IN GROUPE

Root Certification Policy

CA Certificate

Security Document

Distribution Method	**EXTERNAL**
Document Status	**VALIDATED**
Application Date	01/01/2020

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

VERSION HISTORY

Version	Date	Author	Nature of revision Paragraphs modified
1.0	09/02/2017	Imprimerie Nationale	Initial version
2.0	13/08/2019	Franck Leroy (IN Groupe)	Restructuring

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

CONTENTS

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

I Introduction

I.1 GENERAL PRESENTATION

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 *Référentiel Général de Sécurité* (RGS - French General Security Database) and the European eIDAS regulations.

IN Groupe thus offers certificate issue services aimed at implementing authentication and signature functions. IN Groupe is an Electronic Certification Service Provider.

This document constitutes the certification policy (CP) of IN Groupe Root 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 under 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 Root CA self-signs its certificate and signs the Authority Revocation List (ARL) and certificates of the Subordinate Certification Authorities (SCAs). The SCAs issue certificates to holders.

Therefore, the hierarchy of certification authorities is the following:

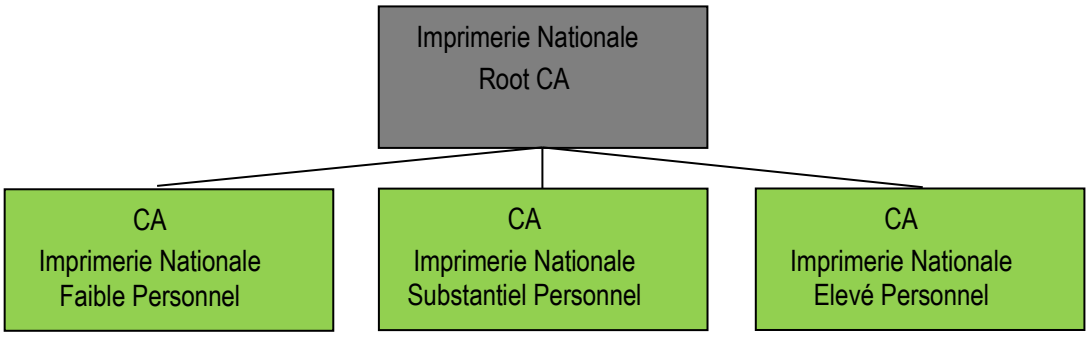


Figure1: Hierarchy of Certification Authorities

The purpose of this document is to describe the life cycle management of the certificate and associated key pairs of the Root CA and SCAs. It is also the general framework applicable to SCAs, which will be the subject of complementary policies in order to set out their specificities.

As the Root CA and SCAs are under the responsibility of IN Groupe, we will refer to the moral authority responsible for the Root CA and SCAs under the acronym CA.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

The structure of this document complies with [RFC3647] "X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework" of the Internet Engineering Task Force (IETF).

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 NAME OF THE DOCUMENT AND IDENTIFICATION

This named CP is the property of IN Groupe.
This CP is identified in the following table by the following OIDs:

Name of the Certification Authority	
Imprimerie Nationale Root CA	1.2.250.1.295.1.1.13.8.2.109.1
All the Subordinate CAs	1.2.250.1.295.1.1.13.8.2.109.1

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 Practice Statement
HSM	*Hardware Security Module*
ICD	*International Code Designator*
PKI	Public Key Infrastructure
IN Groupe	Groupe Imprimerie Nationale
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
ARL	Authority Revocation List

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

CRL	Certificate Revocation List
LDAP	*Lightweight Directory Access Protocol*
RLAR	Registered Letter with Acknowledgment of Receipt
CAG	Certification Agent
OID	*Object Identifier*
CP	Certification Policy
OCSP	Online Certificate Status Protocol
CSO	Certification Services Operator
QSCD	Qualified Signature Creation Device
LR	Legal representative
RSA	Rivest Shamir Adleman
SHA-256	*Secure Hash Algorithm 256*
PS	Publication Service
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.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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]

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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 one or more certification authorities (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 chapter §.

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 CA (Root CA or SCA) and provides the public key to be certified to the certificate generation service.
- Generation of certificates: This service generates electronic certificates for the Root CA or SCAs from information provided by the registration authority.
- Revocation: This service processes certificate revocation requests from CA (Root CA or SCA) and determines the actions to be taken, including generation of the list of revoked CAs (ARL).
- Publication: This service provides certificate users (CUs) and certificate holders with the information required to use certificates issued by CAs (General Terms and Conditions of Use, CP, CA certificates, etc.) as well as the processing results of the certificate revocation management service (ARL, information notice, etc.).

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

I.4.1 Certification Authorities

The Root CA generates and revokes the certificates from requests sent by the Registration Authority. The CA is used for the implementation of certificate generation, certificate revocation, logging and audit services.

The PMA can delegate a part of the services.

It delegates to the Certification Operator, the generation and revocation of certificates of the Root CA and SCAs.

I.4.2 Registration Authority

The RA is used for the implementation of certificate application registration, certificate delivery, certificate revocation, logging and audit services.

The RA is comprised of representatives of the PMA, which guarantee the naming of the Root CA and SCAs during key ceremonies.

I.4.3 Certificate holders

A "Certificate Holder" is defined as any entity that holds a key pair and the associated certificate issued by the CA. The holder may be a natural person or legal entity, computer equipment or an application. When the holder is not a natural person, it is

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

represented by the person who is responsible for it. This person must hold a certificate issued by the CA in order to apply for the certificate for the entity for which he is responsible.

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 the security policy of Groupe Imprimerie Nationale, in order to validate the security functions implemented using authentication, signature or encryption certificates. The certificate user must hold his own certificate. A holder who receives a certificate from another holder becomes a user certificate. Under this CP, the certificate user must validate the CA certificates and check the ARL.

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.

The CSO provides the technical services required for the certification process, in accordance with this CP.

The CSO is technically custodian of the private key of the Root CA used to sign SCA certificates. His responsibility is limited to compliance with the procedures defined by the CA to meet the requirements of this CP.

I.4.5.2 Certification Agent

Not applicable.

I.4.5.3 Publication service

The PS is used for the implementation of the publication service (see § II).

The PS shall act in accordance with the CP.

I.4.5.4 Customer entity

Not applicable.

I.5 USE OF CERTIFICATES

I.5.1 Applicable fields of use

I.5.1.1 Holders' key pairs and certificates

Not applicable.

I.5.1.2 CA and components' key pairs and certificates

The key pair of the Root CA is used to sign the certificate of the Root CA, SCAs and ARLs. The electronic certificate of the Root CA identifies the certification chain of IN Groupe used under its own applications or for customers who agree to recognise it as a certification authority.

The online SCA keys are used to sign holders' certificates and the Certificate Revocation Lists (CRL).

The certificate chains issued from IN Groupe are formed as follows:

- Root CA certificate (CA offline): self-signed electronic certificate from the Root CA,
- SCA certificate (SCA online): electronic certificate issued to an SCA by the Root CA,

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

- Certificate holder: electronic certificate issued by an SCA online.

I.5.2 Prohibited areas of use

The use of certificates issued by the Root CA for purposes other than those provided for in this CP 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.

Certificates may only be used in accordance with the laws in force and applicable, in particular only to the extent permitted by import and export laws.

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 de 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 point of contact.

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 not authorise 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 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 holder certificate families,
- Update the list of applications concerned by the CP,
- Adapt to technological developments.

II Responsibilities for the provision of information to be published

II.1 ENTITIES RESPONSIBLE FOR PROVIDING THE INFORMATION

The publication service is responsible for publishing the data identified in & II.2.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

II.2 INFORMATION TO BE PUBLISHED

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

Information	Publication address
This CP	http://www.imprimerienationale.fr/GIN/CP
Valid certificates from the Imprimerie Nationale Root CA and SCAs	http://www.imprimerienationale.fr/GIN/CA
Authority Revocation List (ARL)	http://www.imprimerienationale.fr/GIN/CRL/ACR.crl http://crl.imprimerienationale.fr/GIN/ACR.crl

Unless otherwise indicated, all other information is considered confidential.

II.3 TIME LIMITS AND FREQUENCY OF PUBLICATION

Any new CP is published on the IN Groupe site in 24 working hours after its update. It is accessible on the site 24/7.

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

CA certificates (Root CA or SCA) and information allowing certificate users to ascertain the origin of the Root CA's certificate must be circulated prior to any circulation of bearer certificates and/or corresponding ARL/CRLs. The publication systems are available 24/7.

II.4 ACCESS CONTROL TO PUBLISHED INFORMATION

All information published for certificate users is freely accessible for reading and protected against unauthorised changes.

III Identification and authentication

III.1 NAMING

III.1.1 Type of names

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

In each X.509 certificate, the supplier (Issuer) and the holder (subject) are identified by a DN (Distinguished Name).

III.1.2 Need to use explicit names

III.1.2.1 Identity of the Root CA

The DN of the *issuer* field of the certificate of the Imprimerie Nationale Root CA is the following:

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

DN Attributes	Attribute name	Value
CN	*commonName*	Imprimerie Nationale Root CA
OI	*organizationIdentifier*	NTRFR-410494496 (Reference base for the identity of the legal entity + Country + SIREN No.)
OU	*organizationalUnitName*	0002 410494496 (ICD + SIREN No.)
O	*organizationName*	Groupe Imprimerie Nationale
C	*countryName*	FR

Comment:
ICD "0002" corresponds to the Système Informatique pour le Répertoires des Entreprises et des Établissements (SIRENE).
The "NTR" character string identifies that the basis for company registrations is the Commercial Register.

III.1.2.2 Identity of the Subordinate CA (issuing CA)

The DN of the *subject* field of the certificates issued by the Imprimerie Nationale Root CA identifies this SCA.

DN Attributes	Attribute name	Value
CN	*commonName*	[Name of the SCA]
OI	*organizationIdentifier*	NTRFR-410494496 (Reference base for the identity of the legal entity + Country + SIREN No.)
OU	*organizationalUnitName*	0002 410494496 (ICD + SIREN No.)
O	*organizationName*	Groupe Imprimerie Nationale
C	*countryName*	FR

Comment:
ICD "0002" corresponds to the Système Informatique pour le Répertoires des Entreprises et des Établissements (SIRENE).
The "NTR" character string identifies that the basis for company registrations is the Commercial Register.

III.1.3 Pseudonymisation of holders

Regarding the Root CA and the SCAs, the notions of pseudonymisation are not applicable.

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

CUs (applications, networks, machines, external organisations, etc.) and holders can use CA certificates contained in the authorised certification chains (see § above), to implement and validate security functions by verifying among others the identities (DN) of the CAs as contained in the CA certificates.

III.1.5 Uniqueness of names

The identities held by the Root CA and the SCAs in the certificates are unique within CA's certification domain.
The CA ensures this uniqueness through its registration process.
In the event of a dispute over the use of a name for a certificate, the CA is responsible for resolving the dispute.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

III.1.6 Identification, authentication and role of trademarks

The CA cannot be held liable for any unlawful use by the user community 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 proof of the CA's possession of the private key is carried out by the procedures for generating (see § VI.1.2) the private key corresponding to the public key to be certified and the mode of transmission of the public key (see §).

III.2.2 Validation of the identity of an organisation

The identity of the organisation is validated by IN Groupe, which communicates the identification data to include in the identity of the CA (Root CA or SCA) (see § III.1.1) to the CSO before the key ceremony.

III.2.3 Validation of the identity of an individual

This point is not applicable in this CP.

III.2.4 Unverified holder information

The certificates do not contain unverified information.

III.2.5 Validation of the applicant's authority

CA certificates are issued in the name of IN Groupe.

III.2.6 Interoperability criteria

This point is not applicable in this CP.

III.3 IDENTIFICATION AND VALIDATION OF A KEY RENEWAL REQUEST

Renewal of a CA's key pair (Root CA or SCA) automatically results in the generation and delivery of a new CA certificate.

III.3.1 Identification and validation for a current renewal

Checks relating to the renewal of a key pair are carried out in accordance with the initial procedures (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 corresponding key public certificate are carried out in accordance with the initial procedures (see III.2 above).

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

III.4 IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST

Requests for revocation of a CA (Root CA or SCA) give rise to an authentication of the applicant which must be authorised to request the revocation from the CA.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

IV Operational requirements for the certificate life cycle

IV.1 CERTIFICATE REQUEST

IV.1.1 Origin of a certificate request

IN Groupe is responsible for the creation of the Root CA offline and SCA online.

IV.1.2 Process and responsibilities for preparing a certificate application

A Root CA or SCA online creation request contains the identifier of the Root CA offline which must sign its certificate.

IV.2 PROCESSING A CERTIFICATE REQUEST

IV.2.1 Execution of the request identification and validation processes

IN Groupe identifies and authenticates the request to create the Root CA and SCA online.

IV.2.2 Acceptance or rejection of the request

IN Groupe accepts or rejects the request to create an online SCA. In the event of acceptance, a key ceremony is then organised.

IV.2.3 Duration of certificate preparation

The processing time for an application for a certificate by the PMA shall be a maximum of 30 days from the date of acceptance of the application by the PMA.

IV.3 ISSUE OF THE CERTIFICATE

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

The Root CA and SCAs “online” are generated during a key ceremony (see VI.1).

Prior to the key ceremony, IN Groupe verifies the content of the CA naming documents, in terms of completeness and accuracy of the information present. This document is used as the basis for the key ceremony for the creation of the Root CA and SCAs.

The Root CA and SCAs certificates are signed by the Root CA during the key ceremony (see VI.1).

IN Groupe checks at the end of the CA key ceremony that the produced CA certificates comply with the naming documents.

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

Notification is made at the end of the CA key ceremony by handing over the CA certificate to a representative of the PMA present at the key ceremony.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

IV.4 ACCEPTANCE OF THE CERTIFICATE

IV.4.1 Procedure for accepting the certificate

The CA checks that the certificate contains the information described in the naming document signed by IN Groupe. As soon as the CA confirms that the certificate matches the naming document, the CA accepts the CA certificate issued.

IV.4.2 Publication of the certificate

CA certificates are published by the publication service.

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

This point is not applicable in this CP.

IV.5 USE OF THE KEY PAIR AND CERTIFICATE

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

Use of the key pairs and certificates are defined in § I.5 above. Use of a key pair and the associated certificate is also indicated in the certificate itself, via the extensions concerning the use of key pairs (see § VI.1.7 below).

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

CA certificates can only be used by a CU for the purpose of validating a chain of trust.

It is the sole responsibility of the CU to ensure the validity of certificates issued by the Root CA or the SCA using the lists of revoked authority certificates published by the SP.

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 of the Root CA or SCA).

Under this CP, there can be no certificate renewal without renewal of the corresponding key pair. This operation is therefore not authorised by this CP.

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

IV.7.1 Possible causes for changing a key pair

The key pairs must be periodically renewed:

- according to the recommendations issued by the ANSSI in terms of cryptanalysis, in order to minimise the possibilities of cryptographic attacks,
- so that the Root CA can continue to issue SCA certificates of constant duration,
- in the event of compromise, suspected compromise, theft, malfunction or loss of the means of reconstruction of the private key of one of the CAs.

The change of key pair results in the change of certificate, the procedure to be followed is identical to the initial certification procedure described in § III.2, § IV.1, § IV.3 and § IV.4 above.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

IV.7.2 Origin of a new certificate request

The request for a new certificate may be made at the initiative of the PMA.

IV.7.3 Procedure for processing a new certificate request

Processing of a request for a new certificate shall be carried out under the same conditions and in accordance with the same procedures as the initial request. (see § above).

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

For any renewal: the Root CA notifies the Subordinate CA, under the conditions of section.

IV.7.5 Procedure for accepting the new certificate

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

IV.7.6 Publication of the new certificate

See section.

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

See section.

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.

IV.9 REVOCATION AND SUSPENSION OF CERTIFICATES

IV.9.1 Possible causes for revocation

IV.9.1.1 Revocation of the Root CA

The reasons for revoking a Root CA certificate are as follows:

- cessation of business of the Root CA,
- compromise, suspicion of compromise, theft, loss of means of reconstituting the private key of the Root CA (loss of the main secret, loss of the activation code and loss of more than two shared secrets),
- non-compliance by the Root CA of the CP,
- change of information in the certificate,
- obsolescence of cryptography with regard to ANSSI requirements.

IV.9.1.2 Revocation of an SCA

The causes for revocation of an SCA certificate are as follows:

- cessation of SCA's activity,
- compromise, suspicion of compromise, theft, loss of the means to reconstitute the SCA private key (loss of

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

the main secret, loss of the activation code and loss of more than two shared secrets),
- SCA's non-compliance with the CP,
- change of information in the certificate,
- obsolescence of cryptography with regard to ANSSI requirements.

IV.9.2 Origin of a revocation request

The revocation of a CA certificate (Root CA or SCA) can only be requested by the entity responsible for the CA in question, i.e. IN Groupe, or by the judicial authorities via a court decision.

IV.9.3 Procedure for processing a revocation request

When the decision is taken to revoke one of the operational CAs belonging to the chain of trust of a Certificate Holder (SCA or Root CA), the following actions are performed:
- All valid holder certificates issued by this CA are revoked and included in the CRL,
- The persons responsible for the user applications and the holders are notified,
- A revocation request for the CA certificate is forwarded to the Root CA to which the CA is subordinate.

When the decision is made to revoke one of the CA's certificates and the reason for revocation is the compromise (actual or suspected) of the corresponding private key, the following actions are performed:
- All valid holder certificates issued since the date of compromise (with a security period) by this CA are revoked and included in the CRL,
- The persons responsible for the user applications and the holders are notified,
- A revocation request for the CA certificate is forwarded to the Root CA to which the CA is subordinate.

If necessary, the issuance of "replacement" certificates for the Holders will be provided as soon as possible.

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

The PMA must immediately request the revocation of one of the CA certificates as soon as a cause for revocation as defined in § IV.9.1 is identified.

IV.9.5 Timeframe for the processing by the CA of a revocation request

The CA shall process revocation requests as soon as possible after receipt, preferably immediately, and within less than 24 hours.

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/CRL, dCRL, OCSP, etc.) is at the discretion of the user according to their availability and the constraints related to its application.

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

ARLs are issued every year. In the event of revocation of the CA, the ARL is published when it is generated.

IV.9.8 Maximum time limit for publication of an ARL

After being generated, the ARL is published within a maximum period of 24 hours.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

IV.9.9 Availability of an online system for checking the revocation and status of certificates

See § IV.9.6.

IV.9.10 Requirements for online 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

Not applicable.

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 ARLs. These ARLs are in V2 format, published in http at the addresses listed in § II.2.

IV.10.2 Certificate status information function availability

The certificate status information service is available 24/7. This service guarantees a maximum downtime by service interruption (failure or maintenance) of 4 hours and a maximum total downtime of 16 hours per month.

IV.10.3 Optional mechanisms

This point is not applicable in this CP.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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 Root CA and the SCA prior to the end of the validity of its certificate, for one reason or another, the certificate of the CA is revoked.

IV.12 KEY ESCROW AND RECOVERY

This point is not applicable in this CP.

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

Key ceremonies are held on the CSO site.

The CSO's operating site complies with the regulations and standards in force and its installation takes into account the results of the risk analysis, the CSO's business, for example certain specific requirements such as flooding, explosion (proximity of a factory area or chemical product warehouses, etc.) carried out by the CSO.

The operating site of the CSO of the Root CA is geographically located in mainland France.

The Registration Authority (RA) operates on the site of IN Groupe.

The facility is redundant and installed in two separate hosting rooms.

The construction of the site complies with the regulations and standards in force. Its installation takes into account the results of the risk analysis and the operator's business according to the EBIOS method.

Within this framework, specific risks such as flooding, explosion and terrorist attack have been specifically studied.

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 enhanced 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.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

Note - Machines are defined as all servers, cryptographic boxes, stations and active network elements used for the implementation of these functions.

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.

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 media (paper, hard disk, USB keys, CDs, etc.) containing this information are managed in accordance with the defined security needs.

V.1.7 Decommissioning of media

Information media are destroyed at the end of their life.

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.

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. People 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, fault, attempted compromise, etc.
- **Application Manager** - The Application Manager is responsible for the implementation of the PKI CP at the level of the

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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 PKI 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 fulfil the 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.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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

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 (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 section § 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.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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,
- Logging events: starting and stopping the logging function, changing logging settings, actions taken following the failure of the logging function,
- Logging in/out of users with trusted roles, and corresponding unsuccessful attempts,

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.).

In addition to these logging requirements common to all components and functions of the PKI, events specific to individual KM functions are also logged:

- Receipt of a certificate request (initial and renewal),
- Validation/rejection of a certificate request,
- Events related to signature keys and CA certificates (generation, backup/recovery, destruction, etc.),
- Generation of holder certificates,
- Publication and update of CA-related information,
- Receipt of a revocation request,
- Validation/rejection of a revocation request,
- Generation and publication of ARLs.

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).

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

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).

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 (see § 0).

V.4.3 Event log retention period

Event logs are kept on site for at least 5 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).

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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).

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.

In addition, a reconciliation between the different event logs of functions that interact with each other (Registration Authority and generation function, revocation management function and certificate status information function, etc.) is carried out at least once a month, in order to check the concordance between dependent events and thus help detect any anomalies.

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 and ARLs,
- Registers and key ceremony scripts,
- Event logs of the different components of the PKI.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

V.5.2 Archive retention period

Root CA and SCA certificates

The retention period for these certificates, as well as the ARLs produced, is 5 years after their expiry.

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 retention, 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

Paper or electronic records must be retrievable by the Root CA within 48 working hours.

V.6 CA KEY CHANGE

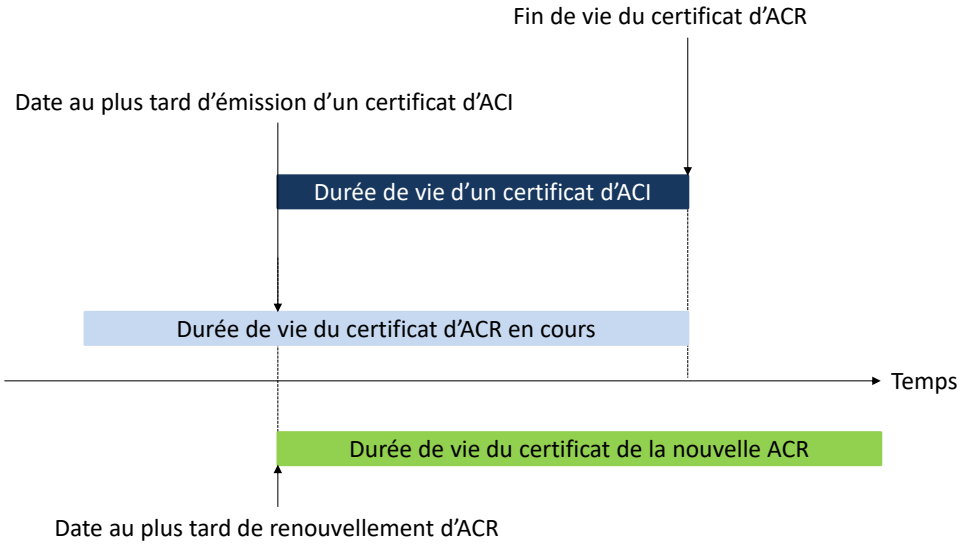
The life span of the CA certificate is determined according to the validity period of the associated private key, in accordance with the security cryptographic recommendations for key lengths, including the recommendations of the relevant national or international authorities.

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 Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.



In addition, the Root 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 private key of the Root CA or an SCA, 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 information on the revocation of the certificate, if necessary, is published 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.

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 section § IV.9. In addition, the CA meets the following commitments:

- Inform without delay the following entities of the compromise: all holders, the entities with which the CA has entered

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

into agreements and third-party users.
- Indicate without delay that certificates and revocation status information issued using this CA key may no longer be valid.
- 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 section § 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 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 Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

VI Technical security measures

VI.1 GENERATION AND INSTALLATION OF KEY PAIRS

VI.1.1 Key pair generation

VI.1.1.1 Root CA Keys

The generation of the key pairs associated with the CA certificate (Root CA or SCA) takes place during a key ceremony using a hardware cryptographic resource qualified at enhanced level.

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

Not applicable.

VI.1.1.3 Subordinate CA keys generated by the Subordinate CA

See VI.1.1.1.

VI.1.2 Transmission of the private key to its owner

The CA private key remains and is implemented on the premises of the Certification Operator.

VI.1.3 Transmission of the public key to the CA

CA public keys are generated during key ceremonies and signed by the Root 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 public key of the Root CA is distributed in a self-signed certificate. As this means of transmission does not make it possible to guarantee their origin, the distribution of the self-signed certificate is accompanied by the digital fingerprint of the certificate and a declaration of ownership of the public key.

This information can be found on the site of Groupe Imprimerie Nationale.

The Imprimerie Nationale Root CA certificate is available at the URLs listed in section II.2 of this CP.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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 Root CA Keys

Imprimerie Nationale Root CA
The key pair is of type RSA 4,096 bits
The hash algorithm is SHA-512 of which the OID is 1.2.840.113549.1.1.13.

VI.1.5.2 Subordinate CA Keys

The key pair is of type RSA 4,096 bits
The hash algorithm is SHA-384

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

The equipment used for the generation of the CA 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 Root CA's private key and associated certificate is strictly limited to signing certificates and ARLs.
The use of the SCA's private key and associated certificate is strictly limited to signing certificates, CRL and OCSP responses.

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

VI.2.1 Standards and security measures for cryptographic modules

The CAs cryptographic resources are qualified at enhanced level by the ANSSI.

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 section § VI.1.1, the activation of the private key in section § VI.2.8 and its destruction in section § VI.2.10.
The checking of private CA signature keys is carried out by trusted personnel (PKI 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

CA key pairs (Root CA and SCA) are stored under the control of several people for availability purposes. Backups of private keys are made using hardware cryptographic resources. Backups are transferred to a secure off-site backup site to provide and

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

maintain the CA's disaster recovery capability. CA private key backups are stored in hardware cryptographic resources or in encrypted form.

VI.2.5 Archiving the private key

CA private keys are never archived.

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

VI.2.6.1 Root 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 AES (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 Subordinate CA private keys

Not applicable.

VI.2.7 Storage of the private key in a 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 Root CA private keys

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

VI.2.8.2 Subordinate CA private keys

Not applicable.

VI.2.9 Method for disabling the private key

VI.2.9.1 Root 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 online only to sign holder certificates and CRLs after authenticating the certificate request and revocation request.

VI.2.9.2 Subordinate CA private keys

Not applicable.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

VI.2.10 Method of destroying private keys

VI.2.10.1 Root 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.

VI.2.10.2 Subordinate CA private keys

Not applicable.

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

The cryptographic modules used by the Root CA and the SCAs are certified at level EAL4+ according to common criteria.

VI.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

VI.3.1 Public key archiving

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

VI.3.2 Life span of key pairs and certificates

As a CA cannot issue bearer certificates with a lifetime longer than that of its own certificate, the key pair and the certificate to which it corresponds are renewed at the latest on the expiry date of the CA certificate minus the life span of the issued bearer certificates.

The certificates of the Holders covered by this CP have a maximum validity period of 10 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 Root CA private key

The activation data of the CA private keys are generated during key ceremonies (refer to § VI.1.1). The activation data are generated automatically according to a type M (3) of N (5) scheme. In all cases, the activation data are 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 Subordinate CA's private key

Not applicable.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

VI.4.2 Protection of activation data

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

Activation data are 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 Subordinate CA's private key

Not applicable.

VI.4.3 Other aspects related to activation data

Activation data are 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:

- Authentication of trusted roles;
- Discretionary access control;
- Prohibition of the reuse of objects;
- Requires the use of cryptography for communications;
- Requires the identification of users;
- Ensures the rigorous separation of tasks;
- Provides self-protection of the operating system.

VI.5.2 IT system qualification level

When a Root CA 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 SECURITY 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 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;
- The hardware and software are dedicated to PKI activities. There are no other applications, hardware, network

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

connections, or software components installed that are not dedicated to PKI's activities;
- It is necessary to take care not to download malware on PKI equipment. Only applications required to perform PKI 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.

VI.7 NETWORK SECURITY MEASURES

The "offline" components of the Root CA are never connected to a network. Therefore, this point is not applicable for this CP.

The network security measures concerning SCAs will be treated in the CPs of these SCAs.

VI.8 TIME-STAMPING/DATING SYSTEM

There is no time-stamp used for the Root CA but an event dating system that allows, from a date provided by the operating system of the Root CA to sequence the events.

Automatic or manual procedures are used to maintain the time of the system. Clock settings are auditable events.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

VII Certificate, OCSP and CRL profiles

VII.1 CERTIFICATE PROFILES

The certificates issued by the CA are X.509 v3 format certificates (populate version field with integer "2"). The fields for CA certificates and holder certificates are defined by RFC 5280.

VII.1.1 Root CA certificate profiles

The main fields of Imprimerie Nationale Root CA certificates are as follows:

Basic fields	Value
Version	2 (=version 3)
Serial Number	Defined by tool
Issuer DN	CN = Imprimerie Nationale Root CA OI = NTRFR-410494496 OU = 0002 410494496 O = Groupe Imprimerie Nationale C = FR
Subject DN	CN = Imprimerie Nationale Root CA OI = NTRFR-410494496 OU = 0002 410494496 O = Groupe Imprimerie Nationale C = FR
PublicKeyAlgorithm	Sha512WithRSAEncryption
Key size	4,096 bits
Life cycle	25 years

as well as the following extensions:

Extensions	Criticality	Value
Authority Key Identifier	N	Identifier of the Imprimerie Nationale Root CA public key
Basic Constraints	O	Basic Constraints: SubjectType=CertAuthority PathLengthConstraint=1
Certificate Policies	N	Certificate strategies: All issuing strategies http://www.imprimerienationale.fr/GIN/CP
Key Usage	O	Certificate signature

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

		Signing of the revocation list offline Signing of the revocation list
Subject Key Identifier	N	Identifier of the Imprimerie Nationale Root CA public key

VII.1.2 Profiles of the certificates of the Subordinate CAs

The main fields of the certificate of an SCA (issued by Imprimerie Nationale Root CA) are as follows:

Basic fields	Value
Version	2 (=version 3)
Serial Number	Defined by tool
Issuer DN	CN = Imprimerie Nationale Root CA OI = NTRFR-410494496 OU = 0002 410494496 O = Groupe Imprimerie Nationale C = FR
Subject DN	CN = [Name of the CA] *(Optional)* OI = NTRFR-410494496 OU = 0002 410494496 O = Groupe Imprimerie Nationale C = FR
PublicKeyAlgorithm	Sha384WithRSAEncryption
Key size	4,096 bits
Life cycle	10 years

as well as the following extensions:

Extensions	Criticality	Value
Authority Key Identifier	N	Identifier of the Imprimerie Nationale 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/CP
CRL Distribution Points	N	ARL distribution point: URL=http://www.imprimerienationale.fr/GIN/CRL/ACR.crl URL=http://crl.imprimerienationale.fr/GIN/ACR.crl

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

Key Usage	O	Certificate signature Signing of the revocation list offline Signing of the revocation list
Subject Key Identifier	N	Identifier of the public key of the CA Imprimerie Nationale Substantiel Personnel

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 identifier (OID) of the CP

CA certificates (Root CA or SCA) do not contain the OID of this CP (see & I.2).

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 ARL PROFILES

The ARL characteristics are:

ARL characteristics	Period of validity: 13 months. Update frequency: Once a year (every 12 months) ARL version (v1 or v2): v2 Extensions: ARL and AKI number Publication URL http: See § II.2

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

Basic field	Value
Version	2
Signature	Identifier of the signature algorithm of CA Imprimerie Nationale Substantiel Personnel SHA-256 RSA 2048
Issuer DN	CN = Imprimerie Nationale Root CA OI = NTRFR-410494496 OU = 0002 410494496 O = Groupe Imprimerie Nationale C = FR
This Update	ARL generation date
Next Update	Next update of the ARL
Revoked certificates	List of serial numbers of revoked Holders' certificates

Plus the following extensions:

Extensions	Criticality	Description
Authority Key Identifier	N	Identifier of the public key of the CA Imprimerie Nationale Substantiel Personnel
CRL Number	N	ARL serial number

VII.3 OCSP PROFILE

This point is not applicable in this CP.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

VIII Compliance audit and other evaluations

Audits and evaluations are those that the PMA is required to perform, or have performed, to ensure that its entire PKI is in compliance with its commitments and practices as set out in this CP.

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 RGS 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 RGS qualification and an eIDAS qualification within the meaning of the SCAs.

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 defined in the CP of the Root CA as well as the resulting elements (operational procedures, resources implemented, etc.).

VIII.5 Actions undertaken 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.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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 an overall offering of IN Groupe services integrating a set of services including the issue and management of digital certificates. 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.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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 Root CA and its components,
- the private keys of the SCAs,
- the activation data associated with the CA private keys (Root CA or SCA),
- all the secrets of the PKI,
- the event logs of the different components of the PKI,
- the elements relating to the key ceremony,
- the causes of revocations, unless explicitly agreed by the Root CA,
- audit reports.

Only authorised persons may access it.

IX.3.2 Information outside the scope of confidential information

Information concerning the PKI published by the PS 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 section § 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.

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).

IX.4.2 Personal data

The CA considers that the following information is personal data:

- Identity of holders of secrets;
- Certificate request (completed);
- Revocation request (completed);
- Reason for revocation.

IX.4.3 Non-personal data

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

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

IX.4.4 Liability in terms of personal data protection

See IX.4

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.

IX.4.7 Other circumstances for disclosing personal data

Not applicable

IX.5 INTELLECTUAL PROPERTY RIGHTS

This CP covers compliance with 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:

- protect and guarantee the integrity and confidentiality of their secret and/or private keys,
- 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,
- respect and apply the part of the CP for which they are responsible (this part must be communicated to the corresponding component),
- submit to compliance checks carried out by the audit team mandated by the PMA and the qualification body,
- respect the agreements or contracts that bind them,
- document their internal operating procedures,
- implement the resources (technical, organisational and human) necessary to perform the services to which they commit themselves under conditions guaranteeing quality and safety,
- implement awareness-raising and training actions,
- set up documentation of the responsibility of each of the parties involved.

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 SCA;
- Ensure and maintain the consistency of its CP;
- Take all reasonable measures to ensure that its holders are aware of their rights and use with respect to the use and

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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,
- Possibility to carry out audits
- Raise awareness among the various parties involved.

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

Not applicable.

IX.6.3 Certificate holders

The holders of SCA certificates are not affected by this CP.

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 Root CA 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

IX.6.5.1 Operator of certification services

It is the duty of the certification services operator to implement and operate the PKI in accordance with the requirements set out in the CP.
- certificate users expressed in this CP.

IX.7 LIMIT OF GUARANTEE

The CA guarantees through its PKI services:
- The identification and authentication of the Root CA with its certificate;
- The identification and authentication of SCAs with the CA certificates generated by the Root CA;
- Management of the corresponding certificates and certificate validity information according to this CP.

These guarantees are exclusive of any other CA guarantee.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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:

- 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.6.5);
- 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 Root CA guarantees that it complies with this CP as well as with current and stable industry standards.

The Root 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 Root CA's fault must be duly proven;
- in the event of proven compromise, entirely and directly attributable to the Root CA.

The Root CA cannot be held liable 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.

The Root 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 Root 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 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 Root 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 Root CA is established and has directly caused damage, IN Groupe will compensate the relevant person/entity within the limit defined in the service contract.

IX.10 DURATION AND EARLY END OF 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 Root CA CP shall remain in force at least until the end of the life of the last certificate issued under this CP.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

IX.10.2 Early end of validity

The publication of a new version of this CP may result, depending on the changes requested, in the need for the PMA to upgrade the CP it implements.

Depending on the nature and importance of the changes made to this CP, the deadline for compliance will be decided by the PMA.

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 must 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.

IX.12 AMENDMENTS TO THE CP

IX.12.1 Amendment procedures

The PMA reviews its CP whenever there are changes in PKI systems and each time a remarkable change in industry standards justifies it.

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.

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.

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 users can clearly distinguish which certificates correspond to which requirements.

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.

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

IX.14 COMPETENT JURISDICTION

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 IN Groupe's registered office.

IX.15 COMPLIANCE WITH LAWS AND REGULATIONS

This CP is subject to national, local and foreign laws, rules, regulations, ordinances, decrees and orders of state concerning KIs, but not limited to PKIs, restrictions on the import and export of cryptographic software or hardware or technical information.

The laws and regulations applicable to the CP are, in particular, those indicated in section § 0 above.

IX.16 MISCELLANEOUS PROVISIONS

IX.16.1 Overall 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 such, 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 pursuant to Article 1148 of the French Civil Code.

IX.17 OTHER PROVISIONS

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

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

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);
http://www.cil.cnrs.fr/CIL/spip.php?rubrique281

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[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")

Ordinance No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between administrative authorities.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig

Article 801-1 of the French criminal procedure code

Article 1316 et seq. of the French Civil Code on electronic signatures

Decree no. 2010-112 of 2 February 2010 implementing Articles 9, 10 and 12 of Ordinance no. 2005-1516
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=vig

Decree No. 2001-272 of 30 March 2001 implementing Article 1316-4 of the 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)

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

- 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)

Decree No. 2006-212 of 23 February 2006 on the security of activities of vital importance
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000634536&dateTexte=&categorieLien=id
Decree No. 2012-491 of 16 April 2012 on access to points of vital importance
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025703623&dateTexte=&categorieLien=id
Decree No. 2011-1425 of 2 November 2011 implementing article 413-7 of the French Criminal Code and relating to the protection of the nation's scientific and technological potential
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024749915&dateTexte=&categorieLien=id

Law No. 2011-267 of 14 March 2011 on guidance and programming for internal security performance
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id

Article 226-4-1 of the French Criminal Code (identity theft)

Art. 226-16 et seq. of the French Criminal Code and Art. R. 625-10 et seq. of the French Criminal Code (human rights violations resulting from computer files or processing)

Council of Europe - Budapest Convention on Cybercrime of 23 November 2001

Main ongoing projects:
Draft European regulation on the protection of personal data
Draft European Directive on the protection of information systems dated 7 February 2013

X.2 TECHNICAL DOCUMENTS

[RGS]
Référentiel général de sécurité (General Security Database) – version 2.0
https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

[RGS_A_2]
"Personal Digital Certificates" type Certification Policy - Version 3.0

IN Groupe: French Limited Company (SA) with share capital of €34,500,000 Head office: 104, avenue du Président Kennedy, 75016 Paris
This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

[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: Cryptographic module security requirements of the Root CA

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.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.

XII Appendix 3: Cryptographic module security requirements of the Subordinate CA

XII.1 REQUIREMENTS FOR SAFETY OBJECTIVES

See XI.1.

XII.2 QUALIFICATION REQUIREMENTS

See XI.2.

This document is the property of IN Groupe. Any reproduction is subject to prior authorisation and compliance with the provisions of the French Intellectual Property Code.