en analyseert de conformiteit van de middelen gebruikt door de bank voor deze vereisten.

*De authenticatiemiddelen die in het kader van dit RB worden aanvaard, zijn:*

- *de intelligente bankkaart (EMV-standaard) waarmee u zich kunt authenticeren met het M1-protocol door middel van een UCR-lezer, via een beveiligd kanaal tussen de klant en de bank (EBW, EBB)*
- *de Isabel-kaart (geleverd door BNP Paribas Fortis of een andere bank) waarmee u zich kunt authenticeren via een certificaat en een kaartlezer, via een beveiligd kanaal tussen de klant en de bank (EBB).*
- *het itsme-systeem, waarmee u zich kunt authenticeren via een beveiligd kanaal tussen de klant en de bank (EBW, EBB)*
- *het Easy PIN-systeem (Gemalto), waarmee u zich kunt authenticeren via een beveiligd kanaal tussen de klant en de bank (EBA, EBBM)*
- 

*De aanvaarde toelatingsmiddelen zijn:*

- *de intelligente bankkaart (EMV-standaard) waarmee u kan ondertekenen met het M2-protocol met een UCR-lezer, via een beveiligd kanaal tussen de klant en de bank (EBW).*
- *de Isabel-kaart (geleverd door BNP Paribas Fortis of een andere bank) waarmee u kunt tekenen via een certificaat en een kaartlezer, via een beveiligd kanaal tussen de klant en de bank (EBB).*
- *het itsme-systeem, waarmee u kunt tekenen via een beveiligd kanaal tussen de klant en de bank (EBW, EBB)*
- *het Easy PIN-systeem (Gemalto), waarmee u kunt tekenen via een beveiligd kanaal tussen de klant en de bank (EBA, EBBM)*

De processen voor de activering en het gebruik van de authenticatie- en autorisatiemiddelen en de technische details van die authenticatie- en autorisatiemiddelen worden in detail beschreven in het document [4] en in de bijlage bij dit EP (hoofdstuk XI). Alleen de in dit bijgevoegde document beschreven combinaties van authenticatie- en autorisatiemiddelen zijn toegestaan. Merk op dat bepaalde middelen gebruikt kunnen worden voor authenticatie en autorisatie.

## **2) Stap 2: aanvraag en gebruik certificaat**

Deze tweede stap, die berust op de elementen die in de eerste stap werden geregistreerd, wordt telkens verricht als de natuurlijke persoon een tijdelijk certificaat vraagt, dus telkens wanneer een transactie een handtekening vereist. Ze vereist een sterke authenticatie van de persoon, door middel van een van de authenticatiemethodes die voor die persoon in 1.3 zijn geregistreerd.

Deze stap vindt plaats tijdens het online contractualisatieproces dat gebaseerd is op 2 stappen:

- *de initialisatie van het proces voor onlinecontractualisatie, dat de voorafgaande authenticatie van de klant vereist via een van de authenticatiemiddelen die BNP Paribas Fortis aanvaardt (hierboven opgesomd).*
- *de start van het proces dat het mogelijk maakt om elektronisch te ondertekenen, volgens de vorige stap.*

Deze stap vereist dat de klant de algemene voorwaarden begrijpt die verband houden met het gebruik van de dienst voor elektronische handtekeningen, in het bijzonder het feit dat een handtekeningcertificaat op zijn naam wordt uitgegeven (“certificate acceptance and subscriber agreement” (CAA)-vereisten, zoals deze zijn gepresenteerd in [2]). Daartoe wordt een reeks schermen aan de klant gepresenteerd, die acties van zijn kant vereisen, zoals gepresenteerd in document [3], waarin wordt weergegeven hoe deze schermen en de stappen die worden gegenereerd na de acties van de klant het mogelijk maken om te voldoen aan de eis van standaard ETSI 319 411-1.

De klant gaat akkoord met een of meerdere specifieke documenten die hij moet ondertekenen. Als de klant het bevestigingsvakje aanvinkt, kan hij vervolgens de aanvraag tot ondertekening formaliseren via een van de door BNP Paribas Fortis aanvaarde (hierboven opgesomde) toelatingsmiddelen.

De klant gaat vooraf akkoord met:

- **de AGV van de BNPPF handtekeningdienst en geeft zijn toestemming voor het gebruik van zijn persoonsgegevens voor de uitgifte van een certificaat in zijn naam.**
- **De algemene voorwaarden van CA Luxtrust, via de aanvaarding van de algemene voorwaarden van de BNPPF handtekeningdienst.**

Indien deze aanvraag geldig is, wordt een certificaataanvraag verstuurd naar de technische RA die een certificaat laat genereren op naam van de natuurlijke persoon.

Opmerking 1: als de klant de stap in dit stadium afbreekt, wordt het handtekeningproces geannuleerd. Er wordt geen certificaat aangemaakt;

Opmerking 2: het is ook deze stap die de aanvraag koppelt aan de te ondertekenen gegevens.

Deze stap formaliseert de aanvraag voor de aanmaak van een handtekeningcertificaat.

Vervolgens is er een onderscheid volgens de layout style-schermen:

1) Mobiele layout:

Er is geen verdere stap aangezien de klant in dit scherm al met een vakje "Kennisgenomen te hebben van de 'Gebruiksvoorwaarden van de elektronische handtekeningcertificaten' aangeeft dat alle gegevens correct zijn en dat in het kader van deze voorwaarden een certificaat met zijn naam kan worden aangemaakt".

2) Weblay-out: een tweede autorisatiescherm biedt de natuurlijke persoon de mogelijkheid om zijn toestemming te geven voor de aanmaak van een elektronische handtekening op zijn naam op basis van de identificatiegegevens die op hem betrekking hebben en op het specifieke contractuele document van het certificaat (voornaam en naam zoals voorgesteld op het scherm).

Opmerking 1: de klant kan in deze fase de AGV [6] en de huidige RP/RPS raadplegen, evenals de CP en de AGV Luxtrust [5].

Opmerking 2: de identificatiegegevens van de klant en de overnames van het aangemaakte certificaat worden opnieuw voorgesteld.

Met deze stap kan ook de aanvaarding van het certificaat worden bevestigd en de inhoud ervan worden gevalideerd, in het bijzonder de persoonsgegevens die het bevat.

Dit proces formaliseert de aanvraag voor een elektronische handtekening. Het aangemaakte certificaat wordt vervolgens gebruikt voor de ondertekening van het document dat de klant of mandataris op wettelijke wijze met de Bank verbindt;

### I.C.3. Functionele uitsplitsing van de RA

De PKI van BNP Paribas Fortis implementeert 2 RA-componenten:

- **Een functionele RA: verantwoordelijk voor de initiële identiteitsverificatie van de natuurlijke persoon en de bewaring van de door hem verstrekte identiteitsbewijzen (REG1 en REG2) en de daaropvolgende identiteitsverificatie van de natuurlijke persoon bij elke transactie die aanleiding kan geven tot de uitgifte van een certificaat (AUTH). De functionele RA is verantwoordelijk voor het volgende:**
  - o **De controle-elementen van de certificaathouder bewaren in toepassing van de regelgeving die van toepassing is op de kredietinstellingen.**
  - o **De vertrouwelijkheid en de integriteit van de persoonsgegevens voor de authenticatie van de houder vrijwaren in overeenstemming met de bankregelgeving.****Alle informatie over de vertrouwelijke gegevens wordt opgeslagen in het systeem voor bankarchivering.**
- **Een technische RA: verantwoordelijk voor de aanmaak en de voorlegging van de certificaataanvragen aan de certificaatautoriteit. Ze maakt ook een bewijsbestand aan bij elke ondertekening door de houder.**

#### **I.C.4. Certificaathouder**

In dit registratiebeleid is een certificaathouder een fysieke persoon klant van BNP Paribas Fortis.

#### **I.C.5. Toepassingen die gebruikmaken van certificaten**

Toepassingen die gebruikmaken van certificaten:

- **Een applicatie voor de aanmaak van een elektronische handtekening die BNP Paribas Fortis ter beschikking stellen van de certificaathouder.**
- **Alle software voor de weergave en de goedkeuring van elektronische handtekeningen.**

#### **I.C.6. Policy Management Authority (PMA)**

De PMA is de governance-instantie van de RA van BNP Paribas met als voornaamste opdrachten:

- **Het bepalen, herzien, goedkeuren en doen toepassen van het Registratiebeleid en de Verklaringen van Registratiepraktijken,**
- **Het beheren van alle risico's verbonden aan de RA;**
- **Het definiëren en beheren van het personeel of de vertrouwensentiteit die de RA uitvoert**
- **Het beheren van de relaties met de externe entiteiten, in het bijzonder met de CA OTU**
- **Alle nodige acties ondernemen om ervoor te zorgen dat alle eerder opgesomde taken worden uitgevoerd.**

#### **I.D. Gebruik van de certificaten**

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

Het enige toegelaten gebruik is de persoonlijke handtekening via de waarde 'Non Repudiation' (2.5.29.15).(1)) van de extensie 'Key Usage', zoals gedefinieerd in de CP van de CA.

#### **I.E. Beheer van het beleid van dit RP and RPS**

##### **I.E.1. Entiteit die de RP en RPS beheert**

De entiteit die belast is met de administratie en het beheer van deze RP en RPS is de PMA (Policy Management Authority), governance instantie van de RP in BNPP Fortis. Ze is verantwoordelijk voor de uitwerking, de follow-up en de eventuele wijziging van deze RP en RPS.

Deze RP en RPS wordt gereviewed door de entiteit die de 'CA' Certification Policy beheert om zich ervan te vergewissen dat de verbintenissen van deze RP/RPS wel degelijk afgestemd zijn op die welke beschreven zijn in de CP van de CA. Deze RP/RPS wordt gevalideerd gezamenlijk door de PMA en de CA. Deze RP wordt regelmatig gereviewed door de RA audit (zie VIII).

### **I.E.2. Contactpunt**

Elke persoon (houder, betrokken partijen) die vragen heeft, kan de relevante contacten vinden in de algemene gebruiksvoorwaarden die aan de houder worden voorgelegd bij de aanvraag van het certificaat, of in de CA CP.

### **I.E.3. Entiteit die bepaalt of een DPE aan dit registratiebeleid voldoet**

De PMA (Policy Management Authority), de governance-instantie van de RA, stelt de personen (of departementen) aan die bepalen of de RP en RPS in overeenstemming is met:

- **de registratievereisten die aan RA's van LuxTrust worden opgelegd (OID 1.3.171.1.1.10) zoals beschreven in de LuxTrust Corporate CA CP (geïdentificeerd door OID 1.3.171.1.1.10.4.5)**
- **Norm EN 319 411-1/NCP+**
- **Registratievereisten voor Adobe AATL-programma's**

### **I.E.4. Procedures voor de goedkeuring van de conformiteit van het PE**

Deze RP en RPS zal worden herzien bij elke belangrijke wijziging en minstens jaarlijks door de PMA (Policy Management Authority), de governance-instantie van deze RA, om toe te zien op

- **de conformiteit met de door de nationale controle-instelling verwachte veiligheidsnormen (cf. Europese verordening eIDAS 910/2014)**
- **de vereisten van de CP van de CA**
- **Adobe AATL vereisten**

### **I.F. Definities en afkortingen**

In dit PE worden de volgende afkortingen gebruikt:

- **AV: Archiveringsautoriteit**
- **VI.AC: Certificaatautoriteit**
- **AE: Registratieautoriteit**
- **ANSSI: Nationaal Agentschap voor de Veiligheid van de Informatiesystemen**
- **ADV: Algemene dienstvoorwaarden van TSP Mediacert, in het kader van de elektronische handtekening en uitgifte van Elektronische Certificaten**
- **AGV: Algemene voorwaarden van de Ondertekeningsdienst**
- **ATV: Algemene toetredingsvoorwaarden**
- **CRL: Lijst van ingetrokken certificaten**
- **DN : Distinguished Name**
- **CPS: Verklaring met betrekking tot de certificatiepraktijken**
- **DPE: Verklaring Registratiepraktijken**
- **ETSI: European Telecommunications Standards Institute**
- **PKI: Infrastructuur sleutelbeheer**
- **OID: Object Identifier**

- **OCSP: Online Certificate Status Protocol**
- **PMA: Policy Management Authority**
- **PC: Certificatiebeleid**
- **PE: Registratiebeleid**
- **RGS : Algemeen veiligheidsreferentiesysteem**
- **RSA: Rivest Shamir Adleman**
- **SSI: Veiligheid van de informatiesystemen**
- **URL: Uniform Resource Locator**

Public Key Infrastructure (PKI)	Geheel van fysieke componenten, procedures en software om de levenscyclus van de certificaten te beheren en authenticatie-, versleutelings- en handtekeningdiensten aan te bieden.
Certificaat	Elektronisch bestand, afgeleverd door een certificaatautoriteit die de identiteit van een houder (natuurlijke persoon, apparaat enz.) bevestigt. Het certificaat is geldig gedurende een bepaalde periode die erin staat vermeld.
Certificaatautoriteit (CA)	Dienst die is belast met de ondertekening, de uitgifte en het onderhoud van de certificaten van een public key infrastructure, overeenkomstig een certificaatbeleid.  Softwarediensten voor het beheer van de certificaten uitgegeven door de certificaatautoriteit van de certificaathouder.
Certificaatbeleid (CB)	Een reeks regels en eisen die een certificaatautoriteit moet naleven bij het organiseren en het verstrekken van haar diensten.
Registratiebeleid (RB)	Een reeks regels en eisen die een registratieautoriteit moet naleven bij het organiseren en het verstrekken van haar diensten.
Verklaring met betrekking tot de certificatiepraktijk (CPS)	Beschrijving van de certificatiepraktijken (organisatie, operationele procedures, technische en menselijke middelen) die de certificaatautoriteit toepast in het kader van het leveren van haar elektronische certificatediensten, overeenkomstig het certificaatbeleid dat zij moet naleven.

Verklaring registratiepraktijken (DPE)	Beschrijving van de registratiepraktijken (organisatie, operationele procedures, technische en menselijke middelen) die de registratieautoriteit toepast in het kader van het leveren van haar registratiediensten, met het oog op elektronische certificatie, overeenkomstig het registratie- en certificaatbeleid dat zij moet naleven.
Lijst met ingetrokken certificaten (CRL)	Door de certificaatautoriteit gepubliceerde lijst met de certificaten die niet langer betrouwbaar zijn (ingetrokken, ongeldig enz.).  Gemakshalve worden daaraan ook de intrekingslijsten van autoriteiten (LAR of ARL genoemd) gekoppeld.
OCSP-responder	Online statusservice certificaten
x 509	Norm van de Internationale Telecommunicatie Unie (ITU) over de public key infrastructures (PKI), met onder andere de standaardformaten voor de componenten: elektronische certificatie, intrekingslijsten, validatiealgoritme, ...
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 certificaatbeleid of de verklaring met betrekking tot de certificatiepraktijk.
Isabel Card	Een kaarttype Isabel met hoogbeveiligde technologie die een sterke technische authenticatie en een juridisch hoogstaande identificatie mogelijk maakt.
EBB Card	Een kaarttype Isabel voor het EBB-platform met een hoogbeveiligde technologie die een sterke

	technische authenticatie en een juridisch hoogstaande identificatie mogelijk maakt.
eID Belgium	Een type identificatiekaart van de Belgische overheid met een hoogbeveiligde technologie die een sterke technische authenticatie en een juridisch hoogstaande identificatie mogelijk maakt.
Drager	"Onderwerp" in de zin van het ETSI. In het kader van dit document is het "onderwerp" de cliënt van BNPP FORTIS, die steeds een natuurlijke persoon is.
Organisatie	"Ondertekenaar" in de zin van ETSI. In het kader van dit document is de "ondertekenaar" steeds BNPP FORTIS.

## 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 informatie die moet worden gepubliceerd voor de houders en de gebruikers van certificaten, steunt de registratieautoriteit 'FORTIS RA' op de publicatiefunctie van de CA, die belast is met de publicatie ervan<sup>2</sup>.

Het certificatiebeleid van de CA verduidelijkt de methodes van terbeschikkingstelling en de overeenkomstige URL's (webservers voor publicatie) voor de documenten van de CA (CP, certificaten van de CA, CRL ...).

De aanvullende documenten met betrekking tot deze RA (dit RB, de AGV) volgen dezelfde publicatiemethoden.<sup>3</sup>

### II.B. Te publiceren informatie

Naast de informatie die beschreven is in de CP van de CA wordt de volgende informatie gepubliceerd:

Deze RP / RPS	<a href="https://www.luxtrust.com/fr/repository">https://www.luxtrust.com/fr/repository</a>
De GTC [6] en GTC van ephemeral certificaten [5]	<a href="https://www.luxtrust.com/fr/repository">https://www.luxtrust.com/fr/repository</a>

<sup>2</sup> FORTIS heeft ook het recht om dit RB en de AGV, in voorkomend geval, om operationele redenen ter beschikking te stellen op andere publicatiesites.

<sup>3</sup> FORTIS staat toe om de plaats van publicatie van deze documenten te wijzigen. In dat geval wordt dit RB bijgewerkt.

### II.C. Publicatietermijnen en -frequenties

Publicatietermijnen en -frequentie voor informatie over de AE (nieuwe versie van de RP/RPS, algemene gebruiksvoorwaarden), de informatie wordt gepubliceerd zodra nodig zodat de gepubliceerde informatie en de effectieve verbintenissen van de CA altijd coherent blijven.

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

Zie PC van de CA

## III. Identificatie en authenticatie

Hier gelden de regels van de CA. We verduidelijken enkel de bijkomende regels opgelegd door de RA.

### III.A. Naamgeving

#### III.A.1. Type namen

Zie PC van de CA

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

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

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

#### III.A.3. Pseudoniemen van de houders

De certificaten van de houders krijgen geen pseudoniem.

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

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

De functionele RA voert in het kader van de relatieopening normalisatietransformaties uit met betrekking tot de naam en de voornamen van de houder. Deze transformaties zijn beperkt tot de volgende gevallen:

- **de naam mag slechts 32 tekens bevatten, die verplicht letters, blanco's of streepjes moeten zijn, met uitsluiting van alle andere tekens.**
- **de voornamen, enkel de eerste voornaam wordt behouden en de voornaam mag niet langer zijn dan 16 karakters en mag enkel letters, blanco's, streepjes, punten of komma's bevatten, met uitsluiting van alle andere.**

Daarnaast worden de volgende transformaties toegepast:

- voor de kleine letters wordt 'abcdefghijklmnopqrstuvwxyzaaaâââçññêêèèïïïöôÁóÁúúäüý' omgevormd tot 'ABCDEFGHIJKLMNPOQRSTUVWXYZAAAAACNEEEEEIIIOOOOOOUUY'
- voor de hoofdletters wordt 'ÂËÀÁÇÁÉÊËÈËÏÏÖÖÁÓÏÏÛÛÁÝ' omgevormd tot 'AAAAACNEEEEEIIIOOOOOOUUY' De gedetailleerde regels worden weergegeven in het DPE.

### III.A.5. Unicité van namen

BNP Paribas Fortis is verantwoordelijk voor de uniciteit van de namen van haar houders en de beslechting van geschillen over hun opeising van het gebruik van een naam.

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

Daarom bevat het veld SN (serialNumber) naast de regels die in de CP van de CA OTU zijn bepaald, een nummer (UUID).

De uniciteit wordt gegarandeerd door het toevoegen van een uniek nummer (UUID – cfr. RFC 4122 -) in het SN-attribuut van het onderwerp (DN) van het certificaat. Dit unieke serienummer wordt beheerd door de CA.

De DN moet daarom aan de volgende eisen voldoen voor de houders:

- **CN = identiteit van het subject/de natuurlijke persoon, in de vorm 'voornaam-naam'**
- **SN (surName) = naam van het subject / de natuurlijke persoon**
- **givenName = voornaam van het subject / de natuurlijke persoon**
- **SN (serial number) = Uniek nr. (UUID)**
- **O (organizationName) = BNPPF Customer**
- **OU = identificatiecode van de certificaathouder binnen de organisatie en (optioneel) van het type certificaataanvraag, als volgt:**
  - 1) Identificatie van het subject / de natuurlijke persoon
    - Positie 1-10
      - SMID
  - 2) Handtekeningkanaal
    - Positie 11-12
      - 12: EBB
      - 49: EBA
      - 52: EBW
      - 56: EBBM
- **C = BE**

In het geval van een testcertificaat, conform PC§1.4.4 van de CA is het gebruikte profiel hetzelfde als het profiel van een tijdelijk certificaat. De DN moet echter aan de volgende eisen voldoen:

- **CN (commonName) = ofwel de identiteit van het subject / de natuurlijke persoon, in de vorm 'Voornaam Naam', met toevoeging van een 'TEST' als prefix, ofwel 'TEST-MONITORING'**
- **SN (surName) = ofwel de naam van het subject / de natuurlijke persoon met toevoeging van 'TEST' in suffix, ofwel "TEST-MONITORING"**

- **givenName = ofwel de voornaam van het subject / de natuurlijke persoon, ofwel 'TEST-MONITORING'**
- **SN (serial number) = Uniek nr. (gegenereerd door de CA)**
- **OF= F-1**
- **C = BE**

In het geval van een testcertificaat bevat het veld CN als prefix 'TEST', conform de CP van de CA.

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

- **Het merk BNP PARIBAS is een door BNP PARIBAS gedeponeerd merk, waaronder:** BNP PARIBAS, een merk van de Europese Unie, geregistreerd bij de EUIPO op 8 oktober 1999 in de klassen 35, 36 en 38 en geregistreerd op 19 januari 2001 onder het nummer 1338888.
- BNP PARIBAS, merk van de Europese Unie, geregistreerd bij de EUIPO op 25 november 2005 in de klassen 9, 35, 36 en 38 en geregistreerd op 24 januari 2007 onder het nummer 004743639

Het merk **BNP Paribas Fortis** is een merk, geregistreerd door BNP Paribas Fortis NV bij het Benelux-Bureau voor de Intellectuele Eigendom op 3 januari 2013 in de klassen 35, 36 en 42 en geregistreerd op 07 januari 2013 onder het nummer 931084

Het merk **Fintro** is een gedeponeerd merk van BNP Paribas Fortis NV, waarvan onder meer:

- FINTRO, Benelux-merk, geregistreerd bij het Benelux-Bureau voor de Intellectuele Eigendom op 27 september 2004 in klasse 36 en geregistreerd op 10 maart 2005 onder het nummer 764125.
- FINTRO, merk van de Europese Unie, geregistreerd bij de EUIPO op 27 september 2004 in klasse 36 en geregistreerd op 10 mei 2007 onder het nummer 004046173.

### III.B. Oorspronkelijke goedkeuring van de identiteit

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

De aanvraag van een certificaat aangemaakt door de technische RA wordt ondertekend op basis van de bijbehorende private sleutel, terwijl het sleutelpaar wordt aangemaakt door een versleutelingsmodule van de technische RA van BNP Paribas Fortis

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

Niet van toepassing.

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

De registratie van een houder voor de uitgifte van een certificaat wordt verricht door BNP Paribas Fortis in zijn functie van functionele RA.

BNP Paribas Fortis mag de regels voor de controle van de identiteit van de houder vrij bepalen zoals beschreven in het document [1] (*SEALED - AdES Requirements Part 2 identification*) in het kader van zijn activiteit en in zijn rol van functionele RA. Deze controleregels:

- **Voldoen ten minste aan de vereisten van ETSI EN 319411-1 voor NCP+**
- **Voldoen aan de AATL-vereisten**
- **Voldoen aan de eisen van de CA CP.**

Deze regels zijn in overeenstemming met de vereisten van de CA "CA" CP.

De methoden voor identiteitsverificatie die in het kader van dit beleidsdocument worden aanvaard, in overeenstemming met de hierboven vermelde vereisten, worden gedetailleerd beschreven in document [1] (2024-03-07 - SEALED - AdES Requirements Part 2 identification v1.0) waarin hun naleving van de toepasselijke normen en standaarden (geïdentificeerd in document [1]) wordt geanalyseerd en zijn als volgt:

<b>Methode 1:</b> itsme
<b>Methode 2:</b> Face-to-face registratie door BNPPF
<b>Methode 3:</b> Registratie door face-to-face van een vertegenwoordiger
<b>Methode 4:</b> Gedelegeerde registratie

BNP Paribas Fortis kan in het kader van een toekomstige versie van dit RB, de middelen voor identiteitsverificatie uitbreiden op voorwaarde dat die middelen een bewezen betrouwbaarheidsniveau hebben dat gelijk is aan of hoger is dan de huidige middelen, ongeacht of ze voldoen aan de norm ETSI 319411-1 voor het LCP-niveau en aan de eisen AATL.<sup>4</sup>

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

De procedure voor de controle van de identiteit van de houder in de vorm 'voornaam-naam' en de koppeling van een uniek klantnummer, SMID, valt enkel onder de verantwoordelijkheid van BNP Paribas Fortis in het kader van zijn bankactiviteit.

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

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

Alle gecertificeerde informatie wordt gecontroleerd.

### III.C. Goedkeuring van de autoriteit van de aanvrager

Onderzoek hoofdstuk III.B.4

#### III.C.1. Kruiscertificaat van CA

Niet van toepassing voor een registratiebeleid. Zie de CP 'CA'.

---

<sup>4</sup> De controlemiddelen moeten expliciet worden aanvaard door de CA in het kader van het bijwerkingsproces van dit RP/RPS.

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

#### III.D.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 RP/RPS.

#### III.D.2. Identificatie en goedkeuring voor een vernieuwing na intrekking

Niet van toepassing in het kader van dit RP/RPS.

### III.E. Identificatie en goedkeuring van een intrekkingaanvraag

Niet van toepassing in het kader van dit RP/RPS.

## IV. Operationele eisen voor de levenscyclus van de certificaten

### IV.A. Herkomst van een certificaataanvraag

In het kader van dit RP/RPS mag de certificaataanvraag enkel worden uitgegeven door een metiertoepassing van BNP Paribas Fortis in zijn functie van functionele RA. De metiertoepassing van BNP Paribas Fortis en de technische RA worden grondig geauthenticeerd voor elke aanvraag van een houdercertificaat.

### IV.B. Proces en verantwoordelijkheden voor de opstelling van een certificaataanvraag

De certificaataanvraag vereist een uitgebreide authenticatie van de technische componenten van de functionele RA van BNP Paribas Fortis en de technische RA, door gebruik te maken van beveiligde protocollen die authenticatiecertificaten vereisen.

- ***De functionele RA controleert de statussen van die certificaten voordat ze de aanvraag behandelt.***
- ***De functionele RA van BNP Paribas Fortis is verantwoordelijk voor de controle van de integriteit van de gegevens die ze aan de technische RA bezorgt.***

Het proces voor de aanvraag voor de opstelling van een houdercertificaat wordt beschreven in hoofdstuk I.C.2.

### IV.C. Behandeling van een certificaataanvraag

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

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

- **De aanvraag wordt automatisch in elektronische vorm opgesteld door de functionele RA van BNP Paribas Fortis en naar de technische RA doorgestuurd;**
- **Er wordt een bewijs voor het bezit van de sleutel aangemaakt en geformatteerd door de technische RA, met de te certificeren informatie, in de vorm van een certificaataanvraag.**
- **Dat bewijs wordt ter ondertekening naar de CA gestuurd.**

#### **IV.C.2. Aanvaarding of afwijzing van de aanvraag**

De Registratieautoriteit aanvaardt automatisch om de certificaataanvraag bij de Certificatie-autoriteit in te dienen na authenticatie van de houder met een van de door BNP Paribas Fortis aanvaarde en in clausule I.C.2toelatingsmiddelen.

Het document wordt voorgelegd aan de houder door de metiertoepassing van BNP Paribas Fortis en de houder stemt ermee in vóór ondertekening.

Bij weigering wordt de houder op de hoogte gebracht door de metiertoepassing van BNP Paribas Fortis.

#### **IV.C.3. Duur van de opstelling van het certificaat**

Het certificaat wordt opgesteld door de technische RA binnen het kortst mogelijke tijdsbestek na de ontvangst van de aanvraag.

### **IV.D. Aflevering van het certificaat**

#### **IV.D.1. Acties van de CA voor de aflevering van het certificaat aan de houder**

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

- **Het respecteren van de syntaxis van de attributen van het onderwerp (DN), cfr. §III.A.5**
- **De versleutelingskenmerken van de aanvraag (omvang van de sleutel).**

#### **IV.D.2. Kennisgeving van de aflevering van het certificaat aan de houder**

Het gaat om een automatische verrichting tijdens een proces voor elektronische ondertekening.

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

### **IV.E. Aanvaarding van het certificaat**

#### **IV.E.1. Proces voor de aanvaarding van het certificaat**

De houder geeft zijn toestemming door:

- 1) Schermen layout Web: expliciete aanvaarding van de CN van het in zijn naam aangemaakte certificaat, zie hoofdstuk I.C.2. Hij aanvaardt om de gegevens die hem worden voorgelegd door de functionele RA van BNP Paribas Fortis, te ondertekenen.
- 2) Schermen layout Mobile: door het vakje aan te vinken dat aangeeft dat de klant verklaart "kennis te hebben genomen van de "Gebruiksvoorwaarden van de elektronische handtekeningcertificaten", dat alle gegevens correct zijn en dat in het kader van die voorwaarden een certificaat met zijn naam kan worden

aangemaakt".

#### **IV.E.2. Publicatie van het certificaat**

Het certificaat wordt niet gepubliceerd.

#### **IV.E.3. Kennisgeving van de aflevering van het certificaat**

Overeenkomstig de CP van de CA, stuurt de CA het overgelegde Certificaat door naar de RA als antwoord op de behandeling van de aanvraag voor de aanmaak van het Certificaat. De RA stuurt het op zijn beurt door naar het handtekeningsysteem van BNP Paribas. Deze overdracht geldt als kennisgeving

### **IV.F. Gebruik van het sleutelpaar en het certificaat**

#### **IV.F.1. Gebruik van de private sleutel en het certificaat door de houder**

Voor het tijdelijke certificaat van de ondertekenaar is het gebruik van de private sleutel van de houder die wordt aangemaakt door de ondertekeningdienst van BNP Paribas en het bijbehorende certificaat, uitgegeven in het kader van dit RB, strikt beperkt tot de ondertekeningdienst die BNP Paribas aanbiedt. De zakelijke toepassing van BNP Paribas Fortis laat niet toe om de private sleutel op een andere<sup>5</sup>manier te gebruiken.

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

#### **IV.F.2. Gebruik van de private sleutel en het certificaat door de gebruiker van het certificaat**

De technische RA maakt ook een bewijsbestand aan (spoor van audit, optioneel metiergegevens van de toepassing van BNP Paribas Fortis, bewijsbestanden voor de goedkeuring van de handtekening) bij elke ondertekening door de houder.

De private sleutel van een tijdelijk elektronisch handtekeningcertificaat wordt vernietigd aan het einde van de gebruikerstransactie.

### **IV.G. Vernieuwing van een certificaat**

Niet van toepassing in het kader van dit PE.

### **IV.H. Aflevering van een nieuw certificaat na een verandering van het sleutelpaar**

De verandering van sleutelpaar voor een tijdelijk certificaat wordt beschouwd als een aanvraag voor een nieuw certificaat. Dit kan gebeuren voor een bepaalde houder onder de verantwoordelijkheid van de functionele RA bij het einde van de levensduur van een voorgaand certificaat.

De procedure voor de afgifte is dezelfde als voor een oorspronkelijk certificaat.

---

<sup>5</sup> Er dient te worden aangestipt dat de CA 'CA' certificaten kunnen uitgeven buiten de perimeter van dit RP/RPS, bijvoorbeeld voor andere klanten.

#### **IV.I. 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).

De wijziging van het certificaat is niet toegestaan in het kader van dit RB.

#### **IV.J. Intrekking en opschorting van de certificaten**

Niet van toepassing in het kader van dit RP/RPS.

##### **IV.J.1.Mogelijke oorzaken van een intrekking**

Niet van toepassing in het kader van dit RP/RPS.

##### **IV.J.2.Herkomst van een intrekkingaanvraag**

Niet van toepassing in het kader van dit RP/RPS.

##### **IV.J.3.Procedure voor de behandeling van een intrekkingaanvraag**

Niet van toepassing in het kader van dit RP/RPS.

##### **IV.J.4.Aan de houder toegekende termijn voor de formulering van de intrekkingaanvraag**

Niet van toepassing in het kader van dit RP/RPS.

##### **IV.J.5.Behandelingstermijn van een intrekkingaanvraag**

Niet van toepassing in het kader van dit RP/RPS.

##### **IV.J.6.Eisen voor de controle van de intrekking door de certificaatgebruikers**

Boven op de vereisten van het PC 'CA' is de technische RA ertoe gehouden te controleren of het certificaat van de certificaatautoriteit 'BNPPF Instant CA' die het certificaat van de houder heeft uitgegeven, wel geldig is.

##### **IV.J.7.Frequentie van de opstelling van de CRL's**

Zie 'CA' CP

##### **IV.J.8.Maximumtermijn voor de publicatie van een CRL**

Zie 'CA' CP

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

Zie 'CA' CP

#### **IV.J.10. Eisen voor de onlinecontrole van de intrekking van de certificaten door de certificaatgebruikers**

Zie 'CA' CP

#### **IV.J.11. Andere beschikbare informatiemiddelen in verband met de intrekkingen**

Niet van toepassing.

#### **IV.J.12. Specifieke eisen bij schending van de private sleutel**

Zie 'CA' CP

#### **IV.J.13. Mogelijke oorzaken van een opschorting**

Niet van toepassing.

#### **IV.K. Functie voor informatie over de status van de certificaten**

Zie 'CA' CP

### **V. Niet-technische veiligheidsmaatregelen**

De vereisten die verder in dit hoofdstuk worden gedefinieerd, zijn de minimumvereisten waaraan de registratieautoriteiten van BNP PARIBAS moeten voldoen.

Het vertrouwelijke deel van de verklaring van registratiepraktijken (DPE) beschrijft de middelen die worden ingezet om aan deze vereisten te voldoen

#### **V.A. Fysieke veiligheidsmaatregelen**

BNPP Paribas en BNP Paribas Fortis controleren de fysieke toegangen tot de componenten van de RA waarvan de veiligheid kritiek is voor de levering van de registratiedienst, om het risico verbonden aan de fysieke veiligheid tot een minimum te beperken. In het bijzonder:

- ***De fysieke toegang tot kritieke componenten wordt beperkt tot geautoriseerde personen***
- ***Er worden controles ingevoerd om verlies, beschadiging en verstoring van de goederen en onderbreking van de dienstverlening te voorkomen.***
- ***Er worden controles uitgevoerd om compromittering of diefstal van informatie te voorkomen, vooral in de informatieverwerkingsruimtes***
- ***De voor de veiligheid van de registratieverrichtingen kritieke componenten bevinden zich binnen de veiligheidsperimeter met fysieke inbraakbeveiligingsmiddelen, zoals de fysieke toegangscontrole tot de perimeter en de installatie van een alarm bij inbraak.***

#### **V.B. Veiligheidsmaatregelen voor de procedures**

##### **V.B.1. Vertrouwensrollen**

We onderscheiden de volgende rollen op de perimeter van de RA:

- ***RA officer: een door de PMA aangewezen persoon die deze rol aanvaardt en die belast is met het verifiëren van de juistheid en toereikendheid van de informatie die vereist is voor de aanvraag van een certificaat om te voldoen aan de verschillende vereisten van dit document, met name door het valideren van de verschillende processen die worden gebruikt om deze informatie te verzamelen***

- **RA Technische operator is belast met het gebruik, de configuratie en het technisch onderhoud van de apparatuur die verantwoordelijk is voor het opstellen en indienen van certificaataanvragen bij de certificeringsinstantie en die verantwoordelijk is voor het opstellen van het validatiebestand voor het bewijs van handtekening voor elke handtekening door de houder ("evidence book").**
- **RA Registration operator: elke persoon die betrokken is bij een van de inschrijvingsprocessen die zijn goedgekeurd door de RA officer (bijv. filiaalmedewerkers die face-to-face omgaan met nieuwe klanten, de contractmanager die een persoon toevoegt bij een rekening van een rechtspersoon, personen die IdentiFin- of CheckDoc-controles uitvoeren, enz.).**  
 NOTE : niet alle processen vereisen de betrokkenheid van een inschrijvingsoperator (inschrijving via itsme is bijvoorbeeld volledig geautomatiseerd).

### 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 RB telt een aantal vereisten met betrekking tot deze verdeling, met name voor de verrichtingen in verband met de versleutelingsmodules van de handtekeningdienst van BNP PARIBAS, die in het DPE worden beschreven.

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

ITG laat de identiteit en de machtigingen van elk personeelslid controleren voordat ze hem een rol en de overeenkomstige rechten toekennen. Raadpleeg het EPD voor meer informatie.

### 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 rol van auditor mag niet worden gecumuleerd met enige andere rol;**
- **de personen die een component implementeren mogen niet dezelfde zijn als de personen die ze controleren**

De aan elke rol gekoppelde bevoegdheden worden beschreven in het DPE van de RA en zijn in overeenstemming 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 RA aan de slag gaan, zijn contractueel onderworpen aan een veiligheids- en vertrouwelijkheidsbeding.

Elke dienst die werkzaam is voor een component van de RA, moet erover waken dat de bevoegdheden van

zijn personeelsleden die in de component zullen werken, in overeenstemming zijn met hun professionele vaardigheden.

De RA informeert elke persoon die intervenueert in de vertrouwensrollen van de RA:

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

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

De relevante documenten worden beschreven in V.C.8

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

De personeelsleden van de RA 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 registratieautoriteit 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 BNP Paribas en BNP Paribas Fortis 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 van de registratiepraktijken eigen aan het certificatie domein;**
- **Documenten van de bouwers van de gebruikte hardware en software;**
- **Registratiebeleid onderschreven door de component waartoe hij behoort;**
- **Certificatiebeleid van de CA;**
- **Interne werkingsprocedures.**

De registratieautoriteit ziet erop toe dat haar personeel (zoals bepaald in het DPE) wel degelijk over de hierboven vermelde documenten beschikt op basis van hun behoeften, zoals bepaald in het DPE.

## 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 RA van de groep BNP Paribas Fortis 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 RA 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;**
- **Evenementen die verband houden met de logging: opstarten en afsluiten van de logfunctie, wijziging van de logininstellingen, ondernomen acties na een storing in de logfunctie;**
- **In- en uitloggen van de gebruikers met vertrouwensrollen en overeenkomstige mislukte pogingen.**
- **Ontvangst van een certificaataanvraag (eerste aanvraag en vernieuwing);**
- **-Goedkeuring/afwijzing van een certificaataanvraag;**
- **- Ontvangst van een intrekkingaanvraag;**
- **- Goedkeuring/afwijzing van een intrekkingaanvraag;**

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 technische sporen die de verantwoording van de acties verzekeren worden bewaard afhankelijk van het documenttype voor een periode van minimaal 10 en maximaal 30 jaar:

- (i) na het einde van het document
- (ii) nadat het document vervallen is (als een geldigheids-periode van toepassing is)
- (iii) na de documentdatum als (i) en (ii) niet van toepassing

#### V.D.4. Bescherming van de gebeurtenissenlogboeken

De RA van de groep BNP Paribas Fortis 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 RA van de groep BNP Paribas Fortis treft de vereiste maatregelen om de integriteit en de beschikbaarheid van de gebeurtenissenlogboeken voor de betrokken component te waarborgen, overeenkomstig de eisen van dit RP/RPS.

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

#### V.D.6. Verzamelsysteem van de gebeurtenissenlogboeken

De RA van BNP Paribas Fortis 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 beoordeling van de kwetsbaarheden wordt vermeld in de risicoanalyse van BNP Paribas Fortis over zijn RA.

Er worden periodiek, minstens jaarlijks, bijkomende penetratietests uitgevoerd.

### V.E. Archivering van de gegevens

#### V.E.1. Te archiveren gegevenstypes

Dankzij de archivering is het mogelijk om:

- ***De duurzaamheid garanderen van de logboeken die door de verschillende componenten van de RA werden aangemaakt;***
- ***De papierstukken te bewaren van de verrichtingen en ze zo nodig beschikbaar te maken.***

De te archiveren gegevens betreffen zowel het papieren als het elektronische formaat.

De volgende gegevens moeten worden gearhiveerd:

- ***Het onderhavige RB en het bijbehorende DPE***
- ***De auditgegevens***
- ***De gebeurtenissenlogboeken van de verschillende entiteiten van de RA***
- ***De papierstukken van de RA***
- ***De elementen die op hem rusten in de samenstelling van het evidence boek/audit trail dat aan de handtekening is gekoppeld.***

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

Raadpleeg het betreffende hoofdstuk van CARINA.

### V.E.3. Bewaringsperiode van het archief

De bewaartermijn van het elektronisch archief is als volgt:

- **Bewaartermijn van het archief voor de gebeurtenissenlogboeken: 1 jaar**
- **De registratiedossiers en de identiteitsgegevens van de Ondertekenaar worden bewaard gedurende tien jaar vanaf het einde van de relatie tussen de Klant en BNP PARIBAS FORTIS.**
- **Het ondertekende document wordt naargelang het type document bewaard voor een duur van minimaal 10 en maximaal 30 jaar, te rekenen vanaf:**
  - o (i) van het einde van het contract
  - o (ii) het verstrijken van het document indien een geldigheidsperiode van toepassing is
  - o (iii) van de datum van het document indien (i) en (ii) niet van toepassing zijn.
- **De technische sporen die de toerekenbaarheid van de aandelen garanderen, worden bewaard volgens het type document voor een duur van minimaal 10 en maximaal 30 jaar, te rekenen vanaf:**
  - o (i) het einde van het contract
  - o (ii) het verstrijken van het document indien een geldigheidsperiode van toepassing is
  - o (iii) de datum van het document indien (i) en (ii) niet van toepassing zijn.
- **De bewaartermijn van de elementen die specifiek zijn voor de CA (CRL, technische sporen van de CA ...) is vermeld in de CP 'CA'.**

### 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 DPE 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 betreffende hoofdstuk van Carina.

### V.E.7. Verzamelsysteem van het archief

De registratiesporen worden bewaard in het bewijsbestand dat bij de transactie hoort. Deze wordt bewaard onder voorwaarden die de beschikbaarheid, integriteit en vertrouwelijkheid ervan waarborgen.

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

Het archief wordt beheerd door de RA van BNP Paribas Fortis. Het recuperatieproces maakt het voorwerp uit van een interne werkingsprocedure die in Carina is vermeld. De opgevraagde gegevens kunnen binnen een termijn van maximaal vijf werkdagen beschikbaar zijn.

### V.F. Verandering van sleutel van de autoriteit

Niet van toepassing voor een RA.

### **V.G. Hervatting na schending en schade**

De RA 'FORTIS RA' verbindt zich ertoe alle maatregelen voor de hervatting na een compromis en schadegeval zoals vermeld in het beleid voor de certificatie van de CA OTU van het TSP Mediacert na te leven, in het bijzonder:

- **De RA 'FORTIS RA' heeft een bedrijfscontinuïteitsplan bij schade opgesteld en houdt dat bij.**
- **Bij een schadegeval, met inbegrip van een schending van een handtekeningsleutel of een schending van het authenticatiemiddel, verbindt de RA 'FORTIS RA' zich ertoe om alle maatregelen van het plan voor de bedrijfscontinuïteit in het bijzonder uit te voeren:**
  - o **de onmiddellijke kennisgeving, in voorkomend geval, van de schending aan het TSP Mediacert,**
  - o **De invoering van passende herstelmaatregelen om de veiligheid van de verrichtingen te herstellen.**

### **V.H. Einde levensduur RA**

Bij het einde van de levensduur van de RA worden alle archieven en de sporen van de RA gearchiveerd door BNP Paribas. De CA wordt dus niet beïnvloed door de stopzetting van de RA. De authenticatiemiddelen van de technische RA van BNP Paribas worden ingetrokken.

## **VI. Technische veiligheidsmaatregelen**

De vereisten die verder in dit hoofdstuk worden gedefinieerd, zijn de minimumvereisten waaraan de registratieautoriteit 'FORTIS RA' moet voldoen voor de sleutelparen van de houders.

Voor de technische veiligheidsmaatregelen die van toepassing zijn op de sleutels van de CW, buiten de perimeter van dit document, verwijzen we naar de CP 'CA'.

### **VI.A. Aanmaak en installatie van sleutelparen**

#### **VI.A.1. Aanmaak van sleutelparen**

Het sleutelbaar van een houder wordt aangemaakt via een materiële versleutelingsmodule (HSM) waarvan de eisen worden beschreven in §VI.B.1.

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

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

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

De publieke sleutels van de houders worden aan de CW overhandigd op basis van aanvragen die worden gegenereerd door een handtekeningssoftware in een formaat dat het mogelijk maakt het bezit van sleutels te bewijzen door de aanvraag te ondertekenen. De handtekening wordt gecontroleerd door de CA. Zij geeft een certificaat uit als de controle in orde is.

De integriteit van de aflevering wordt aldus van begin tot einde beschermd bij de aanvraag voor de aanmaak van het certificaat.

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

Zie CP 'CA'

#### **VI.A.5. Omvang van de sleutels**

De houders gebruiken sleutels van minstens 2.048 bits.

Wat de grootte van de sleutels betreft, volgt de handtekeningapplicatie van BNP PARIBAS de aanbevelingen van ANSSI op het vlak van cryptografische dimensionering.

#### **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**

Onderzoek §VI.C.2

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

Voor de certificaten van de houders, zie I.C.4

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

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

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**

De private sleutels van de houders worden niet door meerdere personen gecontroleerd. Ze staan onder controle van de drager.

#### **VI.B.3. Escrow van de private sleutel**

n.v.t.

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

Er wordt geen back-up gemaakt van de private sleutels van de houders.

#### **VI.B.5. Archivering van de private sleutel**

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

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

Niet van toepassing voor de private sleutels van de houders

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

De private sleutels van de houders worden opgeslagen in een versleutelingsmodule die minstens aan de volgende eisen beantwoordt:

- **Gemeenschappelijke criteria EAL4+ , of**
- **FIPS 140-2 level 2**

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

De sleutels worden geactiveerd zodra ze zijn gegenereerd. Het gebruik ervan vereist authenticatie van de drager aan de hand van twee factoren.

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

Niet van toepassing.

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

Na ondertekening wordt de vernietiging van de sleutels opgestart.

### **VI.B.11. Veiligheidsevaluatieniveau van de versleutelingsmodule**

Zie VI.B.1

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

### **VI.C.1. Archivering van de publieke sleutels**

De publieke sleutels van de houders worden niet gearhiveerd door de RA. De CA archiveert ze via de archivering van de uitgegeven certificaten.

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

De levensduur van de certificaten is ingesteld op 50 min.

Is de levensduur van de sleutelparen beperkt tot hun koppeling aan een certificaat.

## **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 het ondertekeningsplatform van BNP Paribas 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 ITG in het kader van de rollen die hen zijn toevertrouwd.

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

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

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

We verwijzen naar het hoofdstuk over DPE.

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

We verwijzen naar het hoofdstuk over DPE

### **VI.E. Veiligheidsmaatregelen voor de informaticasystemen**

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

We verwijzen naar BNPP Fortis interne documenten.

#### **VI.E.2. Kwalificatieniveau van de informaticasystemen**

Zie VI.B.1

### **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 ondertekeningsinfrastructuur van de groep BNP Paribas moeten worden gedocumenteerd en opgenomen in de interne werkingsprocedures van de betrokken component en moeten in overeenstemming zijn met het onderhoudsschema van de conformiteitswaarborg voor geëvalueerde producten.

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

Dit beleid bevat hierover geen specifieke eisen.

### **VI.G. Veiligheidsmaatregelen voor het netwerk**

De onderlinge verbindingen en toegang tot de middelen van de ondertekeningsoplossing 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 infrastructuur de systeemtijd en zorgen ze ervoor dat de systeemklokken 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

Zie CP 'CA'

## VIII. Conformiteitsaudit en andere evaluaties

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

Om de twee jaar wordt een conformiteitscontrole uitgevoerd ten opzichte van het referentiesysteem van ETSI EN 319 411-1 LCP op de perimeter van de RA's van de groep BNP Paribas. BNP Paribas zal ten minste eens in de twee jaar een interne audit uitvoeren.

### VIII.B. Identiteit/kwalificaties van de evaluators

De controle van een component moet door de directie van 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 auditors moeten met name de eisen die van toepassing zijn op het toepassingsgebied van de EA beheersen, in het bijzonder de norm ETSI EN 319 411-1, de Mediacert CP en de eisen van de AATL. Ze moeten rekening houden met de vereisten van die referentiesystemen in hun auditplan en in de ingevoerde controles.

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 het bijbehorende DPE.

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

De conformiteitscontroles of interne controles van BNP Paribas hebben betrekking op de volledige RA van de groep BNP Paribas en zijn bedoeld ter controle van de naleving van de verbintenissen en praktijken zoals bepaald in dit certificaatbeleid en in de overeenkomstige DPE 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 de PMA en LuxTrust.

Het is de verantwoordelijkheid van de actoren die in dit RP/RPS worden geïdentificeerd om 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 en de Luxtrust CA meegedeeld.

## IX. 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 BNP PARIBAS 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 vertrouwelijke gedeelte van het DPE dat met dit RB overeenstemt,*
- *De private sleutels van de componenten en de houders van certificaten van de ondertekeningsdienst van de groep BNP Paribas;*
- *Alle geheimen van de HSM van de handtekeningdienst van de groep BNP Paribas*
- *Voorvalregisters van de technische componenten van de groep BNP Paribas*
- *Het registratiedossier van de houders;*

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

Niet van toepassing.

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

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

### IX.D. Bescherming van de persoonsgegevens

BNP Paribas Fortis past de toepasselijke wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens toe, zowel op het gebied van de verzameling als het gebruik van persoonsgegevens (Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) en andere toepasselijke (nationale of andere) wet- en regelgeving inzake gegevensbescherming).

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

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

#### IX.D.2. **Persoonsgegevens**

Alle gegevens betreffende het registratiedossier van de houders worden ten minste beschouwd als persoonlijk.

### IX.D.3. Niet-persoonsgegevens

Er worden hierover geen specifieke eisen gesteld.

Aansprakelijkheid voor de bescherming van de persoonsgegevens

Zie geldende wetgeving en regelgeving op het Belgische grondgebied.

### IX.D.4. Kennisgeving van en instemming met het gebruik van de persoonsgegevens

Overeenkomstig de geldende wet- en regelgeving op het Belgische grondgebied mogen de persoonsgegevens die door de houders aan de RA worden overhandigd, niet aan een derde worden meegegeefd of doorgegeven, behalve in de volgende gevallen: voorafgaande toestemming van de houder, rechterlijke beslissing of andere wettelijke machtiging.

### IX.D.5. Voorwaarden voor de verspreiding van persoonsgegevens aan de gerechtelijke of administratieve autoriteiten

Zie geldende wetgeving en regelgeving op het Belgische grondgebied.

### IX.D.6. Andere omstandigheden voor de verspreiding van persoonsgegevens

Zie geldende wetgeving en regelgeving op het Belgische grondgebied.

### IX.E. Intellectuele en industriële eigendomsrechten

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

### IX.F. Contractuele interpretaties en waarborgen

#### IX.F.1. Basisverplichtingen van de CA

Zie CP 'CA'

#### IX.F.2. Basisverplichtingen van de RA

De verplichtingen van de RA zijn de volgende:

- **de integriteit en de vertrouwelijkheid van hun geheime en/of private sleutels beschermen en waarborgen;**
- **De 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 CB van de CA, dit PE en de documenten die eruit voortvloeien;**
- **het DPE naleven en toepassen,**
- **zich onderwerpen aan de conformiteitscontroles verricht door het auditteam dat door de CA of RA is gemachtigd (zie hoofdstuk VIII),**
- **de akkoorden of contracten naleven waardoor ze onder elkaar of met de houders zijn verbonden;**
- **de vereiste (technische en menselijke) middelen inzetten voor de verwezenlijking van de taken waartoe ze zich verbinden onder voorwaarden die de kwaliteit en de veiligheid garanderen**

Naast de bovenstaande verplichtingen zijn de verplichtingen uit de CP 'CA' van toepassing.

### **IX.F.3. Certificaathouders**

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

Naast de bovenstaande verplichting zijn de verplichtingen uit de CP 'OCU CA' van toepassing.

### **IX.G. Certificaatgebruikers**

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

De verplichtingen van de CP 'CA' zijn van toepassing.

### **IX.H. Andere deelnemers**

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

De verplichtingen van de CP 'CA' zijn van toepassing.

### **IX.I. Waarborglimiet**

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

### **IX.J. Aansprakelijkheidslimiet**

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

De clausules van het CP 'CA' zijn van toepassing.

### **IX.K. Schadevergoeding**

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

De clausules van het CP 'CA' zijn van toepassing.

## **IX.L. Duur en vervroegde beëindiging van de geldigheid van het PE**

### **IX.L.1. Geldigheidsduur**

De RB van de RA moet van toepassing blijven tot het einde van de levensduur van het laatste certificaat dat in het kader van dat EE is uitgegeven.

### **IX.L.2. Gevolgen van het einde van de geldigheid en van toepassing blijvende bepalingen**

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

De clausules van het CP 'CA' zijn van toepassing.

### **IX.L.3. Individuele kennisgevingen en communicatie tussen de deelnemers**

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

De clausules van het CP 'CA' zijn van toepassing.

## **IX.M. Wijzigingen in het PE**

### **IX.M.1. Wijzigingsprocedures**

Grote wijzigingen in dit RP/RPS 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 RP/RPS. Voor het goedkeuringsproces van het RP/RPS, zie hoofdstuk I.E.4.

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

### **IX.M.2. Mechanisme en periode voor informatie over de wijzigingen**

Eventuele updates worden vermeld in de versietracking en het bijbehorende document wordt gepubliceerd op de LuxTrust-website zodra de definitieve validatie van dit document is verkregen van de aangewezen entiteiten (PMA en LuxTrust).

### **IX.M.3. Omstandigheden waarin de OID moet worden veranderd**

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

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

## **IX.N. Bepalingen betreffende conflictoplossing**

Bij geschillen moet de houder contact opnemen met de contactpunten die zijn vermeld in hoofdstuk I.E.2.

## **IX.O. Bevoegde rechtbanken**

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

## **IX.P. Conformiteit met de wetgeving en regelgeving**

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

Het ontwerp en de implementatie van de diensten, software en procedures van BNP Paribas houden in de mate van het mogelijke rekening met de toegankelijkheid voor alle gebruikers, 'ongeacht hun hardware of software, netwerkinfrastructuur, moedertaal, cultuur, geografische locatie of fysieke of mentale vaardigheden' (<https://www.w3.org/Translations/WCAG20-fr/>).

## **IX.Q. Diverse bepalingen**

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

## **IX.R. Andere bepalingen**

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

# **X. Bijlage – Referentiedocumenten**

## **X.A. Regelgeving**

Niet van toepassing.

## X.B. Technische documenten

Référence	Objet du document
[1] 2024-03-07 - SEALED - AdES Requirements Part 2 identification v1.0	Presents and assesses the various identification methods used to enroll signatories toward the BNPPF eNotary signature platform according to applicable Regulations and Standards presented in [2].
[2] 2023-12-19 - SEALED - AdES Requirements Part 1 applicable requirements v0.4	Identifies and lists the rules and standards that are applicable to the BNPPF eNotary signature platform and derives the applicable requirements.
[3] 2022-05-09 - SEALED - AdES Requirements Part 4 screens - v0.1	Analyses the wording displayed to the customer and the actions (s)he takes in the eSignature screens (with and without eNotary). It indicates if/under which conditions this information complies with the requirements derived from the applicable Regulations and Standards presented in [2] requiring to ensure that the customer understands the general terms and conditions linked to the use of the eNotary signature service, in particular the fact that a signing certificate is issued on his/her name (CAA requirements, as introduced in [2]).
[4] 2022-08-25 - SEALED - AdES Requirements Part 3 tokens - v0.2	Assesses the various tokens used to authenticate the registered customers toward the BNPPF eNotary signature platform and / or used by the customer to trigger a signature. It indicates if/under which conditions these tokens comply with the requirements derived from the applicable Regulations and Standards as introduced in [2].
[5] CGV Luxtrust	<a href="https://www.luxtrust.com/fr/conditions-generales-de-vente">https://www.luxtrust.com/fr/conditions-generales-de-vente</a>
[6] CGU signature services (FORTIS)	<a href="https://easybankingbusiness.bnpparibasfortis.be/pics/BE/commonB/fr/li_b_download/Docserver/eSignature_CGU_Cosi_BNPPF_FR.pdf">https://easybankingbusiness.bnpparibasfortis.be/pics/BE/commonB/fr/li_b_download/Docserver/eSignature_CGU_Cosi_BNPPF_FR.pdf</a>

Alle gedetailleerde procedures betreffende dit RP/RPS worden beschreven in de documenten waarnaar hierboven wordt verwezen en kunnen op verzoek geraadpleegd worden door bevoegde personen.

## XI. Bijlage: Registratieprocedures – authenticatie en toelating aanvaard onder dit RB

## **XI.A. Procedure op basis van EMV-kaart voor retailklant**

### **XI.A.1. Stap 1: registratie (REG).**

De bank gaat over tot de registratiestappen REG 1.1 en REG 1.2 (cf. I.D.1) zoals beschreven in dit RP/RPS. De in [1] beschreven registratiemethoden in overeenstemming met deze RP/RPS zijn:

<b>Methode 1:</b> itsme
<b>Methode 2:</b> Face-to-face registratie door BNPPF
<b>Methode 3:</b> Registratie door face-to-face van een vertegenwoordiger
<b>Methode 4:</b> Gedelegeerde registratie

Bij deze gelegenheid associeert de bank de gebruiker op een ondubbelzinnige manier met een authenticatie- en autorisatiemiddel (AUTH/AUT).

De verschillende manieren waarop de authenticatie- en autorisatiemiddelen aan een geregistreeerde gebruiker kunnen worden gekoppeld, worden beschreven in [4].

Ze kunnen variëren afhankelijk van het kanaal voor elektronisch bankieren (EBW voor particulieren, of EBB voor personen die verbonden zijn aan een organisatie) en afhankelijk van het type applicatie (mobiel of web), maar bieden in alle gevallen hetzelfde beveiligingsniveau in de eenduidige associatie met de persoon

### **XI.A.2. Stap 2: authenticatie (AUTH)**

In deze stap authenticceert de klant zich op een unieke manier (SMID: klantnummer) als een natuurlijke persoon in zijn elektronische EBW-bankkanaal of als een persoon die verbonden is aan een organisatie in zijn elektronische EBB-kanaal, afhankelijk van of hij een niet-professionele klant is of verbonden is aan een organisatie.

De in [4] beschreven authenticatiemiddelen in overeenstemming met deze RP/RPS zijn:

<b>Token1:</b> The BNPPF app based on Gemalto (for both EBW and EBB channels) – van toepassing op alle gebruikers
<b>Token2:</b> Itsme (for both EBW and EBB channels) - van toepassing op alle gebruikers
<b>Token3:</b> The EMV card (M1 – M2 signature with an UCR token, for both EBW and EBB channels) - van toepassing op alle gebruikers
<b>Token4:</b> Isabel card (for EBB channel) - van toepassing op gebruikers gekoppeld aan een organisatie
<b>Token5:</b> Isabel IntelliSign (for EBB channel) - van toepassing op gebruikers gekoppeld aan een

organisatie
<b>Token6:</b> Isabel Isakey (for EBB channel) - van toepassing op gebruikers gekoppeld aan een organisatie

Deze middelen kunnen onafhankelijk van de registratiemethode worden gebruikt. Ze zijn ofwel gekoppeld aan de persoon op het moment van registratie, ofwel achteraf gekoppeld aan de persoon, via een beveiligd kanaal (EBW of EBB) op basis van een geauthenticeerd verzoek van de persoon in kwestie (op basis van de authenticatie- en autorisatiemiddelen die op het moment van registratie zijn verstrekt).

### XI.A.3. Stap 3: autorisatie (AUT)

De natuurlijke persoon ondertekent een challenge met behulp van zijn authenticatie-/autorisatiemiddel (onder zijn controle) in zijn elektronische bankkanaal om de ondertekening van het (de) voorgelegde document(en) te autoriseren.

De in [4] beschreven middelen voor het autoriseren van een handtekening in overeenstemming met deze RP/RPS zijn:

<b>Token1:</b> The BNPPF app based on Gemalto (for both EBW and EBB channels)
<b>Token2:</b> Itsme (for both EBW and EBB channels)
<b>Token3:</b> The EMV card (M1 – M2 signature with an UCR token, for both EBW and EBB channels)
<b>Token4:</b> Isabel card (for EBB channel)
<b>Token5:</b> Isabel IntelliSign (for EBB channel)
<b>Token6:</b> Isabel Isakey (for EBB channel)

Het middel dat wordt gebruikt om de handtekening te autoriseren, is het middel dat werd gebruikt voor authenticatie. Voor dezelfde middelen verschilt het autorisatieprotocol echter over het algemeen van het authenticatieprotocol (bijv. voor EMV-kaarten is authenticatie gebaseerd op het gebruik van de M1-modus, terwijl autorisatie is gebaseerd op een M2-handtekening. Hetzelfde geldt voor itsme, dat verschillende protocollen aanbiedt, afhankelijk van het gebruik).

Met deze stap wordt de aanvraag voor het maken van een ondertekeningscertificaat geformaliseerd.

Als dit verzoek geldig is, wordt een certificaataanvraag gestuurd naar de technische RA die daarop een certificaat genereert op naam van de natuurlijke persoon (voornaam – achternaam – SMID).

