



BNP Paribas Fortis Registration Policy
Registration Authority
of the Mediacert Certification Authority

itg



Review			Approval		
Name	Position	Date	Name	Position	Date
			PMA	Governing body	18/10/23

Versioning			
Version	Date	Author	Nature of the changes
0.4.1	23/09/2020	SealWeb	Document initialisation
0.4.2	21/10/2020	SealWeb	Finalisation of the document for approval
0.4.3	07/11/2020	SealWeb	Consideration of the latest Worldline comments
0.4.4	19/11/2020	SealWeb	Consideration of Fortis feedback
1.0.0	13/10/2021	ITA	Internal review, consideration of BNP Paribas Fortis Legal comments <ul style="list-style-type: none"> Changes to I.A, 1.E.4, V.E.3, V.D.3
1.1	28/10/2021	ITA	Consideration of BNP Paribas Fortis Legal comments following the PMA: <ul style="list-style-type: none"> Changes to V.E.3
1.2	15/12/2021	MBA	Consideration of SealWeb internal audit comments <ul style="list-style-type: none"> Changes to chapter IV.C.2 [Approved by the PMA of 21 December 2021]
1.3	09/09/2022	GFE	Changes as a result of: <ul style="list-style-type: none"> new channels: EBA, EBBM new token: Easy PIN (Gemalto) in EBA, EBBM itsme means of authorisation changes to the OU field of the certificate distinction between web & mobile screen layouts [Validated by the PMA of 19 September 2022]
1.4	01/04/2023	RZE	Taking into account the transfer of the activity from Worldline to Worldline France on the migration of the PKI "Mediacert Root CA 2018" (and AC 2019) to "Mediacert Root CA 2021" Taking into account Worldline's remarks and the change in the OIDs of Mediacert's 2021 CA OTU (active on 17 February 2022 for Worldline France/Mediacert): change from 1.2.250.1.111.20.5.5 to 1.2.250.1.111.20.5.6

Contents

I.	Introduction	6
I.A.	General introduction	6
I.B.	Identification of the document.....	6
I.C.	Entities operating within the PKI	6
I.D.	Use of certificates	11
I.E.	Management of this Registration Policy	11
I.F.	Definitions and acronyms	12
II.	Responsibilities concerning the provision of information to be published.....	15
II.A.	Companies responsible for providing information	15
II.B.	Information to be published	15
II.C.	Publication deadlines and frequency.....	15
II.D.	Control of access to published information.....	15
III.	Identification and authentication	15
III.A.	Naming.....	15
III.B.	Initial identity verification.....	18
III.C.	Validation of the applicant's authority	19
III.D.	Identification and approval of a key renewal application	19
III.E.	Identification and approval of a revocation application.....	19
IV.	Operational requirements on the life cycle of certificates.....	19
IV.A.	Origin of a certificate application	19
IV.B.	Processes and responsibilities for drawing up a certificate application.....	19
IV.C.	Processing a certificate application	20
IV.D.	Issue of the certificate.....	20
IV.E.	Certificate acceptance	20
IV.F.	Uses of dual keys and certificates	21
IV.G.	Renewal of certificates.....	21
IV.H.	Issue of a new certificate following a change to the dual key.....	21
IV.I.	Amendment of certificates	21
IV.J.	Revocation and suspension of certificates	22
IV.K.	Information on the status of certificates	23
V.	Non-technical security measures	23
V.A.	Physical security measures	23

V.B.	Procedural security measures	24
V.C.	Security measures vis-à-vis staff	24
V.D.	Procedures for the creation of audit data	26
V.E.	Archiving of data	27
V.F.	Authority key changeover	28
V.G.	Recovery following compromise or incidents	28
V.H.	RA end of life	28
VI.	Technical security measures	28
VI.A.	Dual key generation and installation.....	29
VI.B.	Security measures for the protection of private keys and for cryptographic modules.....	29
VI.C.	Other dual key management aspects	30
VI.D.	Activation data	31
VI.E.	IT system security measures	31
VI.F.	Security measures associated with system development	31
VI.G.	Network security measures	31
VI.H.	Time-stamping/dating system.....	31
VII.	Profiles of certificates, OCSPs and CRLs	32
VIII.	Compliance audit and other assessments.....	32
VIII.A.	Frequency and/or circumstances of assessments	32
VIII.B.	Identities/qualifications of assessors	32
VIII.C.	Relations between assessors and assessed entities	32
VIII.D.	Subjects covered by the assessments	32
VIII.E.	Actions taken following the assessment findings	32
VIII.F.	Communication of results	32
IX.	Other business and legal issues.....	33
IX.A.	Rates.....	33
IX.B.	Financial liability.....	33
IX.C.	Confidentiality of business data	33
IX.D.	Personal data protection.....	33
IX.E.	Intellectual and industrial property rights	34
IX.F.	Contractual interpretations and guarantees	34
IX.G.	Certificate users	34
IX.H.	Other participants	35
IX.I.	Guarantee limit	35

IX.J.	Limit of liability	35
IX.K.	Compensation.....	35
IX.L.	Duration and early end of validity period of the RP	35
IX.M.	Amendments to the RP.....	35
IX.N.	Dispute resolution provisions.....	36
IX.O.	Courts with jurisdiction.....	36
IX.P.	Compliance with legislation and regulations.....	36
IX.Q.	Miscellaneous	36
IX.R.	Other provisions.....	36
X.	Annex – Referenced documents	36
X.A.	Regulations	36
X.B.	Technical documents.....	36
XI.	Annex: Registration procedures – authentication and authorisation accepted under this RP	37
XI.A.	EMV card-based procedure for retail customers	37
XI.B.	PRO card-based procedure for business customers	37
XI.C.	itsme-based procedure for retail customers	38
XI.D.	itsme-based procedure for business customers.....	38
XI.E.	Easy PIN (Gemalto)-based procedure for retail customers.....	39
XI.A.	Easy PIN (Gemalto)-based procedure for business customers	40

I. Introduction

I.A. General introduction

This document sets out the Registration Policy applicable to certificates of BNP Paribas Fortis customers.

- **issued by the 'Mediacert OTU CA 2021' and 'Mediacert OTU CA S2 2021' of Worldline France certification authorities (hereinafter 'OTU CA') acting as a certification service provider,**
- **in order to meet business application reliability requirements (in particular, in the case of online banking applications).**

This Registration Policy (hereinafter 'RP') applies to the issue of electronic signature certificates for documents in PDF, XML (XAdES, XML-DSig) or CMS format.

The 'OTU CA' authority meets the signature needs of BNP Paribas Fortis customers, users of personal certificates, and is part of the public key infrastructure (PKI) used by the BNP Paribas Group.

This Registration Policy is part of a process for certifying compliance of registration requirements and practices with the European ETSI EN 319 411–1 LCP level standard, the purpose of which is to describe:

- **The commitments of the 'FORTIS RA' Registration Authority relating to the definition of rules of issue and management of certificates issued by 'OTU CA', as well as their implementation**
- **The conditions of use of certificates issued by 'OTU CA' on behalf of BNP Paribas Fortis registered and requested by the 'FORTIS RA'.**

This Registration Policy meets the requirements of the 'Lightweight Certificate Policy' (LCP) defined in standard ETSI EN 319 411-1. The LCP OID is as follows: 0.4.0.2042.1.3.

It also aims:

- **To comply with the registration requirements imposed on 'OTU CA' (OID 1.2.250.1.111.20.5.6.1 and 1.2.250.1.111.20.5.6.5) as described in the Mediacert Certification Policy (CP)¹**
- **To comply with Adobe AATL program registration requirements**

I.B. Identification of the document

This Registration Policy is identified by its object identifier (OID, footer on each page of the document). It can also be identified by other, more specific information such as name, version number and date of most recent update.

OID of this Registration Policy

1.2.250.1.62.10.202.6.5.1

I.C. Entities operating within the PKI

To clarify and facilitate identification of requirements, and in line with ETSI documents in the area of the

¹ Available at: [Certification Authority - Mediacert](#)

functional breakdown of 'OTU CA', it is organised around the following entities:

- **Certification Authority (CA)**
- **Registration Authority (RA)**
- **Certificate holders**
- **User application (application for the signature of documents made available to its customers by BNP Paribas Fortis)**
- **PMA (Policy Management Authority): governing body of the BNP Paribas and Fortis RA signature department.**

The scenarios of use covered by the RP do not require any confiscation functions.

'OTU CA' shall appoint a certificates manager for the management of its PKI, in particular as interface with the operator.

In the context of the 'OTU CA' certification service provision, which it provides directly, 'OTU CA' is a service external to BNP Paribas. However, in the course of its business, it delegates a number of responsibilities to BNP Paribas Fortis. In particular, BNP Paribas Fortis, a legal entity under Belgian law, undertakes to comply with the following requirements:

- **Being in a contractual relationship or being in the process of entering into a relationship with end customers for whom it is responsible for ensuring:**
 - o **The issue and management of certificates using 'OTU CA' public key infrastructure (PKI);**
 - o **The definition, for the scope of certificates issued for BNP Paribas, of registration rules for holders with a view to the issue of certificates by 'OTU CA' and the correct application thereof;**
 - o **The definition of conditions of use of certificates issued by 'OTU CA' on behalf of BNP Paribas Fortis;**
- **The submission of certificates to the user application, on behalf of the holder of certificates issued by 'OTU CA' and for which, through BNP Paribas Fortis, MediaCert is responsible for managing the certificates of holders and customers of BNP Paribas Fortis.**

I.C.1. Certification Authority

The 'OTU CA' Certification Authority is responsible for the provision of services relating to the management of certificates throughout their life cycle (generation, dissemination, renewal, revocation, etc.) using public key infrastructure (PKI).

To clarify and facilitate identification of requirements, and in line with ETSI (European Telecommunications Standards Institute) documents in this area, the functional breakdown of this PKI is as follows:

- **Certificate generation feature – This feature generates certificates (creation of format, electronic signature with associated private key):**
 - o **Using tools specific to technical components or future certificate holders; or**
 - o **Using the tools of its PKI.**
- **Delivery to holder feature – This feature delivers to the user application, on behalf of the holder, as a minimum, the certificate or certification chain.**
- **Publication feature – This feature makes the following available to the various stakeholders: policies published, authority certificates and any other relevant information aimed at holders and/or users of certificates, apart from certificate status information.**
- **Revocation management feature – This feature processes revocation applications and determines the actions to be taken. The processing outcomes are disseminated via the certificate status information feature. In the context of this RP and use of the CA by the BNP**

Paribas signature department, requests for technical revocations are made to the CA by the BNP Paribas signature department on certain occasions during the signing process (e.g. refusal to sign by the future holder) described in this RP.

- **Certificate status information feature – This feature provides users of certificates with information about the status of certificates (in particular revoked status). This feature is implemented according to an information publication method in the form of a Certificate Revocation List (CRL).**
- **PKI administration feature – This feature is associated with the role that defines the functional behaviour and technical configuration of the PKI.**

All the features provided by the PKI are described in the 'OTU CA' CP.

I.C.2. Registration Authority (RA)

The role of the FORTIS RA is to verify the identity of the requester of a certificate in order to approve the application to issue a certificate.

This feature verifies the identification details of the future holder of a certificate, and any other specific attributes, before sending the relevant application (generation, revocation) to the appropriate PKI feature.

It must apply procedures for identifying natural persons that allow for the issuing of certificates in compliance with Belgian banking regulations, in particular the regulation on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Law of 18 January 2017 on combating money laundering and terrorist financing and limiting the use of cash).

The registration procedure for certificates issued by 'OTU CA' for BNP Paribas Fortis consists of two steps, as described below. Step 1 is carried out once and is a prerequisite for the next step.

1) Step 1: Registration

Step 1 is carried out once, when the natural person enters into a relationship with the bank. It is made up of three elements:

- **Step REG 1.1** *Creation of an identity file for the natural person and retention of the identity documents provided by the latter (REG1). These documents are stored electronically. Their validity is maintained over time in accordance with Belgian banking regulations. All documentary proof of identity is stored in the bank archiving system, and this is made available to all BNP Paribas Fortis bank branches.*
- **Step REG 1.2** *Verification that the identity data collected in 1.1 belongs to the person presenting themselves as a customer of the bank or authorised representative (REG2); verification of identity data on the basis of supporting documents in accordance with the regulations applicable to credit institutions. This is carried out face-to-face or equivalent using one of the means described in III.B.3. When the identity data is verified, during the face-to-face meeting with the customer, an acceptance process is initiated to become a customer of the bank or authorised representative.*
- **Step REG 1.3** *Allocation or identification of a strong means of authentication that the person will use to log in and/or give their consent (authorisation) during subsequent contacts with the user application (ENR.AUTH). This is an authentication system (AUTH) that uses the authentication methods recognised by the bank and a high level of assurance regarding the person's identity.*

The means of authentication accepted in the context of this RP are:

- the smart bank card (EMV standard), which allows for authentication using the M1 protocol with a UCR reader through a secure channel between the customer and the bank (EBW, EBB)
- the Isabel card (supplied by BNP Paribas Fortis or another bank), which allows for authentication using a certificate and card reader through a secure channel between the customer and the bank (EBB)
- the itsme system, which allows for authentication through a secure channel between the customer and the bank (EBW, EBB)
- the Easy PIN system (Gemalto), which allows for authentication through a secure channel between the customer and the bank (EBA, EBBM)
-

The following means of authorisation are accepted:

- the smart bank card (EMV standard), which allows for signing using the M2 protocol with a UCR reader through a secure channel between the customer and the bank (EBW)
- the Isabel card (supplied by BNP Paribas Fortis or another bank), which allows for signing with a certificate and card reader through a secure channel between the customer and the bank (EBB)
- the itsme system, which allows for signing through a secure channel between the customer and the bank (EBW, EBB)
- the Easy PIN system (Gemalto), which allows for signing through a secure channel between the customer and the bank (EBA, EBBM)

The processes for activating and using the means of authentication and authorisation and the technical details of these means of authentication and authorisation are detailed in the annex of this RP (Chapter XI). Only the combinations of means of authentication and authorisation described in this annex are allowed. It should be noted that some means can be used for authentication and authorisation.

2) Step 2: certificate application and use

Step 2, which is based on the information recorded in step 1, is carried out whenever the natural person applies for a lightweight certificate; i.e., whenever a transaction requiring a signature is necessary. It requires strong authentication of the person, using one of the authentication methods recorded for this person in 1.3.

This step occurs during the online contracting process, which is twofold:

- *initiation of the online contracting process, which requires prior authentication of the customer via one of the means of authentication accepted by BNP Paribas Fortis (listed above).*
- *initiation of the process that allows for electronic signature, following the previous step.*

The customer agrees to one or more specific documents to be signed. If the customer ticks the confirmation box, they can then formalise the signature request using one of the means of authorisation accepted by BNP Paribas Fortis (listed above).

The customer must first:

- **accept the Fortis signature department Terms of Use (ToU) and give their consent to the use of their personal data for the issue of a certificate in their name;**
- **accept the TSP Mediacert Terms of Service (ToS) by accepting the Fortis signature department ToU.**

If this request is valid, a certificate application will be sent to the technical RA, which will generate a certificate in the name of the natural person.

Note 1: at this stage, if **the customer does not complete the step**, the signature process is cancelled. No certificate is generated.

Note 2: it is also this step that links the request to the data to be signed.

This step formalises the request to create a signature certificate.

Then there is a distinction depending on the screen layout:

1) Mobile layout:

There are no additional steps as the customer declares on this screen, by ticking the box stating that they 'have read the 'Terms of Use of electronic signature certificates', that all data is correct and that a certificate bearing their name can be created under these conditions'.

2) Web layout: A second authorisation screen allows the natural person to give their consent to the creation of an electronic signature in their name based on their identification details taken from the certificate (first name and surname as shown on the screen) on the specific contractual document.

Note 1: at this stage, the customer can view the ToU and RP, as well as the CP and Mediacert ToS.

Note 2: the customer's identification details taken from the certificate generated are shown again.

This step also confirms acceptance of the certificate and approves its content, in particular the personal data it contains.

This process formalises the electronic signature request. Consequently, the certificate generated is used to sign the document legally binding the customer or authorised representative to the bank.

For revocation, see Chapter IV.J.

I.C.3. Functional breakdown of the RA

The BNP Paribas Fortis PKI implements two components of the RA:

- **Functional RA: responsible for initial verification of the identity of the natural person and retention of the proof of identity provided by the latter (REG1 and REG2), and subsequent verification of the identity of the natural person during each transaction that may give rise to the issue of a certificate (AUTH). The functional RA is responsible for:**
 - o **Retention of the verification elements of the certificate holder pursuant to the regulations applicable to credit institutions.**
 - o **Keeping all of the holder's personal authentication data confidential, in compliance with banking regulations.**

All information relating to confidential data is stored in the banking archiving system.
- **Technical RA: responsible for the creation of keys and submission of certificate applications to the Certification Authority. It also generates an evidence file for signature validation at the time of each signature by the holder**

I.C.4. Certificate holder

In this Registration Policy, a certificate holder is a customer of BNP Paribas Fortis.

I.C.5. Certificate user applications

The certificate user applications are as follows:

- ***An electronic signature creation application made available to the certificate holder by BNP Paribas Fortis;***
- ***All electronic signature display and validation software programs.***

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

The PMA is the governing body of BNP Paribas RAs, whose main responsibilities are to:

- ***Define, review, approve and enforce Registration Policies and Registration Practice Statements;***
- ***Manage all risks related to the RA;***
- ***Define and manage the trusted staff or entity operating the RA;***
- ***Manage relations with external entities, in particular 'OTU CA';***
- ***Take all necessary actions to ensure performance of all the tasks listed previously.***

I.D. Use of certificates

The lightweight certificates issued in the context of this Registration Policy are only used in connection with the use of electronic signature solutions and approval of documents in a format defined by BNP Paribas Fortis.

The only permitted use is personal signature through the 'Non Repudiation' value (2.5.29.15(1)) of the 'Key Usage' extension, as defined in the 'OTU CA' CP.

I.E. Management of this Registration Policy

I.E.1. Entity managing the Registration Policy

The entity responsible for the administration and management of this Registration Policy is GITT. It is responsible for the preparation, follow-up and amendment, as necessary, of this RP.

GITT is the Group IT and Technology department.

This RP is reviewed by the entity managing the 'OTU CA' Certification Policy in order to ensure that the commitments of this RP are properly aligned with that described in the 'OTU CA' CP. This RP is approved through the RA audit (see VIII).

I.E.2. Point of contact

BNP Paribas Fortis can be contacted for any questions relating to this RP via the Easy Banking Centre (EBC) on 02 762 20 00 (FR) or 02 762 60 00 (NL).

Fintro can be contacted for any questions relating to this RP via Easy Banking Fintro (Web & App) on 02 433 45 20 (FR) or 02 433 45 10 (NL).

Hello Bank can be contacted for any questions about this RP via Hello Bank! on 02/433 41 42 (FR) or 02/433 41 41 (NL).

The Easy Banking Business Helpdesk can be contacted for any questions relating to this RP via the EBB Helpdesk on 02 565 05 00.

If the response or processing is still not satisfactory, the Complaints Management Department may be asked to intervene.

I.E.3. Entity determining compliance of the Registration Practice Statement (RPS) with this Registration Policy

The PMA (Policy Management Authority), the RA governing body, designates the persons (or departments) determining compliance of the Registration Practice Statement (RPS) with this Registration Policy

I.E.4. RP compliance approval procedures

This Registration Policy will be reviewed at the time of each major change and at least annually by the PMA (Policy Management Authority), the governing body of this RA, to ensure:

- ***its compliance with the security standards expected by the national inspection body (cf. European Regulation eIDAS 910/2014);***
- ***the requirements set out in the 'OTU CA' CP.***

This RP is reviewed by the entity managing the 'OTU CA' Certification Policy in order to ensure that the commitments of this RP are properly aligned with that described in the 'OTU CA' CP. Approval of this RP for the entity managing the 'OTU CA' Certification Policy is based on the RA audit (see VIII).

In addition, this Registration Policy will be approved during PMA proceedings.

I.F. Definitions and acronyms

The acronyms used in this RP are as follows:

- ***AA: Archiving Authority***
- ***CA: Certification Authority***
- ***RA: Registration Authority***
- ***ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information*** [French National Agency for the Security of Information Systems]
- ***ToS: Terms of Service of the Mediacert TSP, within the framework of the electronic signature and issue of electronic certificates***
- ***ToU: Terms of Use of the signature department***
- ***ToM: Terms of Membership***
- ***CRL: Certificate Revocation List***
- ***DN: Distinguished Name***
- ***CPS: Certification Practice Statement***
- ***RPS: Registration Practice Statement***
- ***ETSI: European Telecommunications Standards Institute***
- ***PKI: Public Key Infrastructure***
- ***OID: Object Identifier***
- ***OCSP: Online Certificate Status Protocol***
- ***PMA: Policy Management Authority***
- ***CP: Certification Policy***
- ***RP: Registration Policy***
- ***SGRG: Security General Reference Guide:***
- ***RSA: Rivest Shamir Adleman***
- ***SIS: Security of Information Systems***
- ***URL: Uniform Resource Locator***

Public Key Infrastructure (PKI)	All physical components, procedures and software making it possible to manage the life
---------------------------------	--

	cycle of certificates and to offer authentication, encryption and signature services.
Certificate	Electronic file issued by a Certification Authority certifying the identity of a holder (natural person, machine, etc.). The certificate is valid for a given term specified therein.
Certification Authority (CA)	Entity responsible for signing, issuing and maintaining the certificates of a public key infrastructure, in accordance with a Certification Policy. Application service providers using certificates issued by the Certification Authority of the holder of the certificate.
Certification Policy (CP)	All rules and requirements to which a Certification Authority is subject in the implementation and provision of its services.
Registration Policy (RP)	All rules and requirements to which a Registration Authority is subject in the implementation and provision of its services.
Certification Practice Statement (CPS)	Description of practices (organisation, operational procedures, technical and human resources) applied by the Certification Authority in the context of the provision of its electronic certification services, in accordance with the Certification Policy or policies with which it has undertaken to comply.
Registration Practice Statement (RPS)	Description of practices (organisation, operational procedures, technical and human resources) applied by the Registration Authority in the context of the provision of its electronic certification services, in accordance with the Registration and Certification Policy or policies with which it has undertaken to comply.
Certificate Revocation List (CRL)	List published by the Certification Authority of certificates that are no longer reliable (revoked, invalid, etc.). For simplicity, this also includes authority

	revocation lists (known as ARL).
OCSP responder	Online certificate status service
X 509	Standard of the International Telecommunication Union (ITU) relating to public key infrastructures (PKI), including the standard formats of its components: electronic certificates, revocation lists, validation algorithm, etc.
UTF-8	Encoding of characters defined by Unicode where each character is encoded on a series of one to six 8-bit words (there are currently no characters encoded with more than four words)
Distinguished Name (DN)	Element making it possible to identify a holder or Certification Authority in a unique way.
Object Identifier (OID)	Universal identifier, represented in the form of a series of whole numbers associated in the context of a PKI with a reference element such as the Certification Policy or Certification Practice Statement.
Isabel Card	A type of card from the company Isabel with very secure technology that allows for technically secure authentication and high-level legal identification.
EBB Card	A type of card from the company Isabel for the EBB platform with very secure technology that allows for technically secure authentication and high-level legal identification.
eID Belgium	A type of identification card from the Belgian government with very secure technology that allows for technically secure authentication and high-level legal identification.

II. Responsibilities concerning the provision of information to be published

II.A. Companies responsible for providing information

For the provision of information to be published for holders and users of certificates, the 'FORTIS RA' Registration Authority relies on the 'OTU CA' publication department, which is responsible for its publication².

The CA's Certification Policy specifies the provision methods and corresponding URLs (publication web servers) for the CA's documents (CP, CA certificates, CRL, etc.).

Additional documents relating to this RA (this RP, the ToU) follow the same publication practices³.

II.B. Information to be published

In addition to the information described in the 'OTU CA' CP, the following information is published:

This Registration Policy	https://www.mediacert.com/
The ToS of lightweight certificates	https://www.mediacert.com/certification/en/wls-otu-f022

II.C. Publication deadlines and frequency

For information related to the RA (new version of the RP, Terms of Use), information is published as soon as necessary to ensure consistency at all times between the information published and the CA's actual commitments.

II.D. Control of access to published information

See 'OTU CA' CP

III. Identification and authentication

'OTU CA' rules apply here. We only specify the additional rules imposed by the RA.

III.A. Naming

III.A.1. Types of names

See 'OTU CA' CP

III.A.2. Need to use clear names

The names chosen to designate certificate holders must be clear. The DN respects the structure of the identity used in the BNP Paribas Fortis reference systems and which the bank communicates in its role as

² FORTIS also agrees to make this RP and the ToU, if applicable, available on other publication sites for operational reasons.

³ FORTIS reserves the right to change the place of publication of these documents. In such a case, this RP will be updated.

technical RA to the operator for signature of the relevant certificate.

The subject's common name (CN) must represent the identity of the recipient, whose identity must have been verified (cf. §III.B), and may not in any event represent anything other than their identity in connection with their marital status (no machine name, or the identity of another person).

III.A.3. Using pseudonyms for holders

Pseudonyms are not used for holders' certificates.

III.A.4. Rules for interpreting different forms of names

The functional RA is responsible for the uniqueness of the names of its holders and the settlement of disputes relating to claims on the use of a name by said holders.

The functional RA, in the context of entering into a relationship, carries out standardisation transformations concerning the holder's surname and first names. These transformations are limited to the following cases:

- ***the name may only contain 32 characters, which must be letters, blanks or dashes, to the exclusion of all others.***
- ***first names: only the first name may be used. The length of the first name may not exceed 16 characters and may contain only letters, blanks, dashes, full stops or commas, to the exclusion of all others.***

In addition, the following transformations will be applied:

- ***for lowercase letters, 'abcdefghijklmnopqrstuvwxyzâäåöçñéèëìíîïóôõúüý' will be converted into 'ABCDEFGHIJKLMNOPQRSTUVWXYZAAAAACNEEEEEIIIOOOOUUUUY';***
- ***for uppercase letters, 'ÀÁÂÃÄÅÇÑÉÈËËÌÍÎÏÏÒÓÔÕÛÜÝ' will be converted into 'AAAAACNEEEEEIIIOOOOUUUUY'. The detailed rules are set out in the RPS.***

III.A.5. Uniqueness of names

BNP Paribas Fortis is responsible for the uniqueness of the names of its holders and the settlement of disputes relating to claims on the use of a name by said holders.

In order to ensure continuity of the holder's unique identification within the 'OTU CA' domain, the DN in the 'Subject' field of each holder's certificate allows for unique identification of the relevant holder within the CA's domain.

Therefore, in addition to the rules defined in the 'OTU CA' CP, the SN (serialNumber) field contains a number (UUID)

Uniqueness is guaranteed by the addition of a unique number (UUID – cf. RFC 4122 –) in the SN attribute of the subject (DN) of the certificate. This unique serial number is managed by 'OTU CA'.

To this end, this DN must meet the following requirements for holders:

- ***CN = Identity of subject/natural person, in the form 'First name, Surname'***
- ***SN (surName) = surname of subject/natural person***
- ***givenName = first name of subject/natural person***

- **SN (serialNumber) = unique no. (UUID)**
- **OU =**
 - 1) Means of signature for authorisation
 - Position 1:
 - F: UCR
 - I: Isabel/intellisign
 - G: Gemalto
 - B: ITSME
 - 2) Identification of the subject/natural person
 - Position 2–11
 - SMID
 - 3) Signature strip
 - Position 12-13
 - 12: EBB
 - 49: EBA
 - 52: EBW
 - 56: EBBM

- **C = BE**

In the case of a test certificate, in accordance with §1.4.4 of the 'OTU CA' CP, the template used is the same as a lightweight certificate template. However, the DN must meet the following requirements:

- **CN (commonName) = either the identity of the subject/natural person, in the form 'First name, Surname' with the addition of 'TEST' as a prefix, or 'TEST-MONITORING'**
- **SN (surName) = either the surname of the subject/natural person with the addition of 'TEST' as a suffix, or 'TEST-MONITORING'**
- **givenName = either the first name of the subject/natural person or 'TEST MONITORING'**
- **SN (serialNumber) = unique no. (UUID)**
- **OU = F-1**
- **C = BE**

In the case of a TEST certificate, the CN field will contain the prefix 'TEST', in accordance with the 'OTU CA' CP.

III.A.6. Identification, authentication and role of registered trademarks

- **The BNP PARIBAS trademark is a registered trademark of BNP PARIBAS including BNP PARIBAS**, a European Union trademark filed with the EUIPO on 8 October 1999 in classes 35, 36 and 38 and registered on 19 January 2001 under number 1338888.
- **BNP PARIBAS**, a European Union trademark filed with the EUIPO on 25 November 2005 in classes 9, 35, 36 and 38 and registered on 24 January 2007 under number 004743639

BNP Paribas Fortis is a registered trademark of BNP Paribas Fortis NV, filed with the Benelux Office for Intellectual Property on 3 January 2013 in classes 35, 36 and 42 and registered on 7 January 2013 under number 931084

The **Fintro** trademark is a registered trademark of BNP Paribas Fortis NV, including:

- FINTRON, a Benelux trademark filed with the Benelux Office for Intellectual Property on 27 September 2004 in class 36 and registered on 10 March 2005 under number 764125.
- FINTRON, a European Union trademark filed with the EUIPO on 27 September 2004 in class 36 and registered on 10 May 2007 under number 004046173.

III.B. Initial identity verification

III.B.1. Method for proving possession of private keys

The certificate application generated by the BNP Paribas technical RA is signed using the associated private key, the dual key being generated by a cryptographic module of the BNP Paribas technical RA.

III.B.2. Verification of identity of the BNP Paribas customer body

Not applicable.

III.B.3. Verification of identity of an individual

Registration of a holder for the issue of a certificate is carried out by BNP Paribas Fortis in its functional RA role.

The rules for verification of the holder's identity are left to the discretion of BNP Paribas Fortis in the course of its business and in its role as functional RA. However, these verification rules must:

- ***Be documented in the BNP Paribas RPS***
- ***Meet, as a minimum, the requirements of ETSI EN 319411–1 for the LCP level***
- ***Meet AATL program requirements***
- ***Comply with the requirements of the 'OTU CA' CP***

These rules must comply with the requirements of Chapter 3.2.2.2 of the 'OTU CA' CP, in particular:

- ***The certificate application must be signed electronically.***
- ***Identity verification must be carried out in the context of KYC regulations using one of the following identity documents:***
 - o ***The Belgian electronic identity card for Belgian residents***
 - o ***The national identity card or passport issued by the country of residence is used for non-residents.***
- ***The validity date of the identity document must be checked***

BNP Paribas Fortis may, in a future version of this RP, extend the means of identity verification provided that these means are of an equivalent or higher standard of reliability than the current means, and comply with the ETSI 319411–1 standard for the LCP level and AATL requirements⁴.

The procedure for issuing a certificate is based on the specifications of the technical RA, which uses the holder's information based on data sent by the BNP Paribas Fortis business application to the technical RA.

The procedure for verification of the holder's identity in the form 'First name, Surname' is the sole responsibility of BNP Paribas Fortis in the context of its banking activity.

⁴ The means of verification will be subject to explicit acceptance by the CA, as part of the process of updating this RP.

The common name (CN) of the certificate may only be associated with a natural person and not with a service name, application or similar.

III.B.4. Unverified holder information

All certified information is verified.

III.C. Validation of the applicant's authority

See Chapter III.B.4

III.C.1. CA cross-certification

Not applicable for a Registration Policy. See 'OTU CA' CP.

III.D. Identification and approval of a key renewal application

III.D.1. Identification and approval of a routine renewal

In accordance with the document [RFC 3647], the notion of 'certificate renewal' corresponds to the issue of a new certificate for which only the validity dates are changed. All other information is identical to the previous certificate (including the holder's public key).

Renewal does not apply in the context of this RP.

III.D.2. Identification and approval of renewal after revocation

Not applicable.

III.E. Identification and approval of a revocation application

The application for revocation of the final certificate can only be made by the holder in the context of their online transactions. Acceptance of the revocation application is automatic. The holder applies for revocation by cancelling the signature request, particularly if the CN information contained in the lightweight certificate (First name, Surname) shown to it is incorrect.

The terms and conditions of this application are specified in Chapter IV.A

IV. Operational requirements on the life cycle of certificates

IV.A. Origin of a certificate application

Under this RP, the certificate application can only be issued by a business application of BNP Paribas Fortis in its functional RA role. The BNP Paribas Fortis business application and the technical RA are strongly authenticated by certificate for any holder certificate application.

IV.B. Processes and responsibilities for drawing up a certificate application

The certificate application requires strong authentication of the technical components of the BNP Paribas Fortis functional RA and technical RA, using secure protocols that use authentication certificates.

- ***The functional RA must verify the status of these certificates before processing the application.***
- ***The BNP Paribas Fortis functional RA is responsible for verifying the integrity of the data it sends to the technical RA.***

The process for drawing up a holder certificate is described in Chapter I.C.2.

IV.C. Processing a certificate application

IV.C.1. Implementation of the application identification and approval processes

The procedure for identification and approval of the holder's certificate application is as follows:

- ***The application is prepared automatically by the BNP Paribas Fortis functional RA in electronic form and sent to the technical RA.***
- ***Proof of possession of the key is generated and formatted by the technical RA, with the information to be certified, in the form of a certificate application.***
- ***This proof is sent to 'OTU CA' for signature***

IV.C.2. Acceptance or rejection of the application

The Registration Authority automatically agrees to apply to the Certification Authority for the certificate following authentication of the holder with one of the means of authorisation accepted by BNP Paribas Fortis and listed in clause I.C.2.

The document is submitted to the holder by the BNP Paribas Fortis business application and the holder gives their consent before signature.

In the event of rejection, the holder is informed by the BNP Paribas Fortis business application.

IV.C.3. Duration of preparation of certificate

The certificate is prepared within thirty (30) hours of receipt of the application by the technical RA.

IV.D. Issue of the certificate

IV.D.1. Actions of the CA concerning issue of the certificate to the holder

After authentication of the technical RA vis-à-vis 'OTU CA', the certification application sent by the technical RA is automatically signed by 'OTU CA' after checking that its content meets the requirements, namely:

- ***The syntax respects the attributes of the subject (DN), cf. §III.A.5;***
- ***The cryptographic attributes of the application (key size).***

IV.D.2. Notification of certificate issuance to the holder

This is an automatic operation in the electronic signature process.

The certificate is sent to the holder via a signed document submitted at the end of a BNP Paribas Fortis business transaction.

IV.E. Certificate acceptance

IV.E.1. Certificate acceptance procedure

The holder gives their consent by:

1) Web layout screens: explicitly accepting the CN of the certificate generated in their name; see Chapter I.C.2. They agree to sign the data presented to them by the BNP Paribas Fortis functional RA.

2) Mobile layout screens: ticking the box indicating that the customer declares that they 'have read the 'Terms of Use of electronic signature certificates', that all data is correct and that a certificate bearing their name may be created under these conditions'.

IV.E.2. Publication of the certificate

The certificate will not be published.

IV.E.3. Notification of certificate issuance

In accordance with the 'OTU CA' CP, the CA sends the certificate produced to the RA in response to processing the certificate creation application. The RA in turn sends it to the BNP Paribas signature facility. This submission constitutes notification

IV.F. Uses of dual keys and certificates

IV.F.1. Use of private keys and certificates by the holder

As regards the lightweight certificate of the signatory, the use of the holder's private key generated by the BNP Paribas signature department and the associated certificate, issued within the framework of this RP, is strictly limited to the signature service offered by BNP Paribas. By design, the BNP Paribas Fortis business application does not allow any other use of private keys⁵.

The Terms of Use of the certificate specify the roles and responsibilities of the parties.

IV.F.2. Use of private keys and certificates by the user of the certificate

The technical RA generates an evidence file (audit trail, optionally business data from the BNP Paribas Fortis application, signature validation evidence files) at the time of each signature by the holder.

The private key of a lightweight electronic signature certificate is destroyed at the end of the user transaction.

IV.G. Renewal of certificates

Not applicable in the context of this RP.

IV.H. Issue of a new certificate following a change to the dual key

A change to the dual key for a lightweight certificate will be considered as an application for a new certificate. This can be done for a given holder under the responsibility of the functional RA at the end of life of a previous certificate.

The issuing procedure will be the same as for an original certificate.

IV.I. Amendment of certificates

Amendment of a certificate corresponds to the issue of a new certificate for the same public key, following changes to information other than validity dates and serial number (otherwise, this is a certificate renewal).

⁵ It should be noted that 'OTU CA' may issue certificates outside the scope of this RP, e.g. for other customers.

Amendment of certificates is not authorised within the scope of this RP.

IV.J. Revocation and suspension of certificates

Suspension does not apply in the context of this RP.

Information on revocation of final certificates will be given below.

IV.J.1.Possible causes of a revocation

The following circumstances may result in revocation of a holder's certificate, in addition to those described in the CP:

- ***The information on the holder's certificate does not match their identity;***
- ***The holder has discontinued their electronic signature transaction⁶.***

IV.J.2.Origin of a revocation application

. On the screens,

1) Web layout: the holder's identity is shown to the holder based on the CN resulting from their certificate. If this identity is incorrect, the holder must reject this certificate using a "Cancel" feature in the online application.

2) Mobile layout: the holder's identity, used for the CN of their certificate, is shown to the holder. If this identity is incorrect, the holder must not complete the step. If the customer does not complete the step, the signing process is cancelled. No certificate is generated.

IV.J.3.Procedure for processing a revocation application

A holder's revocation application is processed automatically by the technical RA.

IV.J.4.Deadline given to the holder to submit the revocation application

Due to its nature, a revocation application must be processed urgently. Revocation of the certificate is effective when the certificate serial number is included on the 'OTU CA' revocation list, and when this list is available to download.

Due to the nature of the certificates issued (life cycle limited to no more than the duration of the signature session), as indicated in the Mediacert CP, revocation is 'primarily a means of providing a CRL for technical components that are required to have one'. However, the task is carried out by the CA and used by the BNP Paribas signature department. As the revocation application must be made during the validity period of the certificate, the application must be processed during the session time of an electronic signature of a BNP Paribas application.

To this end, the BNP Paribas signature department automatically creates a revocation application for 'OTU CA' when the events described in IV.J.1 occur.

⁶ In this case, the RA automatically sends a revocation application to the CA.

IV.J.5. Deadline for processing a revocation application

See 'OTU CA' CP.

IV.J.6. Requirements for verification of the revocation by certificate users

In addition to the requirements of the 'OTU CA' CP, the technical RA is required to verify that the certificate of the 'OTU CA' Certification Authority that issued the holder's certificate is valid.

IV.J.7. CRL drafting frequency

See 'OTU CA' CP.

IV.J.8. Maximum deadline for publication of a CRL

See 'OTU CA' CP.

IV.J.9. Availability of an online system for verification of revocations and certificate status

See 'OTU CA' CP.

IV.J.10. Requirements for online verification of the revocation of certificates by certificate users

See 'OTU CA' CP.

IV.J.11. Other available information resources regarding revocations

Not applicable.

IV.J.12. Specific requirements in the case of compromise of private keys

See 'OTU CA' CP.

IV.J.13. Possible causes of a suspension

Not applicable.

IV.K. Information on the status of certificates

See 'OTU CA' CP.

V. Non-technical security measures

The requirements set out hereinafter are the minimum requirements with which BNP PARIBAS registration authorities must comply.

The confidential part of the Registration Practices Statement (RPS) describes the means implemented to comply with these requirements

V.A. Physical security measures

BNPP Paribas and BNP Paribas Fortis control physical access to RA components whose security is critical to the provision of the registration service, in order to minimise the physical security risk. In particular:

- ***Physical access to critical components is restricted to authorised persons only***

- **Controls are in place to prevent loss, alteration and compromise of assets and disruption of service.**
- **Controls are implemented to prevent information compromise or theft, especially in information processing areas**
- **Security-critical components of registration processes are located within a security perimeter with physical means of intrusion protection, such as physical perimeter access control and intrusion alarms.**

V.B. Procedural security measures

V.B.1. Trusted roles

A distinction is made between the following roles within the RA scope:

- **RA Security Officer: responsible for enforcing this Registration Policy.**
- **RA technical operators: responsible for the use, configuration and technical maintenance of equipment, cryptographic boxes and servers. In particular, they oversee the key ceremony on a technical level.**
- **Auditor: person appointed by BNP Paribas or 'OTU CA' whose role is to carry out regular compliance checks on the implementation of the features provided by the component in relation to certification and registration policies, Certification Practice Statements made by the PKI and the RA, and the component's security policies.**

V.B.2. Number of persons required per task

Depending on the type of operation carried out, the number and capabilities of persons who must be present, as actors or witnesses, may vary.

For security reasons, sensitive roles will be assigned to more than one person. This RP contains a number of requirements regarding this assignment, in particular for transactions linked to the cryptographic modules of the BNP PARIBAS signature department. These are described in the RPS.

V.B.3. Identification and authentication for each role

GITT has the identity and authorisations of all staff checked before assigning them a role and the corresponding rights. See the RPS for more information.

V.B.4. Roles requiring a separation of powers

- **Several roles may be assigned to the same person, provided the holding of more than one role does not compromise the security of the tasks carried out. For trusted roles, it is nevertheless recommended that the same person does not hold more than one role and, as a minimum, the requirements below of not holding more than one role must be met. The role of auditor cannot be combined with any other role;**
- **the persons implementing a component cannot be the same as the persons inspecting it**

The assignments associated with each role are described in the RA's RPS and comply with the security policy of the relevant component.

V.C. Security measures vis-à-vis staff

V.C.1. Required qualifications, competences and skills

All staff required to work within RA components are contractually subject to a security and confidentiality

clause.

Each department operating an RA component must ensure that the remit of staff required to work within the component match their professional competences.

The RA must inform any person working in its trusted roles of:

- ***Their responsibilities relating to PKI services;***
- ***Procedures associated with the security of the system and staff supervision.***

Each person must have, as a minimum, the appropriate documentation concerning the operational procedures and specific tools they implement as well as the general policies and practices of the component within which they work.

The appropriate documentation is described in V.C.8

V.C.2. Procedures for background checks

The RA's staff must be identified and must not have any convictions that conflict with their duties.

V.C.3. Requirements in terms of initial training

Operating staff must be trained in the software, hardware and internal operating procedures of the component for which they work.

V.C.4. Requirements and frequency of ongoing training

The staff concerned must receive appropriate information and training prior to any changes to systems, procedures, organisation, etc., according to the nature of these changes.

V.C.5. Frequency and sequence of rotation between various duties

In terms of career management for a given operator, the rules applicable are those practised by the employer.

V.C.6. Sanctions in the case of unauthorised actions

The Certification Authority will decide on the penalties to be applied when an employee abuses their rights or carries out an operation that is not within their remit.

V.C.7. Requirements vis-à-vis the staff of external service providers

With regard to contracted staff working for BNP Paribas and BNP Paribas Fortis, they must comply with the Human Resources policies and checks carried out by their company.

V.C.8. Documentation provided to staff

The documents that staff must have are as follows:

- ***Registration Practices Statement specific to the certification domain;***
- ***Manufacturers' documents for hardware and software used;***
- ***Certification policies supported by the component to which they belong;***
- ***'OTU CA' Certification Policy;***
- ***Internal operating procedures.***

The Registration Authority shall ensure that its staff (as defined in the RPS) have the documents identified above according to their needs as specified in the RPS.

V.D. Procedures for the creation of audit data

Logging consists of recording events manually or electronically, by entry or automatic generation.

The resulting files, in hard copy or electronic format, must allow for traceability and accountability of the operations carried out.

V.D.1. Types of event to be recorded

The BNP Paribas Group RA logs the following events automatically on start-up of a system and in electronic format, concerning systems related to the functions it implements in the context of the RA:

- **Creation/modification/removal of user accounts (access rights) and corresponding authentication data (passwords, certificates, etc.);**
- **Start-up and stoppage of IT systems and applications;**
- **Events related to logging: start-up and stoppage of the logging function, modification of logging configuration, actions taken following failure of the logging function;**
- **Connection/disconnection of users with trusted roles, and the corresponding unsuccessful attempts;**
- **Receipt of a certificate application (initial and renewal);**
- **Approval/rejection of a certificate application;**
- **Receipt of a revocation application;**
- **Approval/rejection of a revocation application.**

Each recording of an event in a log must contain, as a minimum, the following fields:

- **Type of event;**
- **Name of the operator or reference of the system triggering the event;**
- **Date and time of the event;**
- **Outcome of the event (failure or success).**

Accountability for an action lies with the person, body or system that performed it. The name or identifier of the operator must explicitly feature in one of the fields of the event log.

V.D.2. Frequency of processing of event logs

Analysis of the content of event logs must be regular, and at least once a quarter.

V.D.3. Retention period for event logs

RA event logs are kept for 7 years by keeping the evidence file.

V.D.4. Protection of event logs

The BNP Paribas Fortis Group RA puts in place the required measures to ensure the integrity and availability of the event logs for the component in question, in accordance with the requirements of this policy.

V.D.5. Procedure for backing up event logs

The BNP Paribas Group RA puts in place the required measures to ensure the integrity and availability of the events logs for the component in question, in accordance with the requirements of this policy.

A back-up copy of event logs is made after each ceremony on the BNP Paribas Group signature platforms.

V.D.6. System for collection of event logs

The BNP Paribas Group RA relies on the internal collection systems of each of its components.

V.D.7. Notification of the logging of an event to the event manager

Not applicable.

V.D.8. Assessment of vulnerabilities

The vulnerability assessment process is referenced in the BNP Paribas Fortis risk analysis on its RA.

Additional intrusion tests are carried out regularly, at least annually.

V.E. Archiving of data

V.E.1. Type of data to be archived

Archiving makes it possible to:

- **Ensure the durability of logs created by the various components of the RA.**
- **Keep paper documents associated with the operations, along with their availability if required.**

The data to be archived concerns both hard copies and electronic format.

The data to be archived is as follows:

- **The (executable) software and configuration files of IT equipment implemented by the RA**
- **This RP and the associated RPS**
- **Audit data**
- **Event logs of the various entities of the RA**
- **Paper documents associated with the RA.**

V.E.2. Procedure for the establishment of archives

See the relevant chapter of the RPS.

V.E.3. Retention period for archives

The retention period for the electronic archives is as follows:

- **Retention period for archives of event logs: 1 year**
- **Registration files and data relating to the identity of the signatory will be kept for a period of 10 years from the end of the relationship between the customer and BNP PARIBAS FORTIS.**
- **The signed document will be kept according to the type of document for a minimum of 10 and a maximum of 30 years from:**
 - o **(i) the end of the agreement**
 - o **(ii) expiry of the document if a validity period applies**
 - o **(iii) the date of the document if (i) and (ii) do not apply.**
- **Technical records ensuring the accountability of actions will be kept according to the type of document for a minimum of 10 and a maximum of 30 years from:**
 - o **(i) the end of the agreement**
 - o **(ii) expiry of the document if a validity period applies**
 - o **(iii) the date of the document if (i) and (ii) do not apply.**
- **The retention period of elements specific to the CA (CRL, technical traces of the CA, etc.) is specified in the 'OTU CA' CP**

V.E.4. Archive recovery period

Archives may be recovered within 5 working days.

V.E.5. Protection of archives

Throughout their storage, archives and their back-ups are:

- ***Protected in full;***
- ***Accessible to authorised persons;***
- ***Accessible for reading and analysis.***

The RPS specifies the methods used to archive documents securely.

V.E.6. Data time-stamping requirements

See the relevant chapter of the RPS.

V.E.7. Archive collection system

Traces of the registration process are kept in the evidence file associated with the transaction. It is kept under conditions ensuring its availability, integrity and confidentiality.

V.E.8. Procedures to recover and verify archives

Archives are managed by the BNP Paribas Group RA. The recovery process is subject to an internal operating procedure mentioned in the RPS. Recovery must be carried out within a maximum of 5 working days.

V.F. Authority key changeover

Not applicable for an RA.

V.G. Recovery following compromise or incidents

'FORTIS RA' undertakes to comply with all the recovery measures following compromise or incidents set out in the Mediacert TSP OTU CA Certification Policy, in particular:

- ***'FORTIS RA' has set out and maintains a business continuity plan in the event of an incident.***
- ***In the event of an incident, including compromise of a signature key or means of authentication, 'FORTIS RA' undertakes to implement all the measures in its business continuity plan, in particular:***
 - o ***Immediate notification of the compromise to Mediacert TSP, if applicable;***
 - o ***Implementation of appropriate remedial measures to restore operational security.***

V.H. RA end of life

In the event of end of life of the RA, all RA archives and traces will be archived by BNP Paribas. 'OTU CA' will therefore not be impacted by the stoppage of the RA. The authentication methods of the BNP Paribas technical RA will be revoked.

VI. Technical security measures

The requirements set out in the remainder of this chapter are the minimum requirements that must be met by the 'FORTIS RA' Registration Authority with regard to the dual keys of holders.

For the technical security measures applicable to CA keys, outside the scope of this document, see the 'OTU CA' CP.

The RPS describes the resources deployed in order to meet these requirements.

VI.A. Dual key generation and installation

VI.A.1. Dual key generation

A holder's dual key is generated by a hardware security module (HSM), the requirements of which are described in §VI.B.1.

VI.A.2. Transfer of the private keys to its owner

The holder's private key remains under the individual's sole control via signature software and can only be used by this software to sign a document made available by BNP Paribas Fortis or a revocation in case of a refusal to sign. It is destroyed immediately after use.

VI.A.3. Transfer of the public key to the CA

Holders' public keys are delivered to the CA based on applications generated by the signature software in a format that makes it possible to prove possession of the key by signing the application. The signature is verified by the CA. The CA issues a certificate if this verification is correct.

Issue is thus protected in full end-to-end at the time of a certificate generation application.

VI.A.4. Transfer of the public key from the CA to certificate users

See 'OTU CA' CP.

VI.A.5. Size of keys

Holders use keys with a minimum of 2048 bits.

Regarding the size of the keys, the BNP PARIBAS signature application follows ANSSI recommendations in terms of cryptographic sizes.

VI.A.6. Verification of the generation and quality of dual key settings

Dual key generation equipment uses settings that meet the security standards specific to the algorithm corresponding to the dual key (cf. Chapter VII).

VI.A.7. Life cycle of keys

See §VI.C.2.

VI.A.8. Objectives for the use of keys

For holder certificates, see I.C.4

VI.B. Security measures for the protection of private keys and for cryptographic modules

VI.B.1. Security standards and measures for cryptographic modules

The holder's private key is protected by a cryptographic box, the resistance level of which is a minimum of FIPS 140-2 level 2.

VI.B.2. Check of private keys by more than one person

The private keys of holders are not checked by more than one person. They are under the holder's control.

VI.B.3. Confiscation of private keys

Not applicable

VI.B.4. Back-up copies of private keys

There are no back-up copies of holders' private keys.

VI.B.5. Archiving of private keys

Holders' private keys are never archived.

VI.B.6. Transfer of the private key to/from the cryptographic module

Not applicable to holders' private keys

VI.B.7. Storage of the private key in a cryptographic module

Holders' private keys are stored in a cryptographic module that meets, as a minimum, the requirements below:

- **Common criteria EAL4+ , or**
- **FIPS 140-2 level 2**

VI.B.8. Method of activating private keys

Keys are activated once generated. Their use requires two-factor authentication of the holder.

VI.B.9. Method of deactivating private keys

Not applicable.

VI.B.10. Method of destroying private keys

The keys are destroyed at the end of the signing process.

VI.B.11. Level of security assessment of the cryptographic module

See VI.B.1

VI.C. Other dual key management aspects**VI.C.1. Archiving of public keys**

Holders' public keys are not archived by the RA. They are archived by the CA through the archiving of issued certificates.

VI.C.2. Life cycle of dual keys and certificates

The life cycle of certificates is 50 mins.

The life cycle of dual keys is limited to their association with a certificate.

VI.D. Activation data

VI.D.1. Generation and installation of HSM activation data

Generation and installation of activation data of a cryptographic module of the BNP Paribas signature platform occur during the cryptographic box initialisation and customisation phase. The activation data is chosen and entered by the persons responsible for this data.

It is only known to members of GITT in the context of the roles assigned to them.

VI.D.2. Protection of HSM activation data

Activation data generated for the BNP Paribas Group PKI cryptographic modules are protected in terms of integrity and confidentiality.

VI.D.3. Protection of activation data corresponding to holders' private keys

See the relevant chapter of the RPS.

VI.D.4. Other aspects relating to activation data

See the relevant chapter of the RPS.

VI.E. IT system security measures

VI.E.1. Technical security requirements specific to IT systems

See the relevant chapter of the RPS.

VI.E.2. Level of qualification of IT systems

See VI.B.1

VI.F. Security measures associated with system development

The development environments are separate from the production environment.

VI.F.1. Measures associated with security management

Any significant changes to the system of a component of the BNP Paribas Group signature infrastructure must be documented, must feature in the internal operating procedures of the relevant component and must comply with the compliance assurance maintenance schedule, in the case of assessed products.

VI.F.2. Level of security assessment of the life cycle of systems

This policy does not contain any specific requirement on the subject.

VI.G. Network security measures

Interconnections and access to the signature solution's resources are controlled by hardware and software that allow for segmentation of data, services and users by role and function. These solutions ensure control of incoming and outgoing flows. Changes to open ports, access rights and modifications must be systematically traced in a space for tracking changes to logic access.

VI.H. Time-stamping/dating system

To date these events, the various infrastructure components use system time, ensuring synchronisation among the system clocks, to at least the nearest minute, and in relation to a reliable UTC time source, to at

least the nearest second.

VII. Profiles of certificates, OCSPs and CRLs

See 'OTU CA' CP.

VIII. Compliance audit and other assessments

VIII.A. Frequency and/or circumstances of assessments

A compliance check of the scope of the BNP Paribas Group RAs, in relation to the ETSI EN 319 411-1 LCP reference system, is carried out every two years. An internal audit will be carried out by BNP Paribas every year.

VIII.B. Identities/qualifications of assessors

Auditing of a component must be assigned by BNP Paribas management to a team competent in information system security and in the field of activity of the component being audited. In particular, auditors must be familiar with the requirement repositories applicable to the scope of the RA, in particular the ETSI EN 319 411–1 standard, the Mediacert CP and the AATL requirement repository. They must take these requirement repositories into account in their audit plan and in the checks carried out.

Similarly, those carrying out internal audits must satisfy the conditions stipulated in the previous paragraph.

VIII.C. Relations between assessors and assessed entities

The organisation of internal audits is written in the associated RPS.

VIII.D. Subjects covered by the assessments

The compliance checks or internal checks carried out by BNP Paribas concern the whole of the BNP Paribas Group RA and are aimed at verifying compliance with the commitments and practices defined in this Certification Policy and the related RPS, as well as the ensuing elements (operational procedures, resources implemented, etc.).

VIII.E. Actions taken following the assessment findings

After a compliance check or internal audit, the assessor will provide the GITT with a compliance report, accompanied by recommendations.

The GITT, by delegation to the actors identified in this policy, is responsible for settling areas of non-compliance and choosing the measure to be applied.

VIII.F. Communication of results

The results of compliance audits are confidential and can only be communicated to third parties in the case of an explicit request.

Moreover, the results of the compliance audits and audits carried out internally will be communicated to the PMA and 'OTU CA'.

IX. Other business and legal issues

IX.A. Rates

Not applicable.

IX.B. Financial liability

In the event of adverse mismatches for the service provider between licences purchased/used, we can specify that, effectively and in accordance with the agreement signed with the service provider, BNP PARIBAS will remain financially liable and must remedy the situation as soon as possible. However, the service provider may claim damages.

IX.C. Confidentiality of business data

IX.C.1. **Scope of confidential information**

The types of information considered as confidential are, at least, the following:

- ***The confidential part of the RPS corresponding to this RP;***
- ***The private keys of components and holders of certificates of the BNP Paribas Group signature department***
- ***All secrets of the HSM of the BNP Paribas Group signature department***
- ***Event logs of the BNP Paribas Group technical components***
- ***Holders' registration files***

IX.C.2. **Information outside the scope of confidential information**

Not applicable.

IX.C.3. **Responsibilities in terms of protection of confidential information**

As a Registration Authority, BNP Paribas Fortis, is required to comply with the legislation and regulations in force on Belgian territory.

IX.D. Personal data protection

BNP Paribas Fortis applies the applicable laws and regulations relating to the protection of personal data, both with regard to the collection and use of personal data (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)) and other applicable (national or other) data protection laws and regulations.

IX.D.1. **Personal data protection policy**

It is understood that any collection and use of personal data by all components of the BNP Paribas Group's PKI are carried out in strict compliance with the legislation and regulations in force.

IX.D.2. **Personal data**

All data concerning holders' registration files is considered personal data.

IX.D.3. **Non-personal data**

There are no specific requirements on this subject.

Responsibility in terms of personal data protection

See legislation and regulations in force on Belgian territory.

IX.D.4. Notification and consent for the use of personal data

In accordance with the laws and regulations in force in Belgium, the personal information provided by holders to the RA must not be disclosed or transferred to a third party except in the following cases: prior consent of the holder, court decision or other legal authorisation.

IX.D.5. Conditions of disclosure of personal information to the legal or administrative authorities

See legislation and regulations in force on Belgian territory.

IX.D.6. Other circumstances of disclosure of personal data

See legislation and regulations in force on Belgian territory.

IX.E. Intellectual and industrial property rights

Application of the legislation and regulations in force on Belgian territory.

IX.F. Contractual interpretations and guarantees

IX.F.1. Obligations of the CA

See 'OTU CA' CP.

IX.F.2. Obligations of the RA

The obligations of the RA are as follows:

- ***to protect and guarantee the integrity and confidentiality of their secret and/or private keys;***
- ***to use their security keys (public, private and/or secret) solely for the purposes provided for at the time of their issue and with the tools specified in the conditions set by the CA's CP, this RP and related documents;***
- ***to comply with and apply the RPS;***
- ***to submit to compliance checks carried out by the audit team commissioned by the CA or RA (see Chapter VIII);***
- ***to respect agreements or contracts between themselves or with holders;***
- ***to implement the resources (technical and human) necessary to provide the services to which they are committed in conditions that guarantee quality and security***

In addition to the above obligations, the obligations expressed in the 'OTU CA' CP apply.

IX.F.3. Certificate holders

The holder is required to check and communicate accurate and up-to-date information during the identification process (e.g. customer identity)

In addition to the above obligation, the obligations expressed in the 'OTU CA' CP apply.

IX.G. Certificate users

There are no specific requirements in the context of this RP.

The obligations of the 'OTU CA' CP apply.

IX.H. Other participants

There are no specific requirements in the context of this RP.

The obligations of the 'OTU CA' CP apply.

IX.I. Guarantee limit

BNP Paribas Fortis' liability vis-à-vis the user of the certificate is specified in the terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used. The clauses of the 'OTU CA' CP apply.

IX.J. Limit of liability

BNP Paribas Fortis' liability vis-à-vis the user of the certificate is specified in the terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used. The clauses of the 'OTU CA' CP apply.

IX.K. Compensation

BNP Paribas Fortis' financial liability vis-à-vis the user of the certificate is specified in the terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used. The clauses of the 'OTU CA' CP apply.

IX.L. Duration and early end of validity period of the RP**IX.L.1. Validity period**

The RP of the RA must remain in force at least until the end of life of the last certificate issued under this RP.

IX.L.2. Effects of the end of validity and clauses remaining applicable

There are no specific requirements in the context of this RP.

The clauses of the 'OTU CA' CP apply.

IX.L.3. Individual notifications and communications between participants

There are no specific requirements in the context of this RP.

The clauses of the 'OTU CA' CP apply.

IX.M. Amendments to the RP**IX.M.1. Amendment procedures**

Major amendments made to this RP must be presented during a Policy Management Authority (PMA) meeting for approval of the changes made prior to publication of the new version of the RP. For the RP approval process, see Chapter I.E.4.

In the case of minor amendments (misprints, typos, etc.), these amendments do not require formal approval by the PMA to trigger publication of the new version of the RP.

IX.M.2. Mechanism and period for providing information on amendments

No mechanism is provided for giving information about amendments made.

IX.M.3. Circumstances according to which the OID must be changed

The RP OID is changed once significant amendments made by the RP are approved by the PMA.

In this case, the last digit of the OID will be modified to reflect major amendments.

IX.N. Dispute resolution provisions

In the event of any dispute, the holder must contact the points of contact mentioned in Chapter I.E.2.

IX.O. Courts with jurisdiction

Application of the legislation and regulations in force on Belgian territory.

IX.P. Compliance with legislation and regulations

Application of the legislation and regulations in force on Belgian territory.

The design and implementation of BNP Paribas' services, software and procedures take into account, as far as possible, accessibility for all users, 'irrespective of their hardware or software, their network infrastructure, their mother tongue, their culture, their geographical location, or their physical or mental abilities' (<https://www.w3.org/TR/WCAG20/>).

IX.Q. Miscellaneous

There are no specific requirements in the context of this RP.

IX.R. Other provisions

There are no specific requirements in the context of this RP.

X. Annex – Referenced documents**X.A. Regulations**

Not applicable.

X.B. Technical documents

Reference	Purpose of document
FIPS140-2_LEVEL3_CERT	Certificate of qualification FIPS 140-2 level 3 of the nShield cryptographic box (firmware 2.50.16).

All the procedures detailed relating to this RP are described in the annexes to the RPS, which can be viewed on request by authorised persons

XI. Annex: Registration procedures – authentication and authorisation accepted under this RP

XI.A. EMV card-based procedure for retail customers

XI.A.1. Step 1: registration (REG).

The bank carries out the REG 1.1 and REG 1.2 registration steps (see I.D.1) as described in this RP.

The bank is responsible for providing the user it registers with:

- ***a bank card (EMV standard) that allows for authentication using the M1 protocol and signing using the M2 protocol***
- ***PIN code***
- ***UCR on behalf of BNP Paribas Fortis***

The bank unambiguously links the card to the user

XI.A.2. Step 2: authentication (AUTH)

In this step, the customer logs in (SMID: customer number) as a natural person to their Easy Banking Web (EBW) electronic banking channel with their bank card (M1 procedure).

XI.A.3. Step 3: authorisation (AUT)

The natural person encodes the M2 challenge from their bank card as a natural person (SMID) in their electronic banking channel. This step formalises the request to create a signature certificate.

If this application is valid, a certificate application is sent to the technical RA, which generates a certificate in the name of the natural person (first name, surname).

XI.B. PRO card-based procedure for business customers

XI.B.1. Step 1: registration (REG).

The bank carries out the REG 1.1 and REG 1.2 registration steps (see I.D.1) as described in this RP.

The bank is responsible for providing the user it registers, or linking to this user, a smart bank card (Isabel standard) that allows for authentication and signing and optionally handing over their PIN. The card for the Easy Banking Business (EBB) electronic banking channel is activated securely: either face-to-face with the bank or online by the user, via their Belgian identity card (Belgium eID) with the use of their PIN.

The bank may also provide the user with a smart bank card (EBB) that allows for authentication and signing.

XI.B.2. Step 2: authentication (AUTH)

At this stage, the natural person logs in to the electronic banking channel with their card and PIN. The card may be:

- ***An EBB card provided by BNP Paribas Fortis***

- **An Isabel card provided by BNP Paribas Fortis**
- **An Isabel card provided by another bank**

XI.B.3. Step 3: authorisation (AUT)

The natural person uses their EBB or Isabel card in their electronic banking channel and enters their PIN. This step formalises the request to create a signature certificate.

If this application is **valid**, a **certificate application is sent to the technical RA**, which generates a certificate in the name of the natural person (first name, surname).

XI.C. itsme-based procedure for retail customers

XI.C.1. Step 1: registration (REG).

The bank carries out the REG 1.1 and REG 1.2 registration steps (see I.D.1) as described in this RP.

The bank is responsible for providing the user it registers with:

- **a bank card (EMV standard) that allows for authentication using the M1 protocol and signing using the M2 protocol.**
- **PIN code**
- **UCR on behalf of BNP Paribas Fortis**

The bank unambiguously links the card to the user.

itsme activation for the Easy Banking Web (EBW) electronic banking channel is done securely by the user via a secure session where they have previously logged in (SMID: customer number) as a natural person to their Easy Banking Web (EBW) electronic banking channel with their bank card (M1 procedure).

XI.C.2. Step 2: authentication (AUTH)

In this step, the customer logs in (SMID: customer number) as a natural person to their Easy Banking Web (EBW) electronic banking channel using their itsme application, registered at step 1 above.

XI.C.3. Step 3: authorisation (AUT)

The natural person chooses itsme from their electronic banking channel and then uses the itsme app and itsme pincode to authorise the request to create a signature certificate. This step formalises the request to create a signature certificate.

If this application is valid, a certificate application is sent to the technical RA, which generates a certificate in the name of the natural person (first name, surname).

XI.D. itsme-based procedure for business customers

XI.D.1. Step 1: registration (REG).

The bank carries out the REG 1.1 and REG 1.2 registration steps as described in this RP.

itsme activation for the Easy Banking Business (EBB) electronic banking channel is done securely by the user via an itsme secure session where they have previously logged in (unique customer reference + mobile number) as a natural person in their Easy Banking Business (EBB) electronic banking channel. The itsme

session supports itsme token activation for EBB.

XI.D.2. Step 2: authentication (AUTH)

During this step, the customer logs in (unique customer reference + mobile number) as a natural person in their Easy Banking Business (EBB) electronic banking channel using their itsme application, registered at step 1 above.

XI.D.3. Step 3: authorisation (AUT)

The natural person chooses itsme from their electronic banking channel and then uses the itsme app and itsme pincode to authorise the request to create a signature certificate. This step formalises the request to create a signature certificate.

If this application is valid, a certificate application is sent to the technical RA, which generates a certificate in the name of the natural person (first name, surname).

XI.E. Easy PIN (Gemalto)-based procedure for retail customers

XI.E.1. Step 1: registration (REG).

The bank carries out the REG 1.1 and REG 1.2 registration steps (see I.D.1) as described in this RP.

The bank is responsible for providing the user it registers with:

- ***a bank card (EMV standard) that allows for authentication using the M1 protocol and signing using the M2 protocol.***
- ***PIN code***
- ***UCR on behalf of BNP Paribas Fortis***

The bank unambiguously links the card to the user.

Easy PIN (Gemalto) activation for the Easy Banking App (EBA) electronic banking channel is done securely by the user in a secure session where they have previously logged in (SMID: customer number) as a natural person in their Easy Banking App (EBA) electronic banking channel with their bank card (M1 procedure).

XI.E.2. Step 2: authentication (AUTH)

In this step, the customer logs in (SMID: customer number) as a natural person in their Easy Banking App (EBA) electronic banking channel with their Easy PIN (Gemalto), registered at step 1 above.

XI.E.3. Step 3: authorisation (AUT)

The natural person uses their Easy PIN (Gemalto) pincode as a natural person (SMID) in their electronic banking channel. This step formalises the request to create a signature certificate.

If this application is valid, a certificate application is sent to the technical RA, which generates a certificate in the name of the natural person (first name, surname).

XI.A. Easy PIN (Gemalto)-based procedure for business customers

XI.A.1. Step 1: registration (REG).

The bank carries out the REG 1.1 and REG 1.2 registration steps as described in this RP.

The bank is responsible for providing the user it registers, or linking to the user, a smart bank card (Isabel standard) that allows for authentication and signing and optionally handing over their PIN. The card for the Easy Banking Business (EBB) electronic banking channel is activated securely, either face-to-face with the bank or online by the user, via their Belgian identity card (Belgium eID) using their PIN.

Easy PIN (Gemalto) is activated for the Easy Banking Business Mobile (EBBM) electronic banking channel when the EBBM app is installed. At the time of installation, the user is redirected to the Easy Banking Business (EBB) electronic banking channel or enters a secure session where they have previously logged in (by entering their unique customer reference) as a natural person (with their smart bank card or itsme). In the EBB secure session, a personal QR code is available that allows the customer to continue the EBBM installation on their mobile. Easy PIN (Gemalto) is activated and the PIN selected during installation.

XI.A.2. Step 2: authentication (AUTH)

In this step, the customer logs in (unique customer reference) as a natural person in their Easy Banking Business Mobile (EBBM) electronic banking channel with their Easy PIN application (Gemalto), registered at step 1 above.

XI.A.3. Step 3: authorisation (AUT)

The natural person uses their Easy PIN (Gemalto) pincode to authorise the request to create a signature certificate. This step formalises the request to create a signature certificate.

If this application is valid, a certificate application is sent to the technical RA, which generates a certificate in the name of the natural person (first name, surname).