IN GROUPE

CERTIFICATE POLICY

Natural Person Certificates

Security Document

Distribution method	**EXTERNAL**
Document status	**APPROVED**
Application date	01/01/2022

VERSION HISTORY

Version	Date	Author	Nature of revision Paragraphs modified
1.0	09/02/2017	Imprimerie Nationale	Initial version
1.1	23/06/2017	Imprimerie Nationale	Corrections made following the LSTI audit
1.2	15/12/2017	Imprimerie Nationale	Changes following the LSTI audit
2.0	04/07/2019	Franck Leroy (IN Groupe)	Restructuring
2.1	28/09/2021	Franck Leroy (IN Groupe)	eIDAS update
2.1.1	21/12/2021	Franck Leroy (IN Groupe)	Changes following the LSTI audit

CONTENTS

I Introduction

I.1 GENERAL INTRODUCTION

I.1.1 Purpose of the document

IN Groupe has set up a Public Key Infrastructure (PKI) to deliver electronic certificates that comply with the European eIDAS regulations.

IN Groupe thus offers certificate issue services aimed at implementing authentication and signature functions. IN Groupe is a TSP (Trust Service Provider).

This document constitutes the certification policy (CP) of IN Groupe Certification Authorities (CAs). It describes the different levels of responsibility, security measures (technical, organisational, etc.) and certificate profiles. It also sets out the commitments of IN Groupe CAs within the context of the provision of its electronic certification services for holders, in accordance with the requirements of the standard CPs that have been drafted within the framework of the *Référentiel Général de Sécurité*.

This document incorporates public information on certification practices. Details of the practices are set out in a separate document, which can be consulted on request to the CA contact point (see I.6.2), which will communicate the consultation procedures.

The PKI is composed of a root authority (Root CA) and several hierarchically dependent authorities (Intermediate Certificate Authority).

This CP cover two intermediate CAs:
- Imprimerie Nationale Substantiel Personnel, and
- Imprimerie Nationale Élevé Personnel.

These CAs issue two types of certificates:
- Authentication certificates, and
- Signature certificates.

Certificates are issued exclusively to natural persons who use them (and the associated private keys) in the context of their activities in relation to the Customer Entity identified in the certificate and with which these natural persons have a contractual relationship (see definition of the Certificate Holder in § I.3.7). The Customer Entities to which the natural persons are attached may belong to the private or public sector.

The structure of this CP complies with with [RFC3647] "*X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework*" of the *Internet Engineering Task Force* (IETF) and is based on the CP-Type [RGS_A_2] (individual electronic certificates) of the *Référentiel Général de Sécurité* V2.0 (General Security Database) developed by ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information* - French National Agency for Information Systems Security) in conjunction with SGMAP (*Secrétariat Général pour la Modernisation de l'Action Publique* - General Secretariat for the Modernisation of Public Action).

Given the complexity of reading the CP for Certificate Holders or Users who are not specialists in the field, IN Groupe publishes General Terms and Conditions of Use *(PKI Disclosure Statement)* defined in the ETSI EN 319411-1 standard.

I.1.2 Drafting conventions

In order to emphasise the rules specific to a security level, type of use or type of holder, they will be presented in a box, the title of the box specifying its scope (use of the electronic certificate, security level and type of holder of the electronic certificate). The form is as follows:

Name of the Certification Authority	
Use	Security level

The requirements that are not in a box apply in the same way to all IN Groupe CAs.

I.2 DOCUMENT IDENTIFICATION

This CP is identified in the following table by the following OIDs:

AC Imprimerie Nationale Substantiel Personnel	
OID	Security level
Authentication: 1.2.250.1.295.1.1.8.6.1.101.1	ETSI NCP
Signature: 1.2.250.1.295.1.1.8.6.1.102.1	ETSI QCP-n+qscd
Authentication: 1.2.250.1.295.1.1.8.0.1.101.0	ETSI NCP+
Signature: 1.2.250.1.295.1.1.8.0.1.102.0	ETSI QCP-n+qscd

AC Imprimerie Nationale Elevé Personnel	
OID	Qualification level
Signature: 1.2.250.1.295.1.1.20.7.1.102.1	ETSI QCP-n+qscd
Signature: 1.2.250.1.295.1.1.20.0.1.102.0	ETSI QCP-n+qscd

The date this CP applies is 1 January 2022 (01/01/2022).

I.3 DEFINITIONS AND ACRONYMS

I.3.1 Acronyms

CA Certification Authority
RCA Root Certification Authority
RA Registration Authority
PMA Policy Management Authority
ANSSI French National Information System Security Agency

CMS	*Credentials Management System*
CPS	Certification Practices Statement
HSM	*Hardware Security Module*
ICD	*International Code Designator*
PKI	Public Key Infrastructure
PDS	PKI Disclosure Statement
IN Groupe	Imprimerie Nationale Group
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
ARL	Authority Revocation List
CRL	Certificate Revocation List
LDAP	*Lightweight Directory Access Protocol*
CAG	Certification Agent
OID	*Object Identifier*
CP	Certification Policy
OCSP	Online Certificate Status Protocol
CSO	Certification Services Operator
QSCD	Qualified Signature (or Seal) Creation Device
LR	Legal representative
RSA	Rivest Shamir Adleman
SHA-256	*Secure Hash Algorithm 256*
CU	Certificate User

I.3.2 Definitions

Audit: Independent check of a system's records and activities to assess the adequacy and effectiveness of the system's checks, to verify its compliance with established operational policies and procedures, and to recommend any necessary changes in the checks, policies, or procedures.

Certification Authority (CA): authority on which one or more Certificate Users rely to create and allocate certificates. [ISO/IEC 9594-8; ITU-T X.509].

Registration Authority (RA): See section 1.3.1.

Policy Management Authority (PMA): The IN Groupe Policy Management Authority (PMA) is composed of a PKI SUPERVISORY BOARD within the IN Groupe. This board is responsible for the IN Groupe's CAs and ensures the consistency and management of the security reference framework, as well as its implementation. The security reference framework consists of this CP, the general terms and conditions of use and the procedures implemented by the components of the PKI. The PMA approves the CP. It also ensures that the CPS is consistent with the CP. It authorises and approves the creation and use of CA components. It monitors the audits and compliance checks carried out by the PKI's components, decides on the actions to be taken and ensures their implementation.

Key pairs: Pair of asymmetric keys, consisting of a public key and the corresponding private key.

Key ceremony: A procedure by which a CA dual key is generated and/or its public key certified.

Certificate: an entity's public key, as well as other information, the forging of which is made impossible by encrypting it with the private key of the issuing certification authority [ISO/IEC 9594-8; ITU-T X.509]. The certificate contains identification information of the owner of the key pair.

Self-signed certificate: CA certificate signed by the private key of the same CA.

Certification path: (or chain of trust, or chain of certification) a chain of multiple certificates required to validate a certificate.

Private key: key of the asymmetric key pair of an entity to be used only by that entity [ISO/IEC 9798-1].

Public key: key of the asymmetric key pair of an entity that can be made public. [ISO/IEC 9798-1].

CMS: This system is responsible for managing the life cycle of Holders' smart cards and their certificates. This system handles Holders' certificate requests, certificate renewal requests and revocation requests. It therefore interfaces with the PKI to ask the PKI to perform these various functions.

Compromise: A proven or suspected breach of a security policy, during which unauthorised disclosure or loss of control of sensitive information may have occurred. For private keys, a compromise is the loss, theft, disclosure, modification, unauthorised use, or other compromise of the security of this private key.

Confidentiality: The property that information has of not being made available or disclosed to individuals, entities, or processes [ISO/IEC 13335-1:2004].

Certification Practice Statement (CPS): a statement of the practices that an entity (acting as a Certification Authority) applies in the provision of its certification services (application, issue, renewal and revocation of certificates) in accordance with the CP it has undertaken to comply with [RGS (French General Security Database)-type CP definition].

Availability: The property of being accessible on request to an authorised entity [ISO/IEC 13335-1:2004].

Activation data: Data values, other than keys, that are necessary to operate the cryptographic modules or the elements they protect and that must be protected (e.g. a PIN, a passphrase, etc.).

Hash function: function that links bit strings to fixed-length bit strings, thus satisfying the following three properties:

- It is impossible, by any means of calculation, to find, for a given output, an input that corresponds to that output;
- It is impossible, by any means of calculation, to find, for a given input, a second input that corresponds to the same output [ISO/IEC 10118-1];
- It is impossible by calculation to find two different input data corresponding to the same output.

Public Key Infrastructure (PKI): This is the infrastructure required to produce, distribute, manage and archive keys, certificates and Certificate Revocation Lists as well as the database in which certificates and CRLs/ARLs must be published. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Integrity: refers to the accuracy of the information, the source of the information, and the functioning of the system that processes it.

Certificate Revocation List (CRL): A list digitally signed by a CA that contains certificate identities that are declared invalid before their expiry date (entered in the certificate) or that are no longer trustworthy. The list contains the identity of the CA CRL, the date of publication, the date of publication of the next CRL and the serial numbers of the revoked certificates. When the list contains only CA certificates, the term Authority Revocation List (ARL) is used.

Cryptographic modules: A set of software and hardware components used to implement a private key to enable cryptographic operations (signature, encryption, authentication, key generation, etc.). For a CA, the cryptographic module is an evaluated and certified hardware cryptographic resource (FIPS or common criteria), used to store and implement the CA private key.

Validity period of a certificate: The validity period of a certificate is the period during which the CA guarantees that it will maintain information regarding the validity status of the certificate. [RFC 5280]. Outside this period (before the valid-from date and after the valid-to date), the certificate is deemed invalid.

Disaster Recovery Plan: A plan defined by a CA to restore all or part of its PKI services after they have been damaged or destroyed as a result of a disaster, within a time frame defined in the PC package.

CRL/ARL Distribution Point: Directory entry or other source of CRL distribution; a CRL distributed through a CRL distribution point may include revocation entries for a subset only of all certificates issued by a CA, or may contain revocation entries for multiple CAs. [ISO/IEC 9594-8; ITU-T X.509].

Certification Policy (CP): a set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. [ISO/IEC 9594-8; ITU-T X.509].

Security policy: a set of rules issued by a security authority relating to the use, provision of security services and facilities [ISO/IEC 9594-8; ITU-T X.509].

Secret Holder: persons who hold activation data related to the implementation of a CA's private key using a cryptographic module.

Policy qualifier: Policy information that accompanies a certification policy identifier (OID) in an X.509 certificate. [RFC 3647]

Revocation: opposition procedure against the certificate which aims to cancel the CA's undertaking guarantee before the end of the validity period. Such revocation shall be implemented at the request of one of the parties in accordance with specific procedures.

RSA: public key cryptographic algorithm invented by Rivest, Shamir, and Adleman.

Electronic certificate validation: a checking operation to ensure that the information contained in the certificate has been verified by a certification authority (CA) and is still valid. Validation of a certificate includes, among other things, checking its validity period, its status (revoked or not), the identity of CAs and verification of the certification chain. The validation of an electronic certificate requires prior approval of the certificate from the Root authority (self-signed certificate).

I.4 ENTITIES INVOLVED IN THE PKI

The notion of a Certification Authority (CA) as used in this document is defined in § I.3.1.

The CA is responsible for providing certificate management services throughout their lifecycle (generation, distribution, renewal, revocation) and relies on a technical infrastructure known as the Public Key Infrastructure (PKI). The CA's services are the result of different functions that correspond to the different stages of the life cycle of key pairs and certificates.

The PKI is based on the following functional services:

- Key pair generation: This service generates the key pair for future Holders and provides the public key to be certified to the certificate generation service
- Generation of certificates: This service generates electronic certificates for future Holders based on information provided by the registration authority.
- Revocation: This service processes certificate revocation requests and determines the actions to be taken, including the generation of the certificate revocation list (CRL).
- Publication: This service provides Certificate Users (CUs) and Certificate Holders or certificate managers with the information necessary to use certificates issued by CAs (General Terms and Conditions of Use, PC, CA certificates, etc.) as well as the processing results of the certificate revocation management service (CRL).

This CP defines the security requirements and describes the operational organisation for all the functions described above for issuing certificates to Holders.

I.4.1 Certification Authorities

The certification authority generates and revokes certificates from requests sent by the Registration Authority. The CA implements certificate generation, certificate revocation, certificate status information, logging and audit services.

I.4.2 Registration Authority

The RA is used for the implementation of certificate application registration, certificate delivery, certificate revocation, logging and audit services. In particular, the role of the RA is to verify the identity of future Certificate Holders, as well as that of Certification Agents (CAGs).

The RA falls under the responsibility of the IN Groupe.

Some of the certificate management procedures (issue, revocation, etc.) are based on a third-party technical registration authority, in charge of the RA information system.

I.4.3 Certificate holders

A "Certificate Holder" is defined as any entity that holds a key pair and the associated public key certificate issued by the CA.

In this CP, this entity (the Holder) may only be a natural person, who is involved in the private or public sector. This person uses his/her private key and the corresponding certificate in the context of his/her professional activities, i.e. his/her activities in relation to the Client Entity identified in the certificate and with which s/he has a contractual relationship (see III.2.2).

In practice, there are three types of Holders: the legal representatives (LRs) of a Customer Entity, the certification agents of a Customer Entity (CAGs), and the "final" Holders.

This CP requires that the Holder's private key be stored on a physical medium (smart card) and that the implementation of this key requires authentication (submission of the PIN code to the card).

The Holder shall comply with the conditions incumbent upon him/her and defined in this CP. These conditions are included in the General Terms and Conditions of Use that s/he explicitly accepted when applying for a certificate.

I.4.4 Certificate users

A Certificate User is any application, natural person or legal entity, computer system or equipment that uses a Holder's certificate in accordance with this CP and the security practices set out by the application managers or the person in charge of its Entity, in order to validate the security functions implemented using authentication and signature certificates.

The CU uses a certificate and signature verification device to verify the electronic signature affixed to data or a message by the Certificate Holder.

The Certificate User can hold his/her own certificate. A Holder who receives a certificate from another Holder becomes a Certificate User. Under this CP, the Certificate User must validate the certification chain (validation of the Holder's certificate, the CA certificate and the RCA) and check the non-revocation of certificates (Holder's certificate and CA certificate) through the publication service made available to him/her.

A User (or acceptor) of Authentication Certificates may include:

- An on-line service that uses a certificate and an authentication verification mechanism either to validate an access request made by the certificate holder as part of an access check, or to authenticate the origin of a message or data transmitted by the certificate holder;
- A user who receives a message or data and uses a certificate and an authentication verification device to authenticate its origin.

A User (or acceptor) of Signature Certificates may include:

- An on-line service that uses a certificate and signature verification mechanism to verify the electronic signature affixed to data or a message by the Certificate Holder;
- A user who electronically signs a document or message;
- A user who receives a message or data and uses a certificate and a signature verification mechanism to verify the electronic signature affixed by the certificate holder to that message or data.

I.4.5 Other participants

I.4.5.1 Components of the PKI

The breakdown of the PKI by function is given in section I.4.1 above. The components of the PKI implementing these functions are given in the CA CPS.

A technical operator is in charge to house and manage the CA's private keys in order to generate and revoke the end-user certificates.

The technical operator provides hardware and software for the PKI in order the generate and issue certificates according to the CA's CP.

The technical operator in responsible of the PKI operations and of its security (security of IT and technical equipment, the security of personnel and premises).

The technical operator shall comply with this CP.

I.4.5.2 Certification Agent

The authorised certification representatives and the legal representative of the Customer Entity are natural persons mandated by the legal representative of the Client Entity other than IN Groupe and having the power to:

- authenticate the Customer Entity's future Holders, particularly during the face-to-face meeting,
- apply to the RA for a certificate or renewal of a certificate bearing the name of the Entity,
- make a revocation request of a certificate bearing the name of the Entity,
- if necessary, return the private key media (smart cards) to their Holders.

The CAG has no access to the means to activate and use the private key associated with the public key certificates issued by the CA to the Holders.

Any CAG must be formally appointed by one of the Entity's legal representatives.

The CAG is in direct contact with the CA's RA.

The commitments and obligations of the CAGs are specified in a letter of appointment that they must sign.

This letter of appointment stipulates in particular that the CAG must independently carry out identity checks on future Holders and respect the parts of this CP for which it is responsible.

In the event of a replacement of a CAG for any reason whatsoever of its functions, the Entity must report this to the CA without delay. If necessary, appoint a successor if no other CAG is yet in office.

I.4.5.3 Customer entity

The legal entity (company/local authority/public institution/association, etc.) that is a contracting partner of IN Groupe, indicated in the Certificate Application, to which the Holder is attached, and in whose name the Holder uses the Electronic Certificates. The Customer Entity's Authorised Legal Representative shall sign the Certificate Application Form. However, s/he may use a Certification Agent both for the Certificate application phase and for the Media delivery phase.

I.5 USE OF CERTIFICATES

I.5.1 Applicable fields of use

I.5.1.1 Holders' key pairs and certificates

This CP deals with the key pairs and certificates issued by the CA to the categories of Holders identified in § I.3.7 (natural persons) so that they can authenticate themselves or electronically sign data (documents or messages) in the context of paperless exchanges with the categories of Certificate Users identified in section § I.3.8 above. Such an electronic signature provides, in addition to the authentication of the signatory and the integrity of the data thus signed, the signatory's consent to the content of such data.

Verification of the signature of a document signed with a holder certificate guarantees:

- The origin of the document: authentication of the person who created or issued the document
- The integrity of the document: the recipient is assured that the content of the document has not been modified by a third party
- If applicable, the precedence (existence of the document before a certain date), if the signature is time-stamped: a time-stamp token has been generated by a Time-Stamping Authority and associated with the document in addition to the electronic signature

Comments:

- It is expressly understood that a Certificate Holder may only use his/her private key and certificate for authentication or signature purposes as defined in the use of his/her certificate. In the event of unauthorised use of a private key and its certificate by its Holder, the latter could be held liable.
- It is also expressly understood that the User of the certificate can only trust the certificate in the context of paperless exchanges with the Holder. The electronic signature provides, in addition to the guarantees of the authenticity and integrity of the data thus signed, a guarantee of the signatory's consent to the content of such data.

I.5.1.2 CA and components' key pairs and certificates

The CA has only one key pair and the corresponding certificate is attached to a higher-level CA (CA hierarchy).

The CA's key pair is used to sign the certificates and Certificate Revocation Lists (CRLs) it issues. This key pair is used exclusively for this purpose.

The PKI has additional key pairs and corresponding certificates, signed by the CA to sign the OCSP responses

I.5.2 Prohibited areas of use

The use of certificates issued by the CA for purposes other than those provided for in this CP (see § I.4.1) is not permitted. This means that the CA cannot, under any circumstances, be held liable for any use of the certificates it issues other than that provided for in this CP.

The CA undertakes to enforce these restrictions on potential Certificate Holders and Users of such certificates. To this end, the CA publishes the PKI Disclosure Statement (PDS) intended for them. In particular, the issuing of the certificate to a Holder is subject to the explicit acceptance of these PDS (indicated in the application form that the Holder must sign).

I.6 CP MANAGEMENT

I.6.1 Entity managing the CP

This certification policy is the responsibility of IN Groupe.

I.6.2 Point of contact

Point of contact:

IN Groupe
CA manager
104, avenue du Président Kennedy
75016 Paris
contact.passin@ingroupe.com

Any remarks or comments can be forwarded to this contact point.

I.6.3 Entity determining the compliance of a CPS with this CP

The PMA through its SUPERVISORY BOARD shall determine the compliance of CP practices. It thus carries out compliance checks and audits in order to authorise or otherwise the issue of certificates. Audits may be entrusted to a third-party company chosen by the PMA.

I.6.4 Procedures for approving CPS compliance

Documented CP practices are approved by the PMA following an approval process established by the IN Groupe.

This CP will be reviewed regularly (at least once a year) by the Supervisory Board that constitutes the PMA to:

- Ensure compliance with the security standards expected by applications that reference families of holder certificates,
- Update the list of applications concerned by the CP,
- Adapt to technological developments.

The approval process will be followed for any update of the CP.

II Responsibilities for the provision of information to be published

II.1 ENTITIES RESPONSIBLE FOR MAKING INFORMATION AVAILABLE

The publication function is responsible for publishing the data to be published to Certificate Holders, and Certificate Users (CU).

II.2 INFORMATIONTO BE PUBLISHED

The CA publishes the following for Certificate Holders and Certificate Users (CU):

- PCs in operation
- PDS
- Forms and reports
- CA certificates
- Revocation lists

On the website: https://crl.pass-in.fr/

Unless otherwise indicated, all other information is considered confidential.

IN Groupe does not publish details that it considers sensitive or even confidential in its CP.

This information is carried over to a confidential document that lists all the technical and non-technical procedures applied within the PKI.

The PKI Disclosure Statement describe, among other things:

- The conditions of use of certificates and their limits
- The applicable CP identifier (OID)
- The obligations and responsibilities of the various parties, including requirements for verifying the revocation status of a certificate for Certificate Users.

II.3 TIME LIMITS AND FREQUENCY OF PUBLICATION

The publication timeframes and frequencies depend on the information in question:

- For information related to the PKI (new version of the CP, forms, etc.), the information is published whenever necessary in order to ensure, at all times, consistency between the published information and the CA's actual commitments, means and procedures.
- For the CA's certificates, they are disseminated prior to any issuing of certificates and/or of corresponding CRLs within an interval of 24 hours.

The deadlines and frequencies for publishing certificate status information and the availability requirements for the systems publishing them are described in § IV.9 and § IV.10

The publication systems are available 7 days a week and 24 hours a day.

II.4 ACCESS CONTROL TO PUBLISHED INFORMATION

All information published for Certificate Users is freely accessible for reading and protected against unauthorised changes.

Access to publishing systems for editing (adding, deleting or modifying published information) is strictly limited to the PKI's authorised internal functions, through strong access control (based on two-factor authentication).

III Identification and authentication

III.1 NAMING

III.1.1 Types of names

The names used comply with the specifications of the X.500 standard.

In each X.509 certificate, the *issuer* and the Holder ("*subject*") fields are identified by an X.501-type *Distinguished Name* (DN).

III.1.2 Need to use explicit names

The *subject* field DN of the certificates issued by the CA identifies the Certificate Holder.

DN Attributes	Attribute name	Value
C	*countryName*	FR
O	*organizationName*	Name of the Customer Entity to which the Holder belongs
OU	*organizationalUnitName*	Identifier of the Customer Entity to which the Holder belongs in RGS format.
OI	*organizationIdentifier*	Identifier of the Customer Entity to which the Holder belongs in ETSI format.
CN	*commonName*	First forename and Surname of the Holder's civil status as shown on the identity document submitted at the time of registration.
SN	*surName*	Civil status last name of the Holder
GN	*givenName*	Civil status first forename of the Holder
SerialNumber	*SerialNumber*	Contains a number making it possible to guarantee the uniqueness of the DN and thus resolve cases of homonyms.

Note: IN Groupe only issues certificates to entities governed by French law.

Test certificates are identifiable by the fact that their CN contains the word "TEST", preceding a fictitious first name and surname. All other fields*(except CA information, such as Issuer, AIA, AKI, etc.*) may differ from the profiles of the holder certificates described in section VII.1.

III.1.3 Pseudonymisation of holders

The CA does not issue a certificate with an anonymous identity or a pseudonymous identity.

III.1.4 Rules for the interpretation of the different forms of names

CUs can use CA certificates contained in certification chains (see § above), to implement and validate security functions by verifying, among other things, the identities (DN) of Holders included in certificates issued by the CA.

III.1.5 Uniqueness of names

The identities held by the CA in certificates are unique within the CA's certification domain.

The CA ensures this uniqueness through its registration process: a DN assigned to one Holder cannot be assigned to another Holder.

The SerialNumber attribute, containing a unique number generated by a component of the PKI, is used to resolve cases of homonyms (CN (Common Name) of the certificate to be issued corresponds to the CN of a certificate already issued for two distinct natural persons).

The *Subject Alternative Name* extension containing the email address (RFC822) also helps to uniquely identify the certificate holder.

The uniqueness of a certificate is based on the uniqueness of its serial number within the CA domain. This number is specific to the certificate and not to the Holder. It therefore does not ensure continuity of identification in the successive certificates of a given Holder.

The CA is responsible for the uniqueness of the names of its Holders and for resolving disputes relating to the claim to use a name.

III.1.6 Identification, authentication and role of trademarks

The CA cannot be held liable for any unlawful use by the Certificate Users and customers of trademarks, well-known trademarks and distinctive signs, as well as domain names.

III.2 INITIAL IDENTITY VALIDATION

III.2.1 Method for proving possession of the private key

The operation of generating the Holder's key pair is performed by the CA (centralised generation). The latter ensures the allocation of this key pair to the Holder by importing the private key and the associated public key certificate into the card that will be issued to him/her.

III.2.2 Validation of the identity of an organisation

The validation of the identity of a Holder's affiliated Customer Entity is carried out as part of the registration with the RA of one of the following persons:

- A legal representative of this Customer Entity
- A CAG for this Customer Entity

III.2.3 Validation of the identity of an individual

The initial validation of the identity of a natural person is carried out as part of the registration with the RA or the CAG of one of the following persons:

- A legal representative (LR) of this Customer Entity (registration by the RA)
- A CAG for this Customer Entity (registration by the RA)
- A future Holder belonging to this Customer Entity (registration by a CAG)

The identity of the natural person is verified by checking a valid official identity document (including a photo) (National Identity Card, Passport, Residence Permit). The identification of Holders is carried out as part of a physical face-to-face meeting by the RA or CAG carrying out the registration.

III.2.3.1 Registering an LR

The registration of a legal representative is the first step following the establishment of a contract between the Customer Entity for which it is responsible and IN Groupe.

The registration of a LR requires the validation by the RA of the "natural person" identity of the Holder and his/her status of legal representative with regard to the Customer Entity.

The LR's registration record includes:

- [Optional] The written certificate request, not more than three months old, signed by the LR
- [Optional] The General Terms and Conditions of Use signed by the LR
- A photocopy of a valid official identity document of the LR

Identification information of the Customer Entity;

For a company:

- Any document attesting to the capacity of the RL
- Any document, valid at the time of registration, bearing the identification number of the Customer Entity (KBIS extract (French business registration certificate) or Certificate of Identification from the *Répertoire National des Entreprises et de leurs Établissements* (French National Register of Companies and their Establishments), INSEE (French National Institute for Statistics and Economic Research) legal status notice) or, failing that, another valid document attesting to the unique identification of the company which will appear in the certificate

For an administration:

- Any document, valid at the time of registration, bearing the identification number of the Customer Entity (INSEE legal status notice) or, failing that, another valid document attesting to the administration's unique identification that will appear in the certificate
- A document, valid at the time of registration, delegating or sub-delegating the authority responsible for the administrative structure (any deliberations, decrees and/or appointment orders, designation concerning the administrative authority)
- Contact information for the LR: email or postal address, optionally telephone number

All of these documents are submitted to the RA.

III.2.3.2 Registering a CAG

The registration of a CAG requires the validation by the RA of the CAG's "natural person" identity, his/her connection to the Customer Entity and his/her role as a CAG.

The CAG registration application must include:

- [Optional] The written certificate request, not more than three months old, signed by the CAG
- [Optional] The General Terms and Conditions of Use signed by the CAG
- A mandate, less than three months old, appointing the agent, signed by the LR and the CAG for acceptance.
- A signed undertaking, not more than three months old, from the future CAG to properly and independently perform

checks on applicant's files and to report to the RA that they are leaving the Customer Entity
- A photocopy of a valid official identity document of the CAG
- Contact information for the CAG: email or postal address, optionally telephone number

All of these documents are submitted to the RA.

III.2.3.3 Registration of a Holder via a CAG

The registration of a Holder via a CAG requires the validation by the CAG of the Holder's "natural person" identity and his/her connection to the Customer Entity.

The certificate request application drawn up with the CAG must include:
- The certificate request mentioning the identity of the Holder, not more than three months old, signed by the Holder.
- The General Terms and Conditions of Use signed by the Holder
- A photocopy of a valid official identity document of the Holder
- Contact information for the Holder: email or postal address, optionally telephone number

III.2.4 Unverified holder information

Certificates issued by the CA do not contain any unverified identity information except for technical computer elements such as UPNs and e-mail addresses.

III.2.5 Validation of the applicant's authority

The validation of the authority of the applicant (future Holder) is carried out at the same time as the validation of the identity of the natural person, directly by the RA or by the CAG.

III.2.6 Interoperability criteria

This point is not applicable in this CP.

III.3 IDENTIFICATION AND VALIDATION OF A KEY RENEWAL REQUEST

The CA does not issue a new certificate for a previously issued key pair. Renewal requires the generation of a new key pair and a new certificate application (see § IV.6).

III.3.1 Identification and validation for a current renewal

Checks relating to current renewal shall be carried out in accordance with the initial certificate application procedure (see § III.2 above).

III.3.2 Identification and validation for renewal after revocation

Checks relating to the renewal of a key pair after revocation of the certificate are carried out in accordance with the initial certificate application procedure (see § III.2 above), this case being similar to a renewal of the key pair with the issue of a new certificate.

III.4 IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST

Requests for revocation of a certificate shall give rise to verification of the identity of the applicant and verification of his/her authority in relation to the certificate to be revoked.

In particular, the persons with authority in relation to the certificate to be revoked are:

- the Holder of the certificate to be revoked
- the legal representative of the Customer Entity to which the Holder belongs
- a CAG of the Customer Entity to which the Holder belongs

If the applicant is the Holder, the Holder is authenticated through a set of Questions and Answers (minimum of 5) through the on-line service customer interface.

A revocation request may be made:

- on-line:
  - by the CAG or Legal Representative authenticated with their own certificate;
  - by the Holder authenticated by his/her certificate;
- by telephone:
  - the applicant is authenticated by a set of 5 Questions and Answers known only to the applicant;
- by post:
  - the revocation request must be signed by the applicant and must be accompanied by a photocopy of an official identity document of the applicant. The identity of the applicant is ensured by checking the handwritten signature against a previously recorded handwritten signature. The authority of the applicant with respect to the certificate to be revoked is verified by the revocation service (only the Holder, the CAG and the Legal Representative can request the revocation of the Holder on the side of the Customer Entity).
  - The request can be sent by post or email.

IV Operational requirements for the certificate life cycle

IV.1 CERTIFICATE REQUEST

IV.1.1 Origin of a certificate request

The certificate request comes from the CAG duly mandated by the legal representative of the Customer Entity.

The prior consent of the future Holder is required.

IV.1.2 Process and responsibilities for preparing a certificate application

The certificate application is prepared by the LR or CAG.

This file shall *at least* include the following information:

- The name of the future Holder to be used in the certificate
- The personal identification data of the future Holder
- The identification data of the Customer Entity (corresponding, if applicable, to the Customer Entity to which the CAG is attached)

The application contains the elements described in III.2.3.

In the case of an LR (III.2.3.1) or CAG (III.2.3.2) application, the file is forwarded to the RA by the applicant or remitted by hand at the face-to-face meeting. The file is signed by the RA during the face-to-face meeting.

In the case of an application for a Holder via a CAG (III.2.3.3), the application is sent to the RA by the CAG. The file is signed by the CAG following the face-to-face meeting with the Holder.

The paper application must in all cases be sent within the time limit set by the RA for validation and archiving.

IV.2 PROCESSING A CERTIFICATE REQUEST

IV.2.1 Execution of the request identification and validation processes

The RA performs the following processing operations:

- Checking the CAG's mandate
- Checking the identity of the Holder ("natural person" identification)
- Checking the identity of the Customer Entity ("legal entity" identification)
- Checking the consistency of the supporting documents provided
- Checking the acceptance of the general terms and conditions of use by the Holder

The request application is kept in all cases by the RA, even in the case of a request made by a CAG.

IV.2.2 Acceptance or rejection of the request

In the event of rejection of the certificate request, the RA shall inform the Holder and, where applicable, the CAG. Notification of rejection is made through the application's on-line tracking function. If applicable, the Holder may be informed through the CAG.

In the event of acceptance of the request, the Holder may monitor how processing by the CA is progressing (possible creation of the medium and generation of the key pair and associated certificate).

IV.2.3 Duration of certificate preparation

Once the certificate request has been validated, the certificate is issued as soon as possible.

IV.3 ISSUE OF THE CERTIFICATE

IV.3.1 Action by the CA regarding the issue of the certificate

Following validation of the request by the RA, the CA initiates the process of generating and preparing the elements for the Holder: creation of the medium, generation of the key pair and certificate, as well as the medium activation code.

IV.3.2 Notification by the CA of the issue of the certificate to the holder

The CA notifies the Holder, and if applicable the CAG, of the sending of the medium (bearing the key pair and associated certificate) and its activation code by post, through the application accessible on-line. The medium and activation code are sent separately. The Holder's private key is protected by the media activation code during its sending.

The medium is sent directly to the Holder, or the CAG if appropriate, by secure tracked express transport, provided by a specialised service provider.

IV.4 ACCEPTANCE OF THE CERTIFICATE

IV.4.1 Procedure for accepting the certificate

The acceptance of the certificate by the Holder is carried out explicitly in the form of a signed agreement. Once the Qualified Signature Creation Device (QSCD) has been received, the Holder signs a Certificate Acceptance Report during the activation phase of his/her certificate and returns it to the RA who will keep it.

It is the Holder's responsibility to check the consistency of the information contained in the certificate (e.g. email address) before any use.

In the event of an explicit refusal of the certificate by the Holder, or in the event of non-receipt by the RA of the signed agreement within 40 days of receipt of the card, the certificate is revoked by the CA.

The signed agreement is archived with the Holder's registration file.

IV.4.2 Publication of the certificate

Certificates issued by the CA under this CP are not published.

IV.4.3 Notification by the CA to other entities of the issue of a certificate

The RA is informed of the generation of the certificate by the CA. It is the RA who is responsible for issuing it to the Holder.

IV.5 USE OF THE KEY PAIR AND CERTIFICATE

IV.5.1 Use of the private key and certificate by the holder

Holders must strictly adhere to the authorised uses of the key pairs and certificates.

Otherwise, they could be held liable.

The authorised use of the key pair and the associated certificate are also indicated in the certificate itself, via the extensions concerning the use of the keys.

The use of the holder's private key and associated certificate is strictly limited to the service defined by the OID from its policy (see section I.4.1.1.1).

IV.5.2 Use of the public key and certificate by the certificate user

See previous section and section I.4.

Certificate Users must strictly adhere to the authorised uses of certificates. Otherwise, they could be held liable.

IV.6 CERTIFICATE RENEWAL

In accordance with [RFC3647], the notion of "certificate renewal" refers 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 public key).

Under this CP, there can be no certificate renewal without renewal of the corresponding key pair.

IV.7 ISSUE OF A NEW CERTIFICATE FOLLOWING A CHANGE OF THE KEY PAIR

IV.7.1 Possible causes for changing a key pair

The key pairs must be periodically renewed in order to minimise the possibility of cryptographic attacks. Thus the Holder's key pairs, and the corresponding certificates, will be renewed at least before their end of life as defined in section 6.3.2.

The Holder's key pairs may be renewed in advance, following the revocation of the Holder's certificate. The various reasons for revocation are described in IV.9.1.1.

The change of key pair results in the change of certificate.

IV.7.2 Origin of a new certificate request

The request for a new certificate may be made at the initiative of the Holder or the CAG if applicable.

The Holder and the MC are notified by email of the expiry of the Holder's certificate at least 1 month before the end of the validity of the Holder's certificate.

IV.7.3 Procedure for processing a new certificate request

Processing of an application for a new certificate shall be carried out under the same conditions and in accordance with the same procedures as the initial application. (cf. § IV.2 above).

IV.7.4 Notification to the holder of the drawing up of the new certificate

For any renewal: the CA notifies the Holder, and if applicable the CAG under the conditions of section IV.3.2.

IV.7.5 Procedure for accepting the new certificate

Any renewal shall be carried out under the conditions of section IV.4.1.

IV.7.6 Publication of the new certificate

See section IV.4.2.

IV.7.7 Notification by the CA to other Entities of the issue of the new certificate

See section IV.4.3

IV.8 MODIFICATION OF THE CERTIFICATE

In accordance with [RFC 3647], the modification of a certificate corresponds to changes in information without changing the public key, other than only the modification of validity dates.

This operation is not authorised by this CP. In the event of a change in information, a new certificate must be issued with the generation of a new key pair and the revocation of the old certificate.

IV.9 REVOCATION AND SUSPENSION OF CERTIFICATES

IV.9.1 Possible causes for revocation

IV.9.1.1 Holder certificates

The reasons for revoking a Holder certificate are as follows:

- compromise, suspicion of compromise, theft, loss of private key
- theft, loss or irreversible malfunction of the medium
- the Holder's information contained in his/her certificate no longer complies with the identity or use provided for in the certificate, before the end of the validity of the certificate
- non-compliance by the Holder with the applicable terms and conditions for using the certificate
- non-compliance by the Holder or the CAG with their obligations under the CP
- error detected in the registration application
- non-acceptance of the certificate by the Holder after its issue
- the holder or an authorised entity (legal representative of the Entity or CAG for example) requests the revocation of the certificate (in particular in the case of destruction or alteration of the private key of the Holder and/or its medium);
- death of the Holder, departure of the Customer Entity, termination of the Customer Entity's activity
- revocation of the CA certificate

IV.9.1.2 Certificates of a PKI component

The reasons for revoking a certificate of a PKI component are as follows:

- cessation of activity of the entity operating the component,
- compromise, suspicion of compromise, theft, loss of the means of reconstituting the component's private key (loss of the main secret, loss of the activation code and loss of more than two shared secrets),
- non-compliance with the CA's CP (detected during a negative qualification or compliance audit),
- change in PKI component
- obsolescence of cryptography with respect to ANSSI requirements (requiring renewal of the CA key pair).

IV.9.2 Origin of a revocation request

IV.9.2.1 Holder certificates

The persons authorised to request the revoking of a Holder certificate are as follows:

- The Holder in whose name the certificate was issued
- If appropriate, a CAG of the Customer Entity to which the Holder belongs
- The Legal Representative of the Customer Entity to which the Holder belongs
- The CA issuing the certificate;
- A component of CA (the RA);

IV.9.2.2 Certificates of a PKI component

The revocation of the CA certificate can only be decided by the entity responsible for the CA or by the judicial authorities via a court decision.

The revocation of the other component certificates is decided by the entity operating the component concerned, which shall inform the CA without delay.

IV.9.3 Procedure for processing a revocation request

IV.9.3.1 Revocation of a holder certificate

The requirements for identifying and validating a revocation request, whether made off-line or on-line by the revocation management function, are described in section III.4.

A revocation request may be submitted:

- By logging onto the web portal. The applicant is authenticated by certificate or by a set of Questions and Answers.
- By contacting the revocation department of IN Groupe by telephone or email.
- By post to the revocation department of IN Groupe.

The following information should *at least* be included in the request for revocation of the certificate:

- Identity of the Holder whose certificate is to be revoked
- Identity of the applicant
- Information making it possible to identify the certificate to be revoked unequivocally (serial number etc.)

Once the request has been authenticated and checked, the revocation department revokes the corresponding certificate and communicates the new status of the certificate to the certificate status information service.

The applicant, the Holder (if not the applicant) and the Holder's Customer Entity (directly or via its CAG(s)) are informed of the revocation of the Holder's certificate.

IV.9.3.2 Revocation of a certificate of a PKI component

In the event of revocation of one of the certificates in the certification chain, the CA shall inform all affected holders as soon as possible and by any means (and if possible in advance) that their certificates are no longer valid.

IV.9.4 Period allowed to the holder to formulate the request for revocation

The Holder must immediately request the revocation of his certificate as soon as a cause for revocation as defined in IV.9.1 is identified. Failing this, the request must be made by the LR or one of the CAGs attached to the Customer Entity to which the Holder is attached.

IV.9.5 Timeframe for processing a revocation request

IV.9.5.1 Revocation of a holder certificate

The CA shall process revocation requests as soon as possible after receipt, preferably immediately, and within less than 24 hours. This period refers to the time between receipt of the authenticated revocation request and the provision of revocation information to Certificate Users.

IV.9.5.2 Availability of the system for processing revocation requests

The revocation service is available 7 days a week and 24 hours a day.

The CA guarantees a maximum downtime by service interruption (failure or maintenance) of the revocation management function of 1 hour and a maximum total downtime of 4 hours per month.

IV.9.5.3 Revocation of a certificate of a PKI component

The revocation of the certificate of a PKI component is carried out immediately upon detection of an event described in the possible causes of revocation.

The revocation of a CA signature certificate (signature of certificates, CRL/ARL) is carried out immediately, particularly if the private key is compromised.

IV.9.6 Requirements for verification of revocation by certificate users

The User of a Holder certificate is required, before using it, to check the status of the certificates of the entire corresponding certification chain. The method used (ARL/CRK, OCSP, etc.) is at the discretion of the Certificate User according to their availability and the constraints related to its application.

IV.9.7 Frequency of establishment and duration of validity of CRLs

A new CRL is generated and published at least every 24 hours. The CA does not implement the CRL delta mechanism. In the event of revocation of a Holder Certificate, the CRL is immediately generated.

The CRL is valid for 4 days.

IV.9.8 Maximum time limit for publication of a CRL

After being generated, the CRL is published within a maximum of 30 minutes.

IV.9.9 Availability of an on-line system for checking the revocation and status of certificates

A complementary publication following the OCSP protocol is available.

The response time of the OCSP responder to a status request is less than 10 seconds.

IV.9.10 Requirements for on-line verification of certificate revocation by certificate users

See § IV.9.6.

IV.9.11 Other available information resources on revocations

Not applicable

IV.9.12 Specific requirements in the event of compromise of the private key

For Holder certificates, entities authorised to make a revocation request are required to do so without delay after becoming aware that the private key has been compromised.

For CA certificates, the revocation information following the compromise of the private key will be relayed on the IN Groupe website and possibly by other means (other institutional sites, press, etc.).

Information will be disseminated to the contact point of the *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI - French National Agency for Information Systems Security) identified on the website https://www.ssi.gouv.fr.

IV.9.13 Possible causes for a suspension

The suspension of certificates is not authorised by this CP.

IV.9.14 Origin of a suspension request

This point is not applicable in this CP.

IV.9.15 Procedure for processing a suspension request

This point is not applicable in this CP.

IV.9.16 Limits on the period of suspension of a certificate

This point is not applicable in this CP.

IV.10 CERTIFICATE STATUS INFORMATION FUNCTIONS

IV.10.1 Operational characteristics

The certificate status information service, available to Certificate Users, has a free consultation mechanism for the CRL and ARL. The CRL and ARL revocation lists are in V2 format, published in http at the addresses listed in § II.2.

The CRL and ARL are signed by the same CA certificate that the one used to signed de Holder certificates.

Revocation status information is available beyond the validity period of the certificates. The CRLs also contain the serial numbers of certificates that expired after their revocation.

The status of the certificates is also accessible on-line via the OCSP responder via the address listed in § II.2 and IV.9.9.

The OCSP responses are signed by an OCSP certificate issued by the same CA certificate that the one used to signed de Holder certificates.

IV.10.2 Certificate status information function availability

The certificate status information service is available 24 hours a day, 7 days a week. This service guarantees a maximum downtime by service interruption (failure or maintenance) of 2 hours and a maximum total downtime of 8 hours per month.

IV.10.3 Optional mechanisms

This point is not applicable in this CP.

IV.11 END OF THE RELATIONSHIP BETWEEN THE HOLDER AND THE CA

In the event of the termination of a contractual, hierarchical or regulatory relationship between the CA and the Holder prior to the end of the validity of its certificate, for one reason or another, the certificate is revoked.

IV.12 KEY ESCROW AND RECOVERY

Private keys associated with Holders' authentication and signature certificates cannot be held in escrow.

CA keys shall not, under any circumstances, be held in escrow.

IV.12.1 Key escrow recovery policy and practices

This point is not applicable in this CP.

IV.12.2 Session key encapsulation recovery policy and practices

This point is not applicable in this CP.

V Non-technical security measures

V.1 PHYSICAL SECURITY MEASURES

V.1.1 Geographical location and site construction

The PKI's operating sites comply with current regulations and standards as well as any specific requirements in the event of risks such as earthquakes or explosions (proximity to a factory area or chemical warehouses, etc.).

V.1.2 Physical access

The PKI resources and information used in its implementation are installed in an operating room, access to which is controlled and restricted to authorised persons only.

The access control system ensures the traceability of access to the areas where PKIs are hosted. Outside business hours, security is standard through the use of physical and logical intrusion detection methods. If unauthorised persons are required to enter operating rooms, they shall be handled by an authorised person who shall ensure their supervision. These persons shall be accompanied at all times by authorised personnel.

The machines are installed within a trusted perimeter that respects the separation of trusted roles as provided for in this CP. This security perimeter ensures that the functions and information hosted on the machines are only accessible to people with recognised and authorised trusted roles.

V.1.3 Power supply and air conditioning

Power protection and air conditioning generation systems shall be implemented to ensure the availability and continuity of the services provided, in particular the revocation management service and the certificate status information service.

The equipment used to provide the services is operated in accordance with the conditions defined by their suppliers and/or manufacturers.

V.1.4 Vulnerability to water damage

The systems are installed in such a way that they are not sensitive to flooding and other liquid spills and flows.

V.1.5 Fire prevention and protection

In order to ensure the availability of the PKI's computer systems, systems for generating electricity and protecting electrical installations are implemented. The characteristics of the power supply and air conditioning equipment make it possible to comply with the conditions of use of PKI equipment as defined by their suppliers.

V.1.6 Conservation of the media

The various information involved in the PKI's activities is identified and their security needs defined (in terms of confidentiality, integrity and availability). The CA maintains an inventory of this information and has put in place measures to prevent the compromise and theft of this information.

In particular, the media (paper, hard disk, USB keys, CDs, etc.) containing this information are managed in accordance with the defined security needs: protection against theft, damage and unauthorised access, etc.

V.1.7 Decommissioning of media

Information media are destroyed at the end of their life.

The procedures and means of destruction shall be in accordance with the level of confidentiality of the relevant information.

V.1.8 Off-site Backups

The operator shall perform off-site backups to enable rapid recovery of PKI services following the occurrence of a disaster or event that seriously and permanently affects the performance of its services, in accordance with the CA's undertakings in terms of availability, in particular for revocation management services and certificate status information.

Information backed up off-site shall comply with the requirements of this CP for the protection of the confidentiality and integrity of such information.

Backup and recovery functions are performed by ad-hoc trust roles in accordance with procedural security measures.

V.2 PROCEDURAL SECURITY MEASURES

V.2.1 Trusted roles

People are aware of and understand the implications of the operations for which they are responsible. Persons in a trusted role shall not have any conflict of interest that could affect the impartiality of operations within the PKI.

The CA's trusted roles are classified into 5 groups:

- **Security Officer** - The Security Officer is responsible for the implementation of the PKI security policy. S/he manages physical access controls to system equipment. S/he is authorised to examine the archives and is responsible for analysing event logs in order to detect any incident, anomaly, attempted compromise, etc.
- **Application Manager** - The Application Manager is responsible for the implementation of the PKI CP at the level of the application for which s/he is responsible. His/her responsibility covers all the functions rendered by this application and the corresponding performance.
- **Operating manager** - The operating manager ensures that the systems are maintained in fully operational working condition. S/he is responsible for the start-up, configuration and technical maintenance of the component's IT equipment. S/he provides the technical administration of the component's systems and networks.
- **Operator** - An operator within a component of the PKI performs, as part of his/her responsibilities, the operation of applications for the functions implemented by the component.
- **Controller or auditor** - his/her role is to regularly check the compliance of the implementation of the functions provided by the component with the CP and the component's security policies. The auditor is appointed by the PMA.

In addition to these trusted roles, the CA has defined the role of Secret Share Holder. The Secret Share Holder is responsible for ensuring the confidentiality, integrity and availability of the share entrusted to him/her.

V.2.2 Number of people required per task

The number and type of roles and persons that must be present (as persons involved or witnesses) may be different depending on the type of operations performed.

For reasons of availability, each task must be able to be performed by at least two people.

Sensitive functions (e. g. key ceremonies) are distributed over several people for security reasons.

V.2.3 Identification and authentication for each role

Each entity operating a component of the IGC shall have the identity and authorisations of any of its staff working within the component verified before assigning them a role and the corresponding rights, in particular:

- that his/her name be added to the access control lists of the entity hosting the component concerned by the role,
- that his/her name be added to the list of persons authorised to physically access these systems,
- where applicable and depending on the role, that an account be opened in his/her name in these systems,
- potentially, that cryptographic keys and/or a certificate be issued to it to fulfil its role in the PKI.

These checks are in accordance with the component's security policy.

Each assignment of a role to a member of the PKI staff shall be notified in writing. This role is clearly mentioned and described in his/her job description.

V.2.4 Roles requiring segregation of duties

Several roles may be assigned to the same person, as long as the accumulation of roles does not compromise the safety of the functions implemented. For trusted roles, however, it is recommended that the same person does not hold more than one role and at least the following requirements for non-accumulation are met. The responsibilities associated with each role are in accordance with the security policy of the component concerned.

With regard to trust roles, the following accumulations are prohibited:

- security manager and operations manager/operator,
- controller and any other role,
- operations manager and operator.

V.3 SECURITY MEASURES FOR STAFF

V.3.1 Required qualifications, skills and authorisations

Each person who works in the CA is subject to a confidentiality clause with respect to their employer. It is also verified that the powers of these persons correspond to their professional skills.

Anyone involved in PKI certification procedures is informed of their responsibilities for PKI services and procedures related to system security and personnel checking.

Management personnel have the appropriate expertise and are familiar with safety procedures.

V.3.2 Background check procedures

The CA shall use all legal means at its disposal to ensure the honesty of the staff required to work within the component. This check is based on a background check of the person (employee outside the probationary period). It is specifically checked that each person has not been convicted of a criminal offence (i.e. extract B3 from the criminal record) in contradiction with their powers.

Persons are subject to a specific authorisation (with provisions in their employment contract) and their task is defined in relation to their need to know.

Persons in a trusted role shall not have any conflict of interest that could affect the impartiality of their tasks.

These checks are carried out prior to assignment to a trusted role and reviewed regularly (at least every 3 years).

V.3.3 Initial training requirements

Personnel are trained in the internal software, hardware and operating and security procedures that they implement and must comply with, corresponding to the component in which they operate. Members of staff are aware of and understand the implications of the operations for which they are responsible.

V.3.4 Continuous training requirements and frequency

The staff concerned shall receive adequate information and training prior to any changes in systems, procedures, organisation, etc., depending on the nature of these changes.

V.3.5 Frequency and sequence of rotation between different allocations

There is no provision for a rotation frequency and sequence between the different allocations.

V.3.6 Sanctions in the event of unauthorised actions

Sanctions are provided for actions not authorised by the policies and procedures established by the CP and the internal processes and procedures of the PKI, either through negligence or which are carried out maliciously.

V.3.7 Requirements for staff of external service providers

The staff of external service providers working on the premises and/or on the components of the PKI shall also comply with the requirements of this § V.3. This is reflected in appropriate clauses in contracts with these service providers.

V.3.8 Documentation provided to staff

As a minimum, each staff member shall have adequate documentation regarding the operational procedures and specific tools they implement as well as the general policies and practices of the component in which they work. In particular, s/he shall be given the security policy or policies concerning him/her.

V.4 PROCEDURES FOR COMPILING AUDIT DATA

Event logging consists of recording events manually or electronically by input or automatic generation.

The resulting files, in paper and/or electronic form, make it possible to trace and account for the operations carried out.

V.4.1 Types of events to be recorded

Each component operating a component of the PKI shall log, as a minimum, the events as described below in electronic form. Logging is automatic from system start-up and uninterrupted until it is shut down.

- Creation/modification/deletion of User accounts (access rights) and corresponding authentication data (passwords, certificates, etc.),
- Start-up and shut-down of computer systems and applications,
- Firewall and router logs,
- Logging events: starting and stopping the logging function, changing logging settings, actions taken following the failure of the logging function, software and hardware failures,
- Logging in/out of Users with trusted roles, and corresponding unsuccessful attempts,

V.4.1.1 Information recorded for each event

Each event record in a log contains the following fields:

- Type of event,
- Name of the executor or reference of the system that triggered the event,
- Date and time of the event,
- Result of the event (failure or success).

Depending on the type of event concerned, the following fields can be saved:

- Recipient of the operation,
- Name or identifier of the applicant for the operation or reference of the system making the request,
- Name of persons present (if it is an operation requiring several people),
- Cause of the event,
- Any information characterising the event (for example, for the generation of a certificate, its serial number).

Logging operations are performed during the relevant process. In the case of manual entry, the entry is made, except in exceptional cases, on the same working day as the event.

V.4.1.2 Events recorded by the RA

The events recorded by the RA are as follows:

- Receipt of a certificate request (initial and renewal),
- Validation/rejection of a certificate request,
- Sending of the QSCD to the Holder and acknowledgement of receipt,
- explicit acceptance or rejection by the Holder,
- Activation of the medium by the Holder,
- Receipt of a revocation request,
- Validation/rejection of a revocation request,

V.4.1.3 Events recorded by the CA

The events recorded by the CA are as follows:

- Events related to signature keys and CA certificates (generation, backup / recovery, destruction, etc.),
- Generation of Holder key pairs,
- Generation of Holder certificates,
- Customisation of media and generation of activation codes,
- Publication and update of CA-related information (CP, CA certificates, PDS, etc.)
- Generation and publication of CRLs,
- OCSP requests and responses.

V.4.1.4 Various events

Other events are also collected. These are security events that are not automatically generated by the systems implemented:

- Physical access to sensitive areas,
- System maintenance and configuration change actions,
- Changes to staff in trusted roles,
- Actions to destroy and reset media containing confidential information (keys, activation data, passwords or Holder code, etc.).

V.4.1.5 Accountability

Accountability for an action rests with the person, organisation or system that carried it out. The name or identifier of the executor is explicitly included in one of the fields of the event log.

V.4.2 Frequency of event log processing

Event logs are checked and analysed by a security manager to identify anomalies related to failed attempts at the frequency defined in § V.4.8.

V.4.3 Event log retention period

Event logs are kept on site for at least 10 years. They are archived as soon as possible after their generation and at the latest within 1 month (possible recovery between the on-site storage period and the archiving period).

V.4.4 Protection of event logs

Logging is designed and implemented to limit the risk of bypassing, modifying or destroying event logs. Integrity check mechanisms are in place to detect any changes, voluntary or accidental, to these logs. The availability of event logs is protected (against loss and partial or total destruction, voluntary or not).

Systems generating event logs (except physical access control systems) are synchronised to a reliable source of UTC time (see § VI.8).

V.4.5 Event log backup procedure

Logging is designed and implemented to limit the risk of bypassing, modifying or destroying event logs. Integrity check mechanisms are in place to detect any changes, voluntary or accidental, to these logs.

The availability of event logs is protected (against loss and partial or total destruction, voluntary or not).

The event dating system associates all archives with an archive generation date.

The definition of the sensitivity of event logs depends on the nature of the information contained. It may lead to a need for confidentiality protection.

V.4.6 Event log collection system

The log collection system may be internal or external to the components of the PKI. The system ensures the collection of archives while respecting the level of security relating to data integrity, availability and confidentiality.

V.4.7 Notification of the recording of an event to the event manager

Not applicable.

V.4.8 Vulnerability assessment

Each entity operating a component of the PKI is able to detect any attempt to violate the integrity of the component in question.

Event logs are checked at least once per business day to identify anomalies related to failed attempts.

The logs are analysed in their entirety once a day and as soon as an anomaly is detected. This analysis results in a summary in which important elements are identified, analysed and explained. The summary shows the anomalies and falsifications found.

A reconciliation between the different RA and CA event logs is performed at least once a week, in order to verify the concordance between dependent events and thus help to reveal any anomalies.

In addition, a vulnerability scan is periodically carried out as part of an intrusion test campaign. The preferred method for performing these intrusion tests is a technical audit performed by a qualified information systems security audit service provider.

The vulnerabilities detected during these regular or spot checks are analysed to identify and assess their possible consequences and impacts. Depending on the criticality of the impact, an action plan is implemented to mitigate these vulnerabilities.

V.5 DATA ARCHIVING

Data archiving ensures the sustainability of the logs compiled by the various components of the PKI. It also allows the conservation of paper data related to certification operations.

V.5.1 Types of data to be archived

The data archived at the level of each component is as follows:

- Software and configuration files for each component,
- The certification policy and certification practice statement,
- Certificates, CRLs and OCSP responses as issued or published,
- CAG registration records,
- Certificate application records including the identity documents of the Holders, and their parent company where applicable,
- Event logs of the different components of the PKI.

V.5.2 Archive retention period

V.5.2.1 Certificate application files

Any accepted certificate application record shall be archived for as long as necessary for the purpose of providing proof of certification in legal proceedings, in accordance with applicable law. In this case, it is archived ten years, counted from the beginning of the validity period of the Holder certificate.

During this period of enforceability of documents, the certificate application record may be submitted by the CA at any request by the authorised authorities. This record, supplemented by the information recorded by the RA or CAG, must make it possible to find the real identity of the natural person designated in the certificate issued by the CA.

V.5.2.2 Certificates and CRLs issued by the CA

The retention period for certificates and CRLs issued by the CA, as well as for CA certificates and ARLs, is 10 years after their expiry.

V.5.2.3 OCSP Responses

OCSP responses are archived for at least three months after their expiry.

V.5.2.4 Event logs

The event logs as addressed in § V.4 is 10 years after their generation.

V.5.3 Archive protection

Throughout the entire period of their conservation, the archives:

- Are protected in terms of integrity,
- Are accessible only to authorised persons,
- Can be reviewed or used,
- Are audited and tested regularly (access, readability, exploitation and the absence of format distortion depending on the archiving media)

V.5.4 Archive backup procedure

The technical operator and the CA are responsible for implementing and maintaining the necessary measures to ensure the integrity and availability of the archives as required in this CP.

V.5.5 Data time-stamping requirements

Section VI.8 specifies the dating and time-stamping requirements.

V.5.6 Archive collection system

The system ensures the collection of archives while respecting the level of security of the archives as required by § V.5.3.

V.5.7 Procedure for retrieving and verifying archives

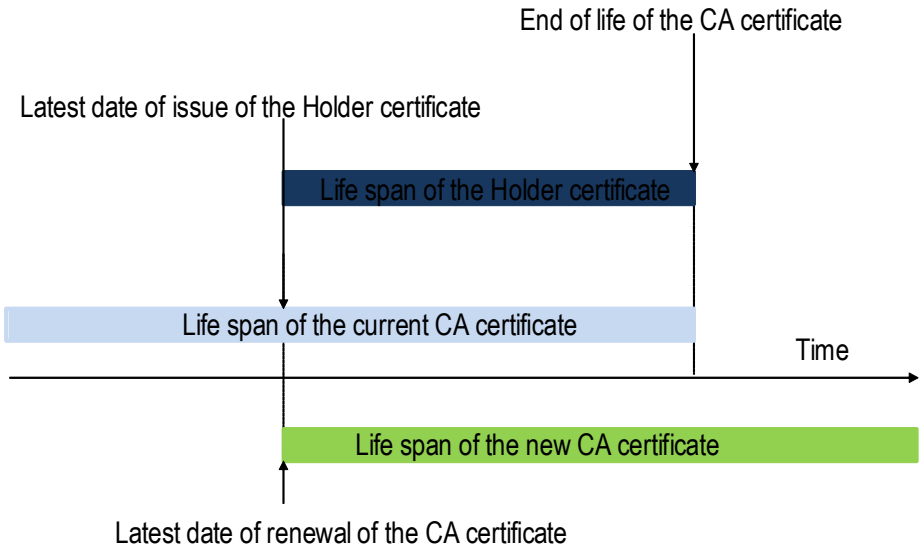
The archives (paper and electronic) are retrievable within less than 2 working days, knowing that only the CA can access all archives (as opposed to an entity operating a component of the PKI that can only retrieve and consult the archives of the component in question).

V.6 CA KEY CHANGE

The life span of the CA certificate is determined according to the validity period of the associated private key, in accordance with the security cryptographic recommendations for key lengths, including the recommendations of the relevant national or international authorities.

The CA may not generate certificates whose life span exceeds the validity period of its CA certificate. Therefore the CA key pair is renewed no later than the expiry date of the CA certificate minus the life span of the certificates issued.

As soon as a new private key is generated for the CA, only that key is used to generate new Holder certificates. The previous CA certificate remains valid to validate the certification path of the old certificates issued by the previous CA private key, until the expiry of all Holder certificates issued using this key pair.



In addition, the CA changes its key pair and the corresponding certificate when the key pair ceases to comply with cryptographic security recommendations regarding key size or if it is suspected it is compromised.

V.7 RECOVERY FROM COMPROMISE AND DISASTER

V.7.1 Procedure for reporting and handling incidents and compromises

Each entity acting on behalf of the PKI implements incident reporting and incident handling procedures. This is achieved through awareness raising and staff training and through the analysis of event logs.

In the case of a major incident, such as loss, suspicion of compromise, compromise, or theft of the CA private key, the initiating event is the recognition of this incident at the level of the component concerned, which immediately informs the CA. A major incident scenario must be dealt with as soon as it is received and the publication of information on the revocation of the certificate, if necessary, is made in the greatest urgency, or even immediately, by any useful or available means. If any of the algorithms, or associated parameters, used by the CA or its Holders become insufficient for its remaining intended use, then the CA shall notify all Holders and third-party Certificate Users with whom the CA has entered into agreements. In addition, all the certificates concerned shall be revoked.

In accordance with regulatory requirements, the National Supervisory Body (ANSSI) will be informed of any security incidents affecting the CA and its services within 24 (twenty-four) hours.

V.7.2 Recovery procedure in the event of corruption of IT resources (hardware, software and/or data)

Each component of the PKI has a business and service continuity plan that addresses the availability requirements of the various PKI functions resulting from this CP, the CA's commitments with respect to the functions related to the publication and revocation of certificates.

This continuity plan is tested at least once a year and corrective measures, if any, are implemented.

V.7.3 Procedure in case of compromise of a component's private key

The case of compromise of an infrastructure key or component check is treated in the component's continuity plan as a disaster.

In the event of compromise of a CA key, the corresponding certificate is immediately revoked as specified in § IV.9.

In addition, the CA meets the following commitments:

- Immediately stop using the key of the compromised component,
- Inform without delay: all Holders, Customer Entities with which the CA has entered into agreements and Certificate Users,
- Indicate without delay that certificates and revocation status information issued using this CA key may no longer be valid.
- Notify ANSSI of the compromise,
- If necessary, file a complaint with the competent authorities.

V.7.4 Business continuity ability in the event of a disaster

The various components of the PKI have the necessary resources (technical, organisational and human) to ensure the continuity of their activities in accordance with the requirements of this CP (see § V.7.2).

V.8 END-OF-LIFE OF THE PKI

One or more components of the PKI may have to cease their activity or transfer it to another entity for various reasons.

The CA shall take the necessary steps to cover the costs of meeting these minimum requirements in the event that the CA is bankrupt or for other reasons is unable to cover these costs on its own, to the extent possible, within the constraints of applicable bankruptcy legislation.

The transfer of activity is defined as the end of activity of a component of the PKI that does not affect the validity of certificates issued prior to the transfer and the resumption of that activity organised by the CA in collaboration with the new entity. The new entity guarantees an adequate level of trust, the maintenance of financial guarantees and continuity of service (including archiving, maintenance of confidentiality, interoperability of certificates, etc.).

Termination of activity is defined as the end of activity of a component of the PKI that affects the validity of certificates issued prior to the termination in question. Thus, the certificates issued will be revoked without delay and the entities informed of the revocation of the certificates.

In the event of cessation of activity, the CA or, if this is not possible, any entity substituted by a law, regulation, court decision or agreement previously concluded with such entity, shall ensure the revocation of certificates and the publication of ARLs/CRLs in accordance with the undertakings made in the CP.

In the event of a transfer of activity, the CA shall notify the Certificate Holders in the event that the proposed changes may affect the undertakings made and shall do so at least within one month. It will also provide information to the administrative authorities. In particular, contacts with ANSSI will be notified.

In the event of cessation of activity, the CA shall notify the Certificate Holders within one month. It will also provide information to the administrative authorities. In particular, contacts with ANSSI will be notified.

VI Technical security measures

VI.1 GENERATION AND INSTALLATION OF KEY PAIRS

VI.1.1 Key pair generation

VI.1.1.1 CA Keys

The generation of the key pairs associated with the CA certificate takes place during a key ceremony using a hardware cryptographic resource qualified at Standard level.

Key ceremonies are conducted under the control of at least three persons in trusted roles (master of ceremonies and witnesses, at least external to the CA). Witnesses shall provide objective and factual evidence of the conduct of the ceremony in relation to the script previously approved by the CA.

Following their generation, the secret shares (activation data) are given to previously designated activation data Holders who are authorised by the CA to perform this trusted role. Regardless of the form (paper, magnetic media or confined to a smart card or USB key), a Holder may not hold more than one CA secret share at any one time. Each secret share is implemented by its Holder.

VI.1.1.2 Holder keys generated by the CA

Holder key pairs are generated by the CA in a secure environment by a cryptographic module, then transferred securely to the Holder's QSCD without the CA keeping any copies.

VI.1.1.3 Holder keys generated by the Holder

Not applicable (see the Holder's key pair is generated by the CA).

VI.1.2 Transmission of the private key to its owner

The private key is transmitted to the Holder in a secure manner. Once generated by the CA, it is imported directly into the QSCD which is then sent by post to the Holder or, if applicable, via the CAG of the entity to which it is attached.

Once submitted, the private key is maintained under the sole control of the Holder.

If the identity of the Holder has not been verified face-to-face at the time of registration, it is verified when the medium is handed over personally by the CAG.

VI.1.3 Transmission of the private key to the CA

Not applicable (see the Holder's key pair is generated by the CA).

VI.1.4 Transmission of the CA public key to certificate users

The CA's public signature verification keys are distributed to Certificate Users in a manner that ensures their end-to-end integrity and authenticates their origin.

The CA public key is issued in a certificate signed by the Root CA. The public key of the Root CA is distributed in a self-signed certificate.

The CA and Root CA certificates are available at the URLs listed in section II.2 of this CP.

VI.1.5 Key sizes

The recommendations of the competent national and international bodies (concerning key lengths, signature algorithms, hash algorithms, etc.) are periodically consulted to determine whether or not the parameters used in the issue of Holder and CA certificates should be modified.

VI.1.5.1 CA Keys

The key pairs of a CA with a validity period of 10 years or more are of a complexity at least equivalent to 4096 bits for the RSA algorithm.

AC key pairs with a complexity of less than 4096 bits for the RSA algorithm are not supported by this PC.

VI.1.5.2 Holder keys

The key pairs of the issued certificates are at least equivalent in complexity to 2048 bits for the RSA algorithm and P-256 for the ECDSA-GF(P) algorithm.

VI.1.6 Verification of the generation of key pair parameters and their quality

The equipment used for the generation of the CA and Holder key pairs are material cryptographic resources qualified at enhanced level by ANSSI and therefore comply with the security standards corresponding to the key pair (see § VI.1.5).

VI.1.7 Usage objectives of the key

The use of the CA's private key and associated certificate is strictly limited to signing certificates and CRLs.

The use of the holder's private key and associated certificate is strictly limited to the security function in question (see sections I.5.1.1, IV.5).

VI.2 SECURITY MEASURES FOR PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULES

VI.2.1 Standards and security measures for cryptographic modules

VI.2.1.1 CA Cryptographic Modules

The CA cryptographic modules (for the generation and implementation of its signature keys and for the generation of Holder keys) are qualified at enhanced level, according to ANSSI requirements.

The CA implements procedures for:

- ensuring the integrity of the cryptographic modules during storage and transport,
- ensuring that the cryptographic modules are working properly,
- ensure that operations on cryptographic modules are performed by at least two staff members in trusted roles.

VI.2.1.2 Devices for protecting the secret elements of holders

The devices for protecting the secret elements of holders, for the implementation of their personal private keys, shall comply with the requirements of section XII below for the level of security concerned.

VI.2.2 Private key control by several people

This section deals with the control of the CA private key for export/import out of/into the cryptographic module. The generation of the key pair is treated in § VI.1.1, the activation of the private key in § VI.2.8and its destruction in § VI.2.10.

The checking of private CA signature keys is carried out by trusted personnel (Secret Holders) and implements a secret sharing tool (3 operators out of 5 must authenticate themselves).

VI.2.3 Holding the private key in escrow

No private keys associated with digital certificates are held in escrow.

VI.2.4 Backup copy of the private key

Holder private keys are not backed up by the CA.

VI.2.5 Archiving the private key

CA private keys shall not, under any circumstances, be archived.

The private keys of the issued certificates shall not be archived under any circumstances by the CA or any of the components of the PKI.

VI.2.6 Transfer of the private key to/from the cryptographic module

VI.2.6.1 CA private keys

CA keys are generated, activated and stored in hardware cryptographic resources.

When not stored in hardware cryptographic resources or during their transfer, CA private keys are encrypted by the AES algorithm (FIPS 197). A CA private key cannot be decrypted without the use of a hardware cryptographic resource and the presence and authentication of several persons holding trusted roles.

VI.2.6.2 Holder private keys

The transfer of the Holder's private key in the QSCD is carried out in accordance with the requirements of § VI.1.1.2.

VI.2.7 Transfer of the private key to/from the cryptographic module

CA private keys stored in hardware cryptographic resources are protected with the same level of security as the one with which they were generated.

VI.2.8 Activation method of the private key

VI.2.8.1 CA private keys

CA private keys can only be activated in the cryptographic module with a minimum of 3 people in trusted roles and who hold activation data for the CA in question.

VI.2.8.2 Holder private keys

Before being able to use its medium, the Holder must activate it. This activation requires the activation code to be entered in the activation function available on-line. The activation code is transmitted securely to the Holder. The activation method meets the requirements defined in §XII.

The medium used is such that the Holder's private key can only be activated upon presentation of an activation code.

During a signature operation, after the card has calculated the signature, the card invalidates the "PIN code submitted" status. This mechanism requires the PIN code to be entered systematically for each signature calculated by the card.

The medium is blocked after several unsuccessful attempts to enter the PIN code. This mechanism protects the medium in the event of a PIN code search by an unauthorised third party.

VI.2.9 Method for disabling the private key

VI.2.9.1 CA private keys

Hardware cryptographic resources in which CA keys have been activated shall not be left unattended or accessible to unauthorised persons. After use, hardware cryptographic resources are disabled. Cryptographic resources are then stored in a secure area to prevent unauthorised handling by roles that are not highly authenticated.

The CA's signature cryptographic resources are on-line only to sign Holder Certificates and CRLs after authenticating the certificate request and revocation request.

VI.2.9.2 Holder private keys

The private key stored on the medium is disabled after each signature calculation performed (whether or not it is powered down). The private key thus remains under the control of the Holder.

VI.2.10 Method of destroying private keys

VI.2.10.1 CA private keys

CA private keys are destroyed when they are no longer in use or when the certificates to which they correspond have expired or been revoked. The destruction of a private key involves the destruction of backup copies, activation data and the deletion of the cryptographic resource containing it, so that no information can be used to find it. The destruction of a CA private key is carried out in the presence of witnesses and is recorded in a report.

VI.2.10.2 Holder private keys

After issue of the QSCD, the Holder is the only one who can destroy the private key (by deleting or destroying the QSCD).

VI.2.11 Qualification level of the cryptographic module and secret element protection devices

The cryptographic modules used by the CA and the RCA are evaluated at EAL4+ level and qualified at enhanced level according to ANSSI requirements.

QSCDs issued by the CA are assessed at EAL4+ level and are qualified at enhanced level according to ANSSI requirements.

The CA monitors QSCD certification and ensures that the deployed product always complies with the regulations.

VI.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

VI.3.1 Public key archiving

The public keys of the CA and the Holders are archived as part of the archiving of the corresponding certificates.

VI.3.2 Life span of key pairs and certificates

The CA certificate is valid for 10 years. The life span of the corresponding key pair is equivalent, i.e. also 10 years. The CA certificate expires after the end of the Holder certificates it issues.

The certificates of the Holders covered by this CP have a maximum validity period of 3 years. The life span of the key pairs is equivalent, i.e. also 3 years.

VI.4 ACTIVATION DATA

VI.4.1 Generation and installation of activation data

VI.4.1.1 Generation and installation of activation data corresponding to the CA private key

CA private key activation data is generated during key ceremonies (refer to § VI.1.1). The activation data is automatically generated according to a Shamir threshold scheme (type M (3) of N (5)). In all cases, the activation data is given to its Holders after generation during the key ceremony. Holders of Activation Data are persons authorised for this trusted role.

VI.4.1.2 Generation and installation of activation data corresponding to the Holder's private key

The activation code is sent to the Holder by post, in a secure letter (mailer) guaranteeing the integrity and confidentiality of its content. This sending is separate in time from the sending of the QSCD to the Holder or, if applicable, to the CAG. The sending of the medium and the activation code may be carried out to separate addresses (the business address and personal address of the Holder respectively).

VI.4.2 Protection of activation data

VI.4.2.1 Protection of activation data corresponding to the CA private key

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Holders of Activation Data are responsible for its management and protection. A Holder of Activation Data may not hold more than one item of activation data of the same CA at any one time.

VI.4.2.2 Protection of activation data corresponding to Holder private keys

Holder device activation data generated by the CA is protected in confidentiality and integrity until it is provided to the Holders. It is not saved by the CA after it is delivered.

Once the QSCD is activated, the Holder initializes his/her PIN code.

Holders are responsible for the confidentiality of their PIN codes, so that only they can use the private key. In the event of a suspected loss of confidentiality, the Holders undertake to modify these PIN codes.

VI.4.3 Other aspects related to activation data

Activation data is not transmitted to any third party under any circumstances, in particular in the case where cryptographic resources are changed or returned to the manufacturer for maintenance.

VI.5 IT SYSTEM SECURITY MEASURES

VI.5.1 Technical security requirements specific to IT systems

The following functions are provided by the operating system, or by a combination of the operating system, software and physical protective mechanisms.

A component of a PKI includes the following functions:

- Strong identification and authentication of trusted roles (physical and logical access);
- Management of access rights based on profiles respecting the least privilege principle;
- Management of user sessions (disconnection after a period of inactivity, management of file access rights)
- Prohibition of the reuse of objects;
- Requires the use of cryptography for communications;
- Ensures the rigorous separation of tasks;
- Protection against computer viruses
- Protection of the network against illegal intrusion
- Performs security monitoring to ensure that security patches are regularly applied to IT systems and that critical vulnerabilities are addressed within 48 hours.
- Provides self-protection of the operating system.
- Audit function

VI.5.2 IT system qualification level

When a PKI component is hosted on a platform assessed for security assurance requirements, it is used in its certified version. At least the component uses the same operating system version as the one on which the component was certified.

VI.6 SAFETY MEASURES FOR SYSTEMS DURING THEIR LIFE CYCLE

Security measures relating to the life cycles of IT systems meet the security objectives that result from the risk analysis conducted by the CA.

VI.6.1 Security measures related to system development

System developments are controlled by the following measures:

- Purchase of hardware and software to reduce the possibility of a particular component being altered;
- The hardware and software developed were developed in a controlled environment, and the development process defined and documented. This requirement does not apply to commercially purchased hardware and software;

- All hardware and software must be shipped or delivered in a controlled manner allowing continuous monitoring from the place of purchase to the place of use;
- It is necessary to take care not to download malware on PKI equipment. Only applications required to perform TMI activities are acquired from sources authorised by applicable CA policy. CA hardware and software are scanned for malicious code on first use and periodically thereafter;
- Hardware and software updates are purchased or developed in the same way as the originals, and are installed by trusted personnel who are trained in accordance with current procedures.

VI.6.2 Measures related to security management

The configuration of the CA system, as well as any modification or change, shall be documented and checked by the CA.

There is a mechanism in place to detect any unauthorised changes to the software or CA configuration. A formal configuration management method is used for the installation and subsequent maintenance of the PKI system. When it is first loaded, it is checked that the PKI software corresponds to the one delivered by the seller, that it has not been modified before being installed, and that it corresponds to the desired version.

VI.6.3 Level of security assessment of the life cycle of systems

With respect to the software and hardware evaluated, the CA continues to monitor the requirements of the maintenance process to maintain the level of trust.

Any significant system change of a PKI component is tested and validated before deployment. These operations are carried out by trusted personnel.

The CA shall inform the national regulatory body (ANSSI), as described on https://www.ssi.gouv.fr, of any significant change in a PKI component system prior to its deployment.

VI.7 NETWORK SECURITY MEASURES

Interconnection to public networks is protected by security gateways configured to accept only those protocols necessary for the operation desired by the CA and to counter denial of service or intrusion attacks. In this case, the network is equipped with routers, firewalls with IPS intrusion detection system with alerting

The CA ensures that local network components are maintained in a physically secure environment and that their configurations are periodically audited for compliance with the requirements specified by the CA.

The IT systems administration network is logically separate from the operating network.

VI.8 TIME-STAMPING/DATING SYSTEM

There is no time stamp used by the CA but an event date that allows the CA to sequence events from the PKI system time.

Automatic or manual procedures are used to synchronise PKI system clocks with each other, at least to the nearest minute, and with respect to a reliable source of UTC time, at least to the nearest second.

VII Certificate, OCSP and CRL Profiles

VII.1 CERTIFICATE PROFILES

The certificates issued by the CA are X.509 v3 format certificates. The fields for CA certificates and Holder certificates are defined by RFC 5280.

VII.1.1 IN Groupe CA certificate profiles

The main fields of CA certificates are as follows:

AC Imprimerie Nationale Substantiel Personnel	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Racine
Validity	10 years
Subject	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel
Subject Public Key Info	4096 bits
Unique Identifiers	Not used

AC Imprimerie Nationale Elevé Personnel	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Racine
Validity	10 years
Subject	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
Subject Public Key Info	4096 bits
Unique Identifiers	Not used

As well as the following extensions:

Extensions	Criticality	Value
Authority Key Identifier	N	Identifier of the Root CA public key
Basic Constraints	O	Basic constraints: SubjectType=CertAuthority PathLengthConstraint=0
Certificate Policies	N	Certificate strategies: All issuing strategies http://www.imprimerienationale.fr/GIN/PC
CRL Distribution Points	N	ARL distribution point: URL=http://www.imprimerienationale.fr/GIN/CRL/ACR.crl URL=http://crl.imprimerienationale.fr/GIN/ACR.crl
Key Usage	O	Certificate signature Signing of the revocation list off-line Signing of the revocation list
Subject Key Identifier	N	Identifier of the CA public key

VII.1.2 Holder certificate profiles

The main fields of Holder certificates are as follows:

AC Imprimerie Nationale Substantiel Personnel	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel
Validity	3 years
Subject	See section 7.2
Subject Public Key Info	See section 5 on requirements in terms of algorithms and key lengths.
Unique Identifiers	Not used.

AC Imprimerie Nationale Elevé Personnel	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI

Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
Validity	3 years
Subject	See section 7.2
Subject Public Key Info	See section 5 on requirements in terms of algorithms and key lengths.
Unique Identifiers	Not used.

VII.1.2.1 Certificate extensions when used on a QSCD:

Extensions	Criticality	Value	
Authority Key Identifier	N	Contains the key identifier of the issuing CA's public key (same value as the "Subject Key Identifier" field of the certificate of that issuing CA). Method 1 defined in RFC 5280 section 4.2.1.2.	
Basic Constraints	N	Basic constraints: SubjectType=EndEntity PathLengthConstraint=none	
Certificate Policies	N	As a minimum, the OID of the CP of the issuing CA	
Subject Alternative Name	N	Other name of the object: Name RFC822 Principal Name (UPN) [Optional Value]	
Issuer Alternative Name	N	Not used	
Subject Directory Attributes		Not used	
CRL Distribution Points	N	Distribution points to the CRL of the issuing CA.	
Authority Information Access	N	Point of distribution to the issuing CA's OCSP	
Freshest CRL	N	Not used	
Subject Key Identifier	N	Identifier of the Holder's public key	
		Authenticity certificates	**Signature Certificates**
Key Usage	O	digitalSignature	nonRepudiation
Extended Key Usage	N	id-kp-clientAuth id-ms-smartcardlogon	id-kp-emailProtection
Qc Compliance	N	Not used	id-etsi-qcs 1
QcSSCD	N	Not used	id-etsi-qcs 4
QcType	N	Not used	id-etsi-qct-esign
QcPDS	N	Not used	URL to the PDS

Note: The nonRepudiation bit is now called contentCommitment.

VII.1.2.2 Certificate extensions when used on a SCD:

Extensions	Criticality	Value	
Authority Key Identifier	N	Contains the key identifier of the issuing CA's public key (same value as the "Subject Key Identifier" field of the certificate of that issuing CA). Method 1 defined in RFC 5280 section 4.2.1.2.	
Basic Constraints	N	Basic constraints: SubjectType=EndEntity PathLengthConstraint=none	
Certificate Policies	N	As a minimum, the OID of the CP of the issuing CA	
Subject Alternative Name	N	Other name of the object: Name RFC822 Principal Name (UPN) [Optional Value]	
Issuer Alternative Name	N	Not used	
Subject Directory Attributes		Not used	
CRL Distribution Points	N	Distribution points to the CRL of the issuing CA.	
Authority Information Access	N	Point of distribution to the issuing CA's OCSP	
Freshest CRL	N	Not used	
Subject Key Identifier	N	Identifier of the Holder's public key	
		Authenticity certificates	**Signature Certificates**
Key Usage	O	digitalSignature	nonRepudiation
Extended Key Usage	N	id-kp-clientAuth id-ms-smartcardlogon	id-kp-emailProtection
Qc Compliance	N	Not used	id-etsi-qcs 1
QcSSCD	N	Not used	Not used
QcType	N	Not used	id-etsi-qct-esign
QcPDS	N	Not used	URL to the PDS

Note: The nonRepudiation bit is now called contentCommitment.

VII.1.3 Algorithm identifier

The identifiers of the algorithms used are:

- Sha-256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}.
- Sha-384WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}.

- Sha-512WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}.

VII.1.4 Name forms

The name forms comply with the requirements of the § III.1.1 for the identity of the Holders and the CA which is included in the certificates issued by the CA.

VII.1.5 Object ID (OID) of the CP

Holder certificates contain the OID of the certificate template (see & **Erreur ! Source du renvoi introuvable.**).

VII.1.6 Extensions specific to the use of the policy

Not applicable

VII.1.7 Syntax and semantics of policy qualifiers

Not applicable

VII.1.8 Semantic interpretation of the "Certificate Policies" critical extension

No requirement formulated

VII.2 CRL PROFILES

IN Groupe CAs issue CRLs with the following characteristics:

CRL Characteristics	Period of validity	:	4 days
	Update frequency	:	daily
	CRL version (v1 or v2):	v2	
	Extensions:		CRL and AKI number
	Publication http URL:		See § II.2

The main fields of the CRL are:

AC Imprimerie Nationale Substantiel Personnel	
Basic fields	**Value**
Version	1 (=version 2)
Serial Number	Defined by the PKI
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel

This Update	Date CRL generated
Next Update	Deadline for issue of the next CRL.
Revoked certificates	List of serial numbers of revoked Holders' certificates

AC Imprimerie Nationale Elevé Personnel	
Basic fields	**Value**
Version	1 (=version 2)
Serial Number	Defined by the PKI
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
This Update	Date CRL generated
Next Update	Deadline for issue of the next CRL.
Revoked certificates	List of serial numbers of revoked Holders' certificates

Plus the following extensions:

Extensions	Criticality	Description
Authority Key Identifier	N	Contains the key identifier of the issuing CA's public key (same value as the "Subject Key Identifier" field of the certificate of that issuing CA). Method 1 defined in RFC 5280 section 4.2.1.2.
CRL Number	N	CRL serial number
ExpiredCertsOnCRL	N	Indicate that the CRLs also contain the serial numbers of certificates that expired after their revocation.

VII.3 OCSP PROFILE

An OCSP responder is set up to check the status of certificates issued by IN Groupe CAs on-line. OCSP responses are signed by the OCSP responder whose certificate is issued by the CA issuing the verified certificate (see rfc6960).

In order to ensure the availability of revocation status at any time and beyond the validity period of the certificate, OCSP responses contain the extension "*id-pkix-ocsp-archive-cutoff*" in accordance with RFC 6960 containing the valid-from date of the issuing CA.

AC Imprimerie Nationale Substantiel Personnel	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = FR O = Groupe Imprimerie Nationale

	OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel
Subject DN	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN =[OCSP Service Name]
Life span	1 year

AC Imprimerie Nationale Elevé Personnel	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
Subject DN	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN =[OCSP Service Name]
Life span	1 year

Plus the following extensions:

Extensions	Criticality	Value
Authority Key Identifier	N	Contains the key identifier of the issuing CA's public key (same value as the "Subject Key Identifier" field of the certificate of that issuing CA). Method 1 defined in RFC 5280 section 4.2.1.2.
Basic Constraints	N	Basic constraints: SubjectType=EndEntity PathLengthConstraint=none
Certificate Policies	N	As a minimum, the OID of the CP of the issuing CA
Key Usage	O	digitalSignature
Subject Key Identifier	N	Identifier of the OCSP responder's public key
Extended Key Usage	N	OCSP Signing

OCSP No Check	N	Null

VIII Compliance audit and other evaluations

Audits and evaluations concern:

- on the one hand, those carried out with a view to issuing a qualification certificate according to the qualification scheme for trust service providers in accordance with the eIDAS Regulations,
- and on the other hand, those that the PMA must carry out, or have carried out, in order to ensure that all its PKI, and where applicable all CAGs, comply with the undertakings published in this CP.

The CA reserves the right to conduct unannounced audits of CAGs in the same way as its PKI staff.

VIII.1 FREQUENCY AND/OR CIRCUMSTANCES OF EVALUATIONS

Prior to the first commissioning of a component of its PKI or following any significant change within a component, the PMA shall also have that component checked for compliance. The PMA also carries out:

- a compliance check once a year of its entire PKI as part of the CA's eIDAS qualification,
- a check once every 2 years of compliance with the ETSI EN 319 411-1 and ETSI EN 319 411-2 standards.

A compliance check of the CA was carried out before first commissioning to obtain the eIDAS qualification.

VIII.2 IDENTITIES/QUALIFICATIONS OF ASSESSORS

The checking of a component must be assigned by the PMA to a team of auditors competent in information systems security and in the field of activity of the checked component. They are authorised, if necessary.

VIII.3 RELATIONSHIP BETWEEN ASSESSORS AND EVALUATED ENTITY

The audit team is in no way part of the entity operating the audited PKI component, whatever that component may be, and is duly authorised to carry out the specified checks.

VIII.4 TOPICS COVERED BY THE ASSESSMENTS

Compliance checks cover a component of the PKI (spot checks) or the entire architecture of the PKI (periodic checks) and aim to verify compliance with undertakings and practices (operational procedures, resources implemented, etc.) defined in the CA's CP.

VIII.5 ACTIONS TAKEN IN RESPONSE TO ASSESSMENT FINDINGS

Following a compliance audit, the audit team issues one of the following opinions to the PMA: "success", "failure", "to be confirmed".

According to the opinion given, the consequences of the check are as follows:

- In the event of failure, and depending on the size of the non-conformities, the audit team issues recommendations to the PMA, which may be cessation (temporary or permanent) of activity, revocation of the component certificate, revocation of all certificates issued since the last positive check, etc. The choice of the measure to be applied is made by the PMA and must comply with its internal security policies.

- In the event of a "to be confirmed" result, the PMA shall provide the component with a notice specifying the period within which the non-conformities must be resolved. Then, a "confirmation" check will verify that all critical points have been resolved.
- If successful, the PMA confirms to the audited component that it complies with the CP requirements.

VIII.6 DISCLOSURE OF RESULTS

The results of compliance checks are disclosed only and solely to the audited component and to the PMA manager. They include the component's corrective actions already taken or in progress.

Given the confidential nature of the results, they will not be published without the authorisation of all parties, nor transmitted to other persons involved without their agreement.

However, the results of compliance audits must be made available to the body responsible for the CA's qualification.

IX Other business and legal issues

IX.1 RATES

IX.1.1 Rates for the provision or renewal of certificates

Pricing is established on the basis of a global offering of IN Groupe services integrating a set of services including the issue and management of digital certificates and signature and authentication media. This pricing, which can be reviewed annually, is defined in the general terms and conditions of services.

IX.1.2 Rates for accessing certificates

Certificates are freely accessible to Certificate Users.

IX.1.3 Rates for accessing certificate status and revocation information

Certificate status and revocation information is available free of charge on the publishing server.

IX.1.4 Rates for other services

No special requirements.

IX.1.5 Refund policy

No special requirements.

IX.2 FINANCIAL RESPONSIBILITY

IN Groupe undertakes to comply with this CP. Any additional conditions not included in this document cannot be considered as an obligation of IN Groupe.

IX.2.1 Insurance coverage

IN Groupe applies reasonable levels of insurance coverage and has taken out public liability insurance for the performance of its professional activity.

IX.2.2 Other resources

IN Groupe is in a financial position to fulfil its task.

IX.2.3 Coverage and guarantee for user entities

User entities must be financially capable of carrying out their task.

In the event of damage for a customer caused by one of the CAs under the control of IN Groupe, the latter shall call upon its insurance to cover part of the customer's damage within the limit of IN Groupe's liability as defined in the general terms and conditions of IN Groupe services and herein.

IX.3 CONFIDENTIALITY OF BUSINESS DATA

IX.3.1 Scope of confidential information

The information considered confidential shall be at least the following:

- the non-public parts of the CA CP and associated internal procedures,
- the private keys of the CA, its components and Certificate Holders
- the activation data associated with the CA private keys as well as those associated with the Holders' private keys (before such data is transmitted to the Holders),
- all the secrets of the PKI,
- the event logs of the different components of the PKI,
- the elements relating to the key ceremony, including the identity of the Secret Holders
- the causes of revocations, unless explicitly agreed by the Holder,
- the Holders' registration records,
- audit reports.

Only authorised persons may access it.

IX.3.2 Information outside the scope of confidential information

Published information concerning the PKI is considered to be non-confidential and is disclosed on a need-to-know basis.

IX.3.3 Responsibility for the protection of confidential information

The CA is required to apply security procedures to ensure the confidentiality of the information identified in § IX.3.1, in particular with respect to the permanent erasure or destruction of the media used for their storage and backup.

In addition, when these data are exchanged, the CA must ensure their integrity.

In particular, the CA is required to comply with the legislation and regulations in force on French territory, in particular disclosure to judicial and/or administrative authorities. In particular, it may be required to make the registration files of the Holders available to third parties as part of legal proceedings. It must also give the Holder access to his/her registration file, where applicable to the CAG and to the RA operators in connection with the Holder's affiliated Customer Entity.

IX.4 PROTECTION OF PERSONAL DATA

IX.4.1 Personal data protection policy

It is understood that any collection and use of personal data by the CA and all its components is carried out in strict compliance with the legislation and regulations in force on French territory, in particular Law No. 78-17 of 6 January 1978, as amended, known as "*Informatique et Libertés*" (French Data Protection Law).

In accordance with the *loi informatique et libertés* (French Data Protection Act) (article 40 of the Law of 6 January 1978), the CA gives Certificate Holders the right to access and modify their personal data in the event of inaccurate, incomplete or ambiguous data at the time of its collection. To exercise this right, the Holders must contact the Registration Authority. In the event of correction of personal data, the CA reserves the right to revoke the valid certificate in the event of an impact on its content.

IX.4.2 Personal data

The CA considers that the following information is personal data:

- The registration records of Holders and CAGs;
- Holders' certificate requests;
- Requests for revocation;
- The reasons for revocation of Holder certificates.

IX.4.3 Non-personal data

In this context, no liability of any kind whatsoever may be incurred.

IX.4.4 Liability in terms of personal data protection

See § **Erreur ! Source du renvoi introuvable.**

The CA has put in place and complies with measures to protect personal data, in particular in order to guarantee its security, while respecting the principles of proportionality and transparency.

IX.4.5 Notification of and consent to use personal data

The CA undertakes to respect the purpose of the collection and processing of personal data.

In accordance with the laws and regulations in force on French territory, the personal information identified in this CP must not be disclosed or transferred to a third party except in the following cases: prior consent of the data owner), judicial decision or other legal authorisation.

IX.4.6 Conditions for disclosing personal information to judicial or administrative authorities

The CA acts in accordance with the regulations in force on French territory and has procedures for disclosing personal information to judicial and administrative authorities at their express request.

IX.4.7 Other circumstances for disclosing personal data

Not applicable

IX.5 INTELLECTUAL PROPERTY RIGHTS

This CP is part of the respect of intellectual and industrial property rights. IN Groupe retains all intellectual property rights and owns this CP, the certificates it issues and the corresponding revocation information it publishes.

IX.6 CONTRACTUAL INTERPRETATIONS AND GUARANTEES

The obligations common to the components of the PKI are as follows:

- to protect and guarantee the integrity and confidentiality of their secret and/or private keys as well as any activation data;
- to use their cryptographic keys (public, private and/or secret) only for the intended purposes when they are issued and with the tools specified under the conditions set by this CP and the resulting documents;
- to respect and apply the part of the CP for which they are responsible (this part must be communicated to the corresponding component);
- to submit to compliance checks carried out by the audit team mandated by the PMA and the qualification body;
- to implement appropriate measures to correct the discrepancies detected during these compliance checks;
- to respect the agreements or contracts that bind them between themselves or to the Holders;
- to document their internal operating procedures;
- to implement the resources (technical, organisational and human) necessary to perform the services to which they commit themselves under conditions guaranteeing quality and safety;
- to implement awareness-raising and training actions;
- to set up documentation of the responsibility of each of the parties involved in question.

IX.6.1 Certification Authority

The CA undertakes to:

- Be able to demonstrate to Certificate Users that it has issued a certificate for a given Holder and that the Holder has accepted that certificate in accordance with § 4.4;
- Ensure and maintain the consistency of its CP;
- Respect and ensure respect for the parts of the CPSs concerned by the various components;
- Take all reasonable measures to ensure that its Holders are aware of their rights and use with respect to the use and management of keys, certificates or equipment and software used for the purposes of the PKI. The relationship between a Holder and the CA is formalised in a contractual or hierarchical relationship specifying the rights and obligations of the parties and in particular the guarantees provided by the CA;
- Carry out audits;
- Raise awareness among the various parties involved regarding security and the technologies used.

IN Groupe must take the necessary measures to cover the responsibilities related to its activities and have the financial stability and resources required to operate in accordance with this CP.

In addition, the CA acknowledges that it is liable for any duly proven fault or negligence by itself or any of its components, regardless of its nature and gravity, that would result in the reading, alteration and misuse of Holders' personal data for fraudulent purposes, whether contained in or in transit in the CA's certificate management applications.

In addition, the CA acknowledges that it has a general duty to monitor the security and integrity of certificates issued by the CA or one of its components. It is responsible for maintaining the security level of the technical infrastructure on which it relies to provide its services. Any changes that have an impact on the level of security provided must be approved by the CA's senior management.

IX.6.2 Registration service

The RA's obligations are:

- Identification and authentication of the Holder, through the CAG if applicable, and identification of its Customer Entity;
- Checking the registration file of the future Holder, validation and processing of certificate applications;
- Checking the registration records of future CAGs;
- The delivery of personalised support to the Holder, via the CAG if applicable;
- The secure sending of activation data to the Holder;
- Identification of the issuer of a revocation request, validation and processing of this request;
- Compliance with the CP of the issuing CA;
- Ensuring the Holder's knowledge and acceptance of his/her obligations (included in the General Terms and Conditions of Use);
- Ensuring that RA operators and CAGs comply with their respective obligations (relevant parts of the CP, letters of appointment, etc.);

IX.6.3 Certificate holders

The Holders are required to:

- Provide accurate and up-to-date information when applying for a certificate (initial application or renewal);
- Protect the QSCD they have been given, their private keys and activation data;
- Comply with the conditions of use of his/her private key and the corresponding certificate (described in the PDS and the CP);
- Inform the CA of any changes to the information contained in their certificate;
- Promptly apply to the RA, or where applicable the CAG, for the revocation of their certificate upon the occurrence of any of the events listed in § IV.9.1.

IX.6.4 Certificate users

Certificate Users must:

- Verify and respect the use for which a certificate has been issued;
- For each certificate in the certification chain, from the Holder's certificate to the RCA certificate, verify the signature of the CA issuing the certificate in question and check the validity of this certificate (validity dates, revocation status);
- Verify and comply with the obligations of Certificate Users expressed in this CP.

IX.6.5 Other participants

Not applicable.

IX.7 LIMIT OF GUARANTEE

The CA guarantees through its PKI services:

- Their identification and authentication through their certificate signed by the IN Groupe Root CA;
- The identification and authentication of Holders through the certificates it issues to them;
- Management of the corresponding certificates and certificate validity information according to this CP.

These warranties are exclusive of any other CA warranty.

It is expressly understood that IN Groupe cannot be held liable for any damage resulting from the fault or negligence of a Customer and/or its Holders or for any damage caused by an external event or force majeure, in particular in the event of:

- Use of the private key for a purpose other than that defined in the associated certificate;
- Using a certificate for an application other than Authorised Applications;
- Use of a certificate to guarantee an object other than the identity of the Holder;
- Use of a revoked certificate;
- Incorrect storage methods for the private key of the Holder's certificate;
- Using a certificate beyond its validity limit;

- Non-compliance with the obligations of other Stakeholders (see § IX.6.4);
- Events external to the issue of the certificate such as a failure of the application for which it can be used;
- Force majeure as defined by French courts.

IX.8 LIMITATION OF LIABILITY

The CA can only be held liable in the cases listed exhaustively below:

- in the event of proven direct damage to a Holder or an application/Certificate User as a result of a breach of the procedures defined in the CP, the CA's fault must be duly proven;
- in the event of proven compromise, entirely and directly attributable to the CA.

The CA disclaims any responsibility for the use of certificates issued by it under conditions and for purposes other than those provided for in this CP and any related applicable contractual documents, in particular:

- use of a certificate for a purpose other than authentication of the Holder or protection of electronic mail;
- use of a certificate to guarantee an object other than the identity of the Holder for whom it was issued;
- use of a revoked certificate;
- use of a certificate beyond its validity limit.

The CA cannot be held liable for the consequences of delays or losses in the transmission of any electronic messages, letters, documents, and for any delays, alterations or other errors that may occur in the transmission of any telecommunications.

The CA cannot be held liable, and shall not assume any liability, for any delay in the performance of obligations or for any failure to perform obligations resulting from this CP when the circumstances giving rise to them and which could result from the total or partial interruption of its activity, or from its disorganisation, fall within the scope of force majeure within the meaning of Article 1148 of the *Code civil* (French Civil Code).

In addition to those usually retained by French court and tribunal case law, labour disputes, the failure of the network or external telecommunications installations or networks are expressly considered to be force majeure or unforeseeable circumstances.

The CA disclaims any liability for indirect damages (including financial or commercial damages) which, as a result, do not give rise to any right to compensation.

In any event, any compensation that IN Groupe may be required to pay in respect of a proven breach of its obligations may not exceed the amount(s) specified in § IX.9 below.

IX.9 COMPENSATION

If a proven fault of IN Groupe in the performance of its obligations under this CP as a CA is established and has directly caused damage, IN Groupe will compensate the relevant person/Customer Entity within the limit defined in the service contract.

IX.10 DURATION AND EARLY TERMINATION OF THE VALIDITY OF THE CP

IX.10.1 Period of validity

The CP becomes effective on its date of validation by the PMA listed herein.

The CA CP shall remain in force at least until the end of the life of the last certificate issued under this CP.

IX.10.2 Early end of validity

The publication of a new version of this CP, may lead, depending on the changes, the need for the CA to have changes made to the associated CPs. Depending on the nature of the changes, the deadline for compliance is set in accordance with the procedures provided for by the regulations in force.

Compliance does not require the early renewal of certificates already issued, except in exceptional cases related to changes in the security requirements contained in this CP.

IX.10.3 Effect of the end of validity and clauses remaining applicable

The clauses that remain applicable beyond the end of use of the CP are those concerning data archiving. All other obligations shall lapse and be replaced by those described in the CP(s) still in force.

IX.11 INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS BETWEEN PARTICIPANTS

In the event of a change of any kind in the composition of the PKI, the PMA undertakes:

- to have this change validated through a technical assessment no later than one month before the start of the operation, in order to assess the impacts on the level of quality and safety of the CA's functions and its various components;
- to inform the qualification body no later than one month after the end of the operation.

The PMA undertakes to send ANSSI a summary of all the changes made to the provision of its qualified trust services on an annual basis.

IX.12 AMENDMENTS TO THE CP

IX.12.1 Amendment procedures

The PMA reviews its CP periodically at least once a year and:

- whenever there are changes in PKI systems or internal PKI procedures that have an impact on the CP;
- whenever a significant change in industry practice or in existing legislation/regulation justifies it;
- or when the results of compliance audit checks so require (non-compliance with the standard CP).

The adoption of amendments shall be carried out under the same conditions as the adoption of the CP and in accordance with the principle of congruent forms.

In the event of a major modification of the CP, the PMA shall verify the compliance of the CP with "electronic personal certificates" type CPs, and the compliance of practices with this new version of the CP. The CP is only applicable after validation by the PMA.

IX.12.2 Mechanisms and notification periods for amendments

The PMA shall give at least two months' notice to the CA components of its intention to modify its CP before making the changes and depending on the purpose of the change.

This time limit applies only to changes of substance (change of key size, change of procedure, change of certificate profile, etc.) and not to the form of the PC.

NB: spelling or typographical corrections do not require notification from the PMA.

IX.12.3 Circumstances under which the OID must be changed

Since the CA's OID is included in the certificates they issue, any change to this CP that has a major impact on certificates already issued must result in a change to the OID, so that Certificate Users can clearly distinguish which certificates correspond to which requirements.

However, Certificate Holders and Users can easily identify and access on the publishing site the version of the CP under which the relevant certificate was issued by the CA. In addition to the current version of the CP, the site disseminates all the old versions, each of which clearly shows the date of publication and therefore the period over which it was in force.

The CA shall inform the national supervisory body (ANSSI) as soon as possible of any change in the OID before it is issued, in accordance with the procedures described on the website https://www.ssi.gouv.fr.

IX.13 PROVISIONS CONCERNING CONFLICT RESOLUTION

The PMA shall establish policies and procedures for the handling of complaints and the settlement of disputes from Customer Entities for which it provides electronic trust services.

IX.14 COMPETENT JURISDICTIONS

The provisions of the CP are governed by French law. In the event of a dispute relating to the interpretation, formation or execution of this CP and in the absence of an amicable settlement, the jurisdiction shall be that of the Courts of the IN Groupe's registered office.

IX.15 COMPLIANCE WITH LAWS AND REGULATIONS

The policies and procedures by which the CA operates are non-discriminatory.

The IN Groupe shall set up, whenever possible, means to facilitate access to its services for people with disabilities.

In addition, the IN Groupe issues certificates to administrations and entities that are already subject to regulatory obligations relating to accessibility. As a result, the use of the services offered by the IN Groupe within these establishments is embedded in the accessibility systems set up by these same entities.

The laws and regulations applicable to the CP are, in particular, those indicated in § X.

IX.16 MISCELLANEOUS PROVISIONS

IX.16.1 Global agreement

Not applicable.

IX.16.2 Transfer of activities

See § V.8

IX.16.3 Consequences of an invalid clause

If any provision of this CP is found to be invalid under applicable law, this shall not affect the validity and enforceability of the remaining provisions.

IX.16.4 Application and waiver

Not applicable

IX.16.5 Force majeure

All cases of force majeure usually retained by the French courts are considered as force majeure, including the case of an irresistible, insurmountable and unforeseeable event.

IN Groupe cannot be held liable, and shall not assume any liability, for any delay in the performance of obligations or for any failure to perform obligations resulting from this CP when the circumstances giving rise to them fall within the scope of force majeure within the meaning of Article 1148 of the *Code civil* (French Civil Code).

IX.17 OTHER PROVISIONS

This CP does not make any specific requirements on this subject.

X Appendix 1: Documents referenced

X.1 REGULATIONS

Law no. 78-17 of 6 January 1978 relating to computing, files and freedoms, amended by law no. 2004-801 of 6 August 2004 (French Data Processing Act); https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
[eIDAS Regulation] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the so-called "eIDAS Regulation")
Article 801-1 of the *code de procédure pénale* (French criminal procedure code)
Decree No. 2001-272 of 30 March 2001 implementing Article 1316-4 of the *code civil* (French Civil Code) on electronic signatures http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=vig
Order of 26 July 2004 on the recognition of the qualification of providers of electronic certification services and the accreditation of bodies that assess them http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678&dateTexte=vig
Law no. 2000-321 of 12 April 2000 on the rights of citizens in their relations with administrations http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629288&dateTexte=vig
Law no. 2004-575 of 21 June 2004 on confidence in the digital economy http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id
Ordinance No. 2011-1012 of 24 August 2011 on electronic communications http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024502658&categorieLien=id

Directives known as the "Telecom Package" which includes:
- a Directive (2009/140/EC) amending three existing Directives:
- access Directive (2002/19/EC)
- authorisation Directive (2002/20/EC)
- framework directive (2002/21/EC)
- a Directive (2009/136/EC) amending two existing Directives:
- universal Service Directive (2002/22/EC)
- directive on privacy and electronic communications (2002/58/EC)
- Regulation (EC) No 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC)

X.2 TECHNICAL DOCUMENTS

[RGS_A_2] "Personal Digital Certificates" type Certification Policy - Version 3.0
[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[ETSI] ETSI EN 319401 v2.1.1: General Policy Requirements for Trust Service Providers ETSI EN 319411: Policy & Security Requirements for TSPs Issuing Certificates ETSI EN 319412: Certificate Profiles

XI Appendix 2: CA Cryptographic Module Security Requirements

XI.1 REQUIREMENTS FOR SAFETY OBJECTIVES

The cryptographic module, used by the CA to generate and implement its signature keys (for the generation of electronic certificates, CRL/ARLs and, if applicable, OCSP responses), as well as, if applicable, to generate the key pairs of the issued certificates, must meet the following security requirements:
- if the key pairs of the issued certificates are generated by this module, ensure that these generations are performed exclusively by authorised users and guarantee the cryptographic robustness of the generated key pairs;
- if the key pairs of the issued certificates are generated by this module, ensure the confidentiality of private keys and the integrity of private and public keys when they are under the responsibility of the CA and during their transfer to the Holder's cryptographic device and ensure their safe destruction after such transfer;
- ensure the confidentiality and integrity of CA private signing keys throughout their life cycle, and ensure their safe destruction at the end of their life;
- be able to identify and authenticate its users;
- limit access to its services according to the user and the role assigned to him/her;
- be able to conduct a series of tests to verify that it is working properly and enter a safe state if it detects an error;
- allow the creation of a secure electronic signature, for signing certificates generated by the CA, that does not reveal the CA's private keys and cannot be forged without knowledge of these private keys;

- create audit records for each security change;
- if a CA private key backup and recovery function is offered, ensure the confidentiality and integrity of the backed up data and require at least dual control of backup and recovery operations.

The CA cryptographic module detects attempted physical alterations and enters a safe state when an attempted alteration is detected

XI.2 QUALIFICATION REQUIREMENTS

The cryptographic module used by the CA is subject to qualification, at enhanced level, according to the process described in the [RGS], and complies with the requirements of section 11.1 above.

XII Appendix 3: Security requirements of the protection device for secret elements

XII.1 REQUIREMENTS FOR SAFETY OBJECTIVES

The cryptographic device used by the Holder to store and implement its private key and, if necessary, generate its key pair, must meet the following security requirements:

- if the key pair of the issued certificate is generated by the device, ensure that this generations is performed exclusively by authorised users and guarantee the cryptographic robustness of the generated key pair;
- ensure correspondence between the private key and the public key;
- generate a stamp or authentication that cannot be falsified without knowledge of the private key.

In addition, organisational, procedural or technical security measures must be put in place in order to:

- detect defects during initialisation, customisation and operation phases and have secure techniques for destroying the private key in the event of re-generation of the private key;
- guarantee the confidentiality and integrity of the private key;
- ensure the authenticity and integrity of the public key when exporting it from the device.

XII.2 QUALIFICATION REQUIREMENTS

The CA provides the Holder with a secret elements' protection mechanism, qualified at enhanced level, according to the process described in the [RGS], and complies with the requirements of section 12.1 above.