CONSEIL SUPÉRIEUR
DU NOTARIAT

CP for management of certificates issued by the REALTS CA – Format RFC 3647

Certification Policy
Technical Certificates issued by the REALTS certificate authority

REALTS CP

Status of the document: Standard
Version: 1.6
Date of approval: 11/02/2025

RELEASED

Document history

11/02/2025

Version 1.6, Standard

- Clarifications provided on the duration of publication and availability of the latest CRLs and pre-generated OCSP tokens (paragraph 5.8.2)
- Clarifications provided on the activation date of pre-generated OCSP tokens (paragraph 5.8.2)
- Clarifications provided on the conservation of event logs in the event of cessation of activity (paragraph 5.8.1)
- Clarification provided on the duration of publication of the certificate and CRLs (paragraph 2.2)

12/03/2024

Version 1.5, Standard

- Changing the size of RSA keys
- New CSN charter
- Anonymization of the table of successive editions

18/10/2022

Version 1.4, Standard

- Modification of point of contact
- Rationalization of document approval dates
- Clarification provided on CRL/OCSP publication deadlines
- Changed archive retrieval timeout

21/01/2021

Version 1.3, Standard

- §1.1 : Correction of eIDAS audit discrepancies of january 2021. Addition of the declaration of conformity at the ETSI NCP + level
- §5.7.3 Addition of the effective recovery time of service following a compromise (14 days)

29/09/2020

Version : 1.2, Standard

- §3 – Updating certificate DN
- §3.2.3 - Addition of "The signature by the CM of the REALTS CGUs during application”
- §4.9.9 – Precision : "annual" availability rate / "service range"
- §5.2.1.3 - Replacement of "steering committee" by "monthly CSN-ADSN security monitoring committee"
- §5.2.1.3 : "is appointed by the president of ADSN"
- §6.2.1 and throughout the rest of the document : Replacement of “EAL4+” by :
  - The CA cryptographic module for signature has a "Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI.
- §6.2.2 Replacement of « process reviews” by “monthly CSN-ADSN security monitoring committee »

16/05/2019

Version : 1.1, Standard

This update is aligned on latest ETSI standards evolutions that have been published in April 2018

- 319 401 (V2.2.1): Electronic Signatures and Infrastructures (ESI) ; General Policy Requirements for Trust Service Providers.
- 319 411-1 (V1.2.2): Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service providers issuing certificates ; Part 1 : General requirements.
- 319 411-2 (V2.2.2): Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service providers issuing certificates ; Part2 : Requirements for trust service providers issuing EU qualified certificates.

GDPR requirements have been better taken in account
Change REAL.NOT in ADSN

11/08/2017

Version: 0.1, Standard
Creation of the document
New CA chain with implementation of the REALTS CA from Notaries of France

Contents

PUBLIC

PUBLIC

1. Introduction

1.1. General overview

The Conseil Supérieur du Notariat has established itself as the electronic certification service provider for the Notaries of France, offering signature support services enabling Notaries to develop paperless authenticated deeds and, more generally, to secure all of their communications.

To this end, a certification structure has been established, which is shown in paragraph 2.3. This certification policy defines the requirements relating to the REALTS CA for the “Timestamp Certificate” profile in accordance with the profile described in [A12] for installation on the timestamp units of the Notariat’s timestamping service. The certificates issued are then used to sign requests for time stamp tokens made by the Notariat’s applications.

This Certificate Authority satisfies the requirements of standards EN 319401 [A8], EN 319411 [A9] and [A10] and EN 319412 [A11] and [A12].

Its structure conforms to RFC 3647, [A1]. The coverage of the CA’s requirements within the framework of the Certification Policy makes it possible to comply with the eIDAS regulation [A12].

This CP complies with the requirements defined by the ETSI NCP + level policy (0.0.2042.1.2).

1.2. Identification of the document

The OID number of this document is 1.2.250.1.78.2.1.3.5.1.1.

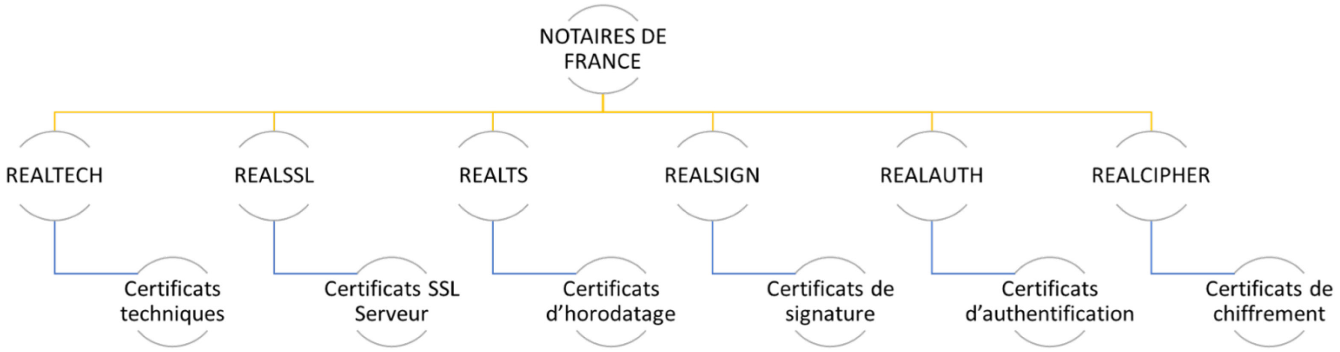
1.3. Entities involved in the KMI

The REALTS CA issues technical certificates (class 0) used to:

- Sign the requests for certificates of the timestamp units of the Notariat’s timestamping service;
- Sign the OCSP (Online Certificate Status Protocol) responses;

The first profile is that addressed in the CP. It is a certificate profile containing the necessary extensions for timestamping.

The following Certificate Authority structure is used:



The electronic certification service provider (ECSP) is the Conseil Supérieur du Notariat. The CSN is also the certificate authority (CA), the body entrusted by users of the certification services to create and issue certificates.

The CSN relies on ADSN as the Certification Service Operator (CSO), to operate the certificate management functions.

1.3.1. Certificate Authorities

The Certificate Authority is the CSN. It is responsible for implementing this Certification Policy.

The CA is responsible for the certificates signed on its behalf and for the Public Key Management Infrastructure (KMI) it has established.

In particular, the CA is responsible for the following functions:

- Implementation of the Certification Policy;
- Management of the certificate managers;
- Management of the certificates;
- Publication of the Certificate Revocation List (CRL) and the Authority Revocation List (ARL);
- Logging and archiving of events and information relating to the functioning of the KMI.

The CA completes these tasks by delegating to ADSN the management of the timestamp unit certificates and the operational maintenance of the technical infrastructures.
The CA retains responsibility under all circumstances.

1.3.2. Certification Service Operator

The Certification Service Operator is ADSN. It is responsible for the following functions:

- Records/Registers
- Certificate generation
- Handover to the certificate manager
- Publication
- Revocation management
- Notification of certificate status

The task of generating secret elements of the timestamp unit due to receive the certificate is performed directly by the CSO during a key ceremony.

1.3.3. Certificate Manager (CM)

The CM is identified for the timestamp certificates. There is no CM for OCSP certificates.

The CM for the Notariat's timestamp units is an officially identified ADSN staff member.

The CM is a natural person who is responsible for the use of the certificate and the private key corresponding to the certificate on behalf of the CSN, who is identified on the certificate. The CM reports to ADSN. He/she is therefore necessarily an internal member of staff.

The CM complies with the conditions and obligations defined in this CP. It should be noted that as the certificate is associated with the timestamping service and not the CM, the CM may change during the validity of the certificate: departure of the CM from the entity, change of role and duties within the entity, etc.

Accordingly, the CSN's Timestamping Authority stipulates the following procedure for the transfer of the CM's responsibility: after appointing the new CM, the TSA calls in the two CMs, and the transfer of responsibility on the timestamp certificate is formalised in a report.

In any case, the CA will revoke the certificate if no CM is appointed by the Timestamping Authority.

1.3.4. KMI Administrator

With respect to the issuing of certificates, the KMI Administrator is responsible for the technical phases of logging and approving requests to generate and revoke certificates.

The KMI Administrator is responsible for checking that the request is compliant and that the name requested for the timestamp unit (the CN field of the certificate) is blank and conforms to the profile of the REALTS CA certificates [A4].

1.3.5. Certificate users

The users are all third parties who rely on the certificates issued by the REALTS CA.

1.3.6. Certificate holders

There are no certificate holders directly in the context of this Certification Policy. There is, however, an individual who is responsible for managing the life cycle of the certificates, namely the CM (see 1.3.3).

1.4. Use of the certificates

1.4.1. Applicable areas of use

1.4.1.1. Key pairs and certificates of the timestamping service

The class 0 certificates issued by the REALTS CA may be used for timestamp signatures for the CSN’s timestamp servers.

1.4.1.2. Key pairs and certificates of the timestamping service

The REALTS CA certificate is used to sign certificates intended for the CSN’s timestamp units.
The CA also issues OCSP response signing certificates.

The REALTS CA certificate is also used to sign the corresponding Certificate Revocation Lists.

The requirements for the key pairs and certificates of the CA and the components are defined in the CP for the NOTARIES OF FRANCE CA [R6].

1.4.2. Prohibited areas of use

Class 0 certificates may not be used for any purpose other than those defined in paragraph 1.4.1.

1.5. Management of the CP

1.5.1. Entity managing the CP

Management of the CP is the responsibility of the CSN.

1.5.2. Point of contact

Responsable de la Sécurité des Systèmes d’Information (RSSI) du Conseil supérieur du notariat
60 Boulevard de la Tour Maubourg
75007 Paris
Tel: 01 44 90 30 00

rssi.csn@notaires.fr

1.5.3. Entity determining the compliance of a CPS with this document

The CSN is responsible for internal monitoring of the compliance of the CPS with the CP.

1.5.4. Procedures for approving the compliance of the CPS

Approval of the compliance of the CPS with the Certification Policy is given by the CSN, in the light of the audits carried out.

1.6. Definitions and acronyms

1.6.1. Acronyms

CA	**C**ertificate **A**uthority
RA	**R**egistration **A**uthority
TSA	**T**ime**S**amping Authority
ANSSI	**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation (the National Cybersecurity Agency of France)
C	**C**ountry
CEN	**C**omité **E**uropéen de **N**ormalisation – The European Committee for Standardisation
CISSI	**C**ommission **I**nterministérielle pour la **S**écurité des **S**ystèmes d'**I**nformation (the Inter-ministerial Committee for the Security of Information Systems)
CN	**C**ommon **N**ame
CSN	**C**onseil **S**upérieur du **N**otariat (the High Council of French Notaries)
DN	**D**istinguished **N**ame
CPS	**C**ertification **P**ractices **S**tatement
DSA	**D**igital **S**ignature **A**lgorithm
EE	**E**nrolment **E**ntity
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
PKI	**P**ublic **K**ey **I**nfrastructure
KMI	**K**ey **M**anagement **I**nfrastructure
ARL	**A**uthority **R**evocation **L**ist
CRL	**C**ertificate **R**evocation **L**ist
O	**O**rganisation
CO	**C**ertification **O**perator
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol
OID	**O**bject **ID**entifier
CSO	**C**ertification **S**ervice **O**perator
CP	**C**ertification **P**olicy

PP	**P**rotection **P**rofile
ECSP	**E**lectronic **C**ertification **S**ervice **P**rovider
CM	**C**ertificate **M**anager
RSA	Rivest Shamir Adleman
S/MIME	**S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtensions
SHA-256/512	**S**ecure **H**ash **A**lgorithm 256/512
PS	**P**ublication **S**ervice
INFOSEC	**I**nformation **S**ystems **S**ecurity
SSL	**S**ecure **S**ockets **L**ayer
TLS	**T**ransport **L**ayer **S**ecurity
URL	**U**niform **R**esource **L**ocator
CGUs	General Conditions of Use

1.6.2. Definitions

User applications
Application services using the certificates issued by the Certification Authority for the purposes of authentication, encryption and signature of the certificate holder.

Certification Authority (CA)
Within an Electronic Certification Service Provider (ECSP), a Certification Authority is responsible, on behalf of and under the responsibility of this ECSP, for the application of at least one certification policy and is identified accordingly, as the issuer ("issuer" field of the certificate), in the certificates issued under the terms of the Certification Policy. Within the context of this CP, the term ECSP is not used outside of the present chapter, only the term CA is used.

Registration Authority
This function checks and validates the identification information of the intended holder of a certificate, as well as any other specific characteristics, before transmitting the corresponding request to the appropriate function of the KMI, in accordance with the services provided and the organisation of the KMI. The RA is also responsible, when necessary, for re-checking the holder's information when the certificate is renewed.

Authentication
Process of checking the declared identity of a person or any other entity, or of guaranteeing the origin of the data received.

Key pair
A key pair is a pairing composed of a private key (which has to be kept secret) and a public key, required for the use of cryptological techniques based on asymmetric algorithms (such as RSA or DSA).

Electronic Certificate
Document in electronic form confirming a link between a public key and the identity of its owner (a natural person or an application service). This confirmation takes the form of an electronic signature produced by an electronic certification service provider (ECSP). It is issued by a Certificate Authority. The certificate is valid for

the period specified in the same. The intended uses of the electronic certificates governed by this document are the electronic signature and the time stamp.

CA Certificate
Certificate of a Certificate Authority.

Certification of an Electronic Certification Service Provider
A document by means of which a certification body certifies the compliance of all or part of the electronic certification offer of an ECSP (family of certificates) with the requirements of the CP for a given level of security corresponding to the service covered by the certificates.

Chain of trust
Set of certificates necessary to validate the genealogy of an end certificate.
In its most basic form, the chain is composed of a Certification Authority Certificate and the end certificate.

Private key
Secret part of a key pair held by its owner. This part of the key must not be disclosed.

Public key
Public part of a key pair made available to third parties to validate the use of a certificate.

Common Name (CN)
Real identity or pseudonym of a Holder, a Server or a CA.

Component
Platform operated by an entity and composed of at least one computer station, an application and, if appropriate, a cryptology tool, and playing a specific role in the operational implementation of at least one function of the KMI. The entity can be the ECSP itself or an external entity linked to the ECSP by contract, regulation or hierarchy.

Compromise
Disclosure, modification, substitution or unauthorised use of confidential data (including cryptographic keys and other basic security parameters).

Certification Practices Statement (CPS)
A CPS identifies the practices (organisation, operational procedures, technical and human resources) that the CA applies in regard to the supply of its electronic certification services to users and in compliance with the certification policy or policies it has undertaken to observe.

Distinguished Name (DN)
Distinguished name X.500 of the Holder, Server or CA for which the certificate is issued.

Certificate generation function
This function generates (creation of the format, electronic signature with the private key of the CA) the certificates from the information transmitted by the Registration Authority and from the public key of the Holder or the Certificate Manager.

Revocation management function

This function processes requests for revocation (especially identification and authentication of the applicant) and decides the actions to be taken. The results of the requests are distributed via the information function on the status of the certificates.

Publication function
This function provides the various parties concerned with the general conditions, policies and practices published by the CA, the CA certificates and any other pertinent information intended for the holders and/or users of the certificates, other than information on the status of the certificates. It can also provide, in accordance with the policy of the CA, the valid certificates of its holders.

Handover to the manager
This function provides the Certificate Manager with the certificate, at least, and if appropriate, the other elements provided by the CA (the CM's mechanism, private key, activation codes, etc.).

Information about certificate status
This function provides certificate users with information about the status of the certificates (revoked, suspended, etc.). This function can be implemented by publishing updated information at regular intervals (CRL, ARL) or using a real-time request / response method (OCSP).

HSM (Hardware Security Module)
Cryptographic device containing the public and private keys of the Certificate Authorities.

Key Management Infrastructure (KMI)
Set of components, functions and procedures devoted to the management of cryptographic keys and their certificates used by the trust services. A KMI can be composed of a Certificate Authority, a Certification Operator, a centralised and/or local Registration Authority, certification agents, an archiving entity, a publishing entity, etc.

Authority Revocation List (ARL)
List containing the identifying details of the certificates of revoked or invalid intermediate authorities.

Certificate Revocation List (CRL)
List containing the identifying details of revoked or invalid certificates.

OID
Unique numeric identifier registered in accordance with the ISO registration standard to designate an item or a class of specific items.

Authorised person
A person other than the holder or certification agent who is authorised by the CA's Certification Policy or by contract with the CA to carry out certain actions on behalf of the holder (request for revocation, renewal, etc.). Typically, in a business or in an administration, this may be one of the holder's line managers or a human resource manager.

CRL distribution point
Internet address for publication of the Certificate Revocation List provided by the Certificate Authority.

Certification Policy (CP)
Set of rules, identified by a name (OID), defining the requirements with which a CA must comply in the setting up and provision of its services and stating the applicability of a certificate to a particular community and/or a

class of applications with common security requirements. A CP can also, if necessary, identify the obligations and requirements concerning the other stakeholders, in particular the certificate holders, managers and users.

Electronic Certification Service Provider (ECSP)
Any person or entity who is responsible for the management of electronic certificates throughout their life cycle, in regard to certificate holders and users. An ECSP can provide different families of certificates for different purposes and/or different security levels. An ECSP involves at least one CA, but can also include several depending on how it is organised. The different CAs of an ECSP can be independent from each other and/or connected by structural or other links (Root CAs / Subordinate CAs). An ECSP is identified in a certificate for which it is responsible by its CA having issued the certificate and which is itself identified in the "issuer" field of the certificate.

Security product
A software and/or hardware device used to implement the security functions necessary to make paperless information secure (during the exchange, processing and/or storage of the information). This generic term covers, in particular, electronic signing, authentication and confidentiality protection systems.

Renewal of a Certificate
Operation carried out at the request of a Certificate Holder or Manager once a Certificate is due to expire, which consists of generating a new Certificate.

Certificate Manager
The natural person responsible for the certificate, and in particular for the use of the certificate and its corresponding key pair, on behalf of the entity on which the service or server identified in the certificate depends.

Revocation of a Certificate
Operation resulting in the withdrawal of the CA’s guarantee on a given Certificate, solely prior to the end of its period of validity.
The request may result from a number of events, such as a key pair becoming compromised, a change of information contained in a certificate, etc.
The revocation operation is considered completed when the certificate to which it relates is published in the Certificate Revocation List. The certificate then becomes unusable.

Information system
Any group of resources intended to develop, process, store or transmit information exchanged electronically between administrative authorities and users, and between the administrative authorities themselves.

Certificate user
Entity or natural person that uses a certificate and relies on it to verify an electronic signature or authentication value from a certificate holder or to encrypt data intended for a certificate holder.

Certificate validation
The act of confirming the status of a Certificate or certification chain.

Signature verification
The act of checking a digital signature.

2. Responsibilities related to the provision of information to be published

2.1. Entities responsible for the provision of information

The CA is responsible for providing the Certification Policy, the Certification Practices Statement and the General Terms and Conditions of Use.

This information is accessible on the Internet, at the website https://www.preuve-electronique.org.

This service is available on a 24 hours a day and 7 days a week service range.

The provision of information about the status of certificates is the responsibility of the CSO. This information is available on the notaries' Intranet through the directory of the publication of CRLs by LDAP, and online at the website https://www.preuve-electronique.org.

This information is also available via the OCSP service used, at the following address: ocsp.preuve-electronique.org.

2.2. Information to be published

The following information is published:

- This Certification Policy and the Certification Policy of the NOTARIES OF FRANCE CA [R6]
- The Certification Practices Statement of the REALTS CA
- The document containing the certificate profiles and CRL [R5]
- The Certificate Revocation List (CRL) for the Certificate Holders and the CA, for a period of 7 years after the end of validity of the AC
- The valid certificates of the REALTS CA and the valid certificates of the NOTARIES OF FRANCE CA (the structure to which the REALTS CA reports), for a period of 7 years after the end of validity of the AC
- The information that enables users to guarantee the origin and status of the certificates of the NOTARIES OF FRANCE CA (self-signed certificates)

The CP, CPS and GTCU documents are published:

- in PDF/A format
- in French for the CPS, French and English for the CP and GTCU.

2.3. Publication times and frequencies

The certification policies are updated and published every two years.

The CA certificates are distributed, or placed online prior to every distribution of certificates, at the time of the key ceremony to enable requests for certificates for the timestamp units to be signed as early as possible.

CRLs should be published within 24 hours of the consideration of a revocation request. CRLs are published every 12 hours.

2.4. Control of access to published information

The information published is placed online on the Notarial Intranet and accessible by the whole community. The CPs, CRLs and ARLs can be read internationally by all those wishing to do so on the website https://www.preuve-electronique.org.

Additions, deletions and modifications are made by means of an automated process further to formal request by authorised individuals within the CA or the CSO. These requests are tracked.

3. Identification and authentication

3.1. Naming

3.1.1. Types of name

The names used in a certificate are described in accordance with the standard ISO/IEC 9594 (distinguished names), [A5], with each holder having a distinguished name (DN).

3.1.2. The need to use explicit names

The names to distinguish the holders are explicit. The distinguished name is in the form of an X.501 UTF8string.

The information contained in the "Subject DN" field of the certificate is described in detail below.
The distinguished name in a timestamping certificate contains:

- The name of the timestamp unit in the form CN = [Body].[Office].TU[n].[date of generation of the key pair associated with the certificate in the format yyyymmddhhmmss] where:
  - [Body] corresponds to the name of the body holding the certificate (ADSN)
  - [Office] corresponds to the name of the office responsible for the server (SDC)
  - [n] is a digital identifier of the TU
  - The unique identifier contains the date and time of the certificate generation request to the REALTS CA.
- The country in which the CA is registered ("Country" field);
- The corporate name of the body, as shown on the K-Bis ("OrganizationName") for the CA's certificate and the TU's certificate;
- The CSN's SIREN number (784350134) preceded by the ICD 0002, to complete the "OrganizationalUnit Name" field of the body for a CA certificate and a TU certificate.
- The OrganizationIdentifier (2.5.4.97) field completed as specified in clause 5 of EN 319 412-1 [A11], with the intra-community VAT number (VATFR-67784350134).

The certificates described in this Certification Policy are exclusively intended for the internal use of the CSN. Test certificates are therefore not issued for third parties. The CA does not allow for the issue of test certificates from the production environments.

3.1.3. Anonymity or use of pseudonyms for holders

The certificates that are the subject of this CP may under no circumstances be anonymous.
The names provided to establish a certificate may under no circumstances be pseudonyms.

3.1.4. Rules of interpretation of the different forms of names

The rules of interpretation are defined in document [R6].

The names used in the CN (Common Name) field of the certificates contain a unique identifier that is established manually when the certificate is generated.

This identifier is based on a number and the date and time of generation of the request.

3.1.5. Uniqueness of the names

The date of generation and an identifier guarantee the unique character of the CN of a timestamping certificate.

3.1.6. Identification, authentication and role of the trademarks

For the marks, corporate names or other distinctive signs, the CSN makes no prior rights search or other checks; It is up to the holder to check that the name requested does not violate the property rights of third parties.

3.2. Initial validation of identity

The initial validation of the identity of the CM is carried out by the process server before the start of the key ceremony. The CM formally requests authorisation from the CSN by email to generate a TU certificate. The email is attached to the process server's report.
The CM is then present during the key ceremony.

3.2.1. Method of proving possession of the private key

The REALTS CA recognises a single channel for proving possession of the private key. The keys are generated directly on the client equipment.
The proof of possession of the private key is conveyed through a certificate request file that is transmitted to the CA to generate the corresponding certificate. This transmission is performed in optimal security conditions.

3.2.2. Validation of the identity of a body

See 3.2.3

3.2.3. Validation of the identity of a CM for the REALTS CA

3.2.3.1. Registration of a CM for a certificate to be issued

Validation of the identity of a CM of a certificate issued by the REALTS CA is carried out by the process server before starting the key ceremony.
The CM must create a request file containing:

- A certificate request sent by email, under three months old, validated by the manager of the Notaries' TSA and containing the name of the timestamping unit for which the certificate is to be issued,

- A mandate, under 3 months old, designating the future CM as being authorised to be CM for the timestamping service of the notariat for which the certificate is to be issued. This mandate is signed by the manager of the CM's entity and jointly signed, for approval, by the future CM,

- A valid official ID document of the future CM containing an identity photograph (specifically an ID card, passport or residence card), which is presented at the key ceremony.

- The signature by the CM of the REALTS CGUs during application

The CSO keeps a record of the request via an email identifying the subject of the request, the information to be shown in the certificate and the CM's contact details (email address) to which the certificate is attached once issued. These elements are attached in the annex to the process server's report of the key ceremony.

3.2.3.2. Registration of a new CM for a previously issued certificate

In the event of a change of CM, ADSN will appoint a new CM under the responsibility of the TSA manager. The latter will be formally notified of this responsibility and will create a registration file containing:

- A mandate, under 3 months old, designating the future CM as being authorised to be CM for the timestamping service of the notariat for which the certificate is to be issued. This mandate is signed by the manager of the CM's entity and jointly signed, for approval, by the future CM,

- A valid official ID document of the future CM containing an identity photograph (specifically an ID card, passport or residence card), which is presented to the RA, which retains a copy,
- The CM's email address.

This file will be stored by the CA for tracking purposes.

3.2.4. Unverified information of the CM

N/A

3.2.5. Validation of the applicant's authority

The CM has a trusted role and is committed to this role. On behalf of the CSN, the CSO makes sure of the CM's legitimacy.

3.2.6. Interoperability criteria

The CA has no recognition agreement with an external CA in this area of security. The certificates it issues under the terms of this CP are for the internal use of the notariat.

If another CA makes a request for an agreement, or if the managers of the REALTS CA express the need to establish a recognition agreement with another CA, the CA's steering committee will conduct a series of investigations (audits / risk analysis) to determine whether the CA to be recognised issues certificates of the same quality, with the same level of security, as those covered by this CA.

In particular, the REALTS CA can expect that CAs requesting a certification agreement conform to the formats of certificates complying with the standard [A11], [A12].

3.3. Identification and validation of a request for renewal of keys

A new certificate may not be supplied to the CM unless the corresponding key pair is renewed.
The renewal takes the form of a new certificate request and follows the same procedures as an initial request (key ceremony).

3.3.1. Identification and validation for a standard renewal

Same as for an initial request.

3.3.2. Identification and validation for a renewal after revocation

Same as for an initial request.

3.4. Identification and validation of a request for revocation

The request for revocation of a certificate may originate from the CM or from an authorised person within the CA's organisation.
The technical aspects of all revocation requests are handled by the KMI administrator.

4. Operational requirements over the life cycle of certificates

4.1. Certificate request

4.1.1. Origin of a certificate request

Technical requests for a certificate originate from the KMI administrator via a tracked internal request from a CM identified for timestamping certificates.

4.1.2. Process and responsibilities for establishing a certificate request

The certificate request is made in the form of a certificate request in PKCS#10 format integrating the public key generated for the timestamp unit, which will be signed by the REALTS CA. This technical generation process is incorporated in a key ceremony in the presence, in particular, of the CM and under the control of a process server.

4.2. Processing a certificate request

4.2.1. 00102Identification and validation of the request

The request is made in PKCS#10 format and dealt with by the KMI Administrator during the key ceremony.
The request file is checked by the process server and the TSA manager before the technical processing of the certificate request by the KMI administrator.

4.2.2. Approval or rejection of the request

All certificate requests are approved or rejected before the request is signed by the REALTS CA.
The rejection of the request is notified to the corresponding CM. The reason for the rejection is then explained to the CM.

4.2.3. Certificate creation time

The certificate is created within a few minutes of the file being submitted to the KMI by the KMI administrator (done during a single key ceremony).

4.3. Issue of the certificate

4.3.1. Actions of the CA concerning the issue of the certificate

The transition to approved status of the request by the KMi administrator in the workflow of the KMI triggers the automatic certificate generation process.

4.3.2. Notification by the CA of the issue of the certificate to the holder

The certificate is handed over directly to the CM identified.

4.3.3. Period of validity of the certificate

The timestamping certificate is valid for three years.

4.4. Acceptance of the certificate

4.4.1. Certificate acceptance procedure

After releasing the certificate to the CM, the CSO supports the CM with the installation and validation of the certificate.
If, during these steps, the certificate does not conform to the request, it will be revoked and a new request will have to be made along the same lines as the original request.

If the certificate is deemed by the CM to be consistent with the request, the CM prepares and signs a certificate installation report. This report is attached to the key ceremony report prepared by the process server.

4.4.2. Publication of the certificate

The certificates issued by the REALTS CA are published on the website https://www.preuve-electronique.org.

4.4.3. Notification by the CA to the other entities of the issue of the certificate

The CM and the TSA manager together certify the installation of the certificate on the timestamp unit. This forms part of the key ceremony report prepared by the process server.

4.5. Use of the key pair and the certificate

4.5.1. Use of the private key and the certificate

The private key is used to sign timestamps within the context of timestamp certificates.
The certificate and the corresponding private key may only be used on the notariat's timestamp unit intended for this purpose.
These uses are specifically defined in the certificate extensions (KeyUsage field) [A4].

4.5.2. Use of the public key and the certificate by the user of the certificate

The public key and the associated timestamp certificate are used to validate the timestamp signatures issued by the timestamp unit concerned.

4.6. Renewal of a Certificate

Renewing a certificate, within the meaning of RFC 3647, [A1], i.e. purely to modify the validity dates, is not permitted.
A new certificate must be issued after changing the key pair.

4.6.1. Possible reasons for renewing a certificate

N/A

4.6.2. Origin of a renewal request

N/A

4.6.3. Procedure for processing a renewal request

N/A

4.6.4. Notification to the holder of the generation of the new certificate

N/A

4.6.5. Acceptance procedure for the new certificate

N/A

4.6.6. Publication of the new certificate

N/A

4.6.7. Notification by the CA to the other entities of the issue of the new certificate

N/A

4.7. Issue of a new certificate after changing the key pair

4.7.1. Possible reason for changing the key pair

The key pairs of timestamp certificates issued by the REALTS CA have a 1-year period of validity. A new certificate can only be issued before the previous one has expired as the result of a revocation, or of a request for renewal after one year to ensure continuity of service.

4.7.2. Origin of a new certificate request

In all cases, the procedure for requesting a new certificate is identical to the original request procedure, and a notification will be sent to the CM by email concerning the forthcoming expiry of the certificate.

4.7.3. Procedure for processing a new certificate request

Same as for the original request.

4.7.4. Notification to the holder of the generation of the new certificate

Same as for the original request.

4.7.5. Acceptance procedure for the new certificate

Same as for the original request.

4.7.6. Publication of the new certificate

Same as for the original request.

4.7.7. Notification by the CA to the other entities of the issue of the new certificate

Same as for the original request.

4.8. Amendments to the certificate

Amendments to the certificate are not permitted.

4.8.1. Possible reasons for amending a certificate

N/A

4.8.2. Origin of a certificate amendment request

N/A

4.8.3. Procedure for processing a certificate amendment request

N/A

4.8.4. Notification to the holder of the generation of the amended certificate

N/A

4.8.5. Amended certificate acceptance procedure

N/A

4.8.6. Publication of the amended certificate

N/A

4.8.7. Notification by the CA to the other entities of the issue of the amended certificate

N/A

4.9. Revocation and Suspension of certificates

4.9.1. Possible reasons for revocation

4.9.1.1. Timestamp certificates

Cases in which a certificate may be revoked are as follows:

- Compromise, suspicion of compromise, loss or theft of the private key;
- Compromise or suspicion of compromise, depreciation of an algorithm;
- Scheduled end of use of the CRC algorithm implemented;
- The CM is no longer identifiable or the KMI administrator has decided to revoke the CM's certificate;
- Termination of the CA's activity;
- Decision following a failed compliance control carried out by internal audit;
- Certificates not compliant anymore with the CP in reference
- Algorithms enforced cannot be further considered as reliable to guarantee the relationship between the subject and its public key
- Revocation of the REALTS CA.

4.9.1.2. CA Certificates

See CP of the NOTARIES OF FRANCE CA [R6]

4.9.2. Origin of a revocation request

4.9.2.1. Electronic timestamp certificates

The individuals who may request the revocation of a timestamp certificate are as follows:

- the CM;
- the President of the CSN for all certificates issued in the name of the REALTS CA.

4.9.2.2. CA Certificates

See CP of the NOTARIES OF FRANCE CA [R6]

4.9.3. Procedure for processing a revocation request

The revocation system is synchronised with UTC time to the nearest second.

4.9.3.1. Revocation of an electronic timestamp certificate

The request is sent by email by a formally identified CM to the technical operators for consideration.

4.9.3.2. CA Certificates

See CP of the NOTARIES OF FRANCE CA [R6]

4.9.4. Time granted to the CM to prepare the revocation request

The revocation request must be prepared at the earliest when the CM becomes aware of effective grounds for revocation.

4.9.5. Time for processing of a revocation request by the CA

4.9.5.1. Revocation of an electronic timestamp certificate

The request must be processed within 24 hours.

4.9.5.2. Revocation of a CA Certificate

See CP of the NOTARIES OF FRANCE CA [R6]

4.9.6. Requirements for verification of the revocation by the certificate users

The user of a certificate is required to verify the status of the certificates of the corresponding chain of trust (NOTARIES OF FRANCE CA, REALTS CA).
The REALTS CA provides users with an updated CRL, published on the website www.preuve-electronique.org and an associated OCSP service.

4.9.7. Frequency of preparation of CRLs

CRLs are drawn up at least every 12 hours or when a certificate is revoked.

4.9.8. Maximum time for publication of a CRL

A CRL must be published within 60 minutes of being generated.

4.9.9. Availability of an online verification system to check revocation and status of certificates

The revocation and verification systems have an annual availability rate of at least 99.5% and are available on a 24 hours a day and 7 days a week service range. In the event of a system failure, the CSO undertakes to restore the system within 24 hours.

If the system fails outside of working hours, the CSO's crisis unit takes action to ensure that the system is operating again within 48 hours.

These services are backed by a redundancy and disaster recovery plan that ensures their availability.

4.9.10. Requirements for the online verification of the revocation of certificates by certificate users

See 4.9.6

4.9.11. Other available resources for information about revocations

N/A

4.9.12. Special requirements in the event of the private key being compromised

As part of the revocation of a CA certificate, the CSN will publish clear evidence of the compromise of the private key on the website https://www.preuve-electronique.org. On its website, the CA will state the consequences and the precautions to be taken in this regard.

4.9.13. Possible reasons for suspension

It is not intended that certificates will be subject to suspension.

4.9.14. Origin of a suspension request

N/A

4.9.15. Procedure for processing a suspension request

N/A

4.9.16. Time limits for the suspension period of a certificate

N/A

4.10. Information regarding certificate status

4.10.1. Operational characteristics

The CRLs are in v2 format, published:

- in an LDAP v3 directory accessible within the notarial community: ldap ://annuaire.real.notaires.fr:389 and ldaps://annuaire.real.notaires.fr :636;
- on the website www.preuve-electronique.org

The CRL contains the extension “ExpiredCertsOnCRL” and stores the serial numbers of all revoked certificates, even those that have expired.

An OCSP service conforming to RFC 6277 and RFC 2560 is also available at the following address: ocsp.preuve-electronique.org (cf. 7).

The OCSP service uses the extension “archive cutoff”, as provided for by RFC 6960, with a date that is identical to the start date of the validity of the CA certificate and retains the revocation status of the certificate available once it has expired.

If the OCSP request contains a request for a serial number not issued by the REALTS CA, the OCSP server will include in the response the status “unknown” if the REALTS CA is still valid, and “unauthorized” if it has expired.
The deadline for publication of the CRL, of 60 minutes maximum, stems from the deadline for copying the CRL from the PKI to the CRLDP www.preuve-electronique.org. The OCSP service is a real-time service, but it requires an operational update of its certificate database to take into account the certificate revocation status. In case of status check of a certificate giving a different answer, the status of the certificate given by the CRL is to be preferred.

4.10.2. Availability of information

Information on the status of certificates is available on a 24 hours a day and 7 days a week service range.

4.10.3. Optional tools

N/A

4.11. End of subscription

In the context of this CP, there is, strictly speaking, no subscriber. The only certificate users are the timestamp units used in the CSN’s timestamping service. In case of the discontinuation of the activity of the CA or the timestamping services, the corresponding certificates will be revoked.

4.12. Key escrow and recovery

Keys are not held in escrow.

4.12.1. Key escrow recovery policies and practices

N/A

4.12.2. Session key encapsulation and recovery policies and practices

N/A

5. Non-technical security measures

The requirements set out in this chapter result from the risk analysis carried out on the KMI [R1] and the requirements defined in the CSN's SMSI approved by its steening committee for the CSO component.

5.1. Physical security measures

5.1.1. Geographical situation and construction of sites

The geographical location of the sites does not require special measures to be taken against such risks as earthquake, explosion, volcanic eruption or flood.

5.1.2. Physical access

Physical access to the certificate generation function, the functions of generating the secret elements of the holder, revocation management and all functions operated by the CSO, is strictly limited to those individuals authorised by name.

Physical access to components of the KMI supporting these functions is limited to authorised individuals by the creation of a physical security perimeter enabling the separation of the roles between the various collaborators.

The traceability of access is guaranteed.

Outside of working hours, intrusion detection measures are implemented.

Physical security measures are also implemented to limit access to the sensitive materials (cryptographic modules, registration file, application documents).

5.1.3. Power supply and air conditioning

Backup measures are implemented by the CSO so that an interruption of the power supply or an air conditioning failure does not threaten the availability undertakings made by the CA (revocation management and information on the status of certificates in particular).

5.1.4. Exposure to water damage

The security perimeter is designed to take into account the inherent risk of water damage. Protective measures must be implemented to protect against residual risks (e.g. burst pipes).

5.1.5. Fire prevention and protection

Fire prevention and extinction systems make it possible to fulfil the commitments made by the CA concerning availability (revocation management and information about the status of certificates in particular) and the durability of archives.

5.1.6. Safeguarding materials

The methods used to safeguard materials make it possible to fulfil the commitments made by the CA concerning the restoration and durability of archives.

5.1.7. Deactivation of materials

Materials that are deemed sensitive in terms of confidentiality are subject to destruction measures, or may be re-used in an identical operational context with the same level of sensitivity.

5.1.8. Off-site backup

To enable recovery after an incident in accordance with the commitments made by the CA, the CSO establishes off-site backups of critical information and functions. The confidentiality of information and the integrity of backed-up applications are guaranteed on both the operational website and the backup website. This concerns in particular the functions of revocation management and information about the status of certificates.

5.2. Procedural security measures

5.2.1. Trust roles

The following trust roles are defined:

5.2.1.1. CA

The Security Manager is responsible for the implementation of the CP, changes to it, and its consideration by the various parties concerned. He/she ensures that compliance controls are carried out, validates the action plans for corrective measures, etc. The Security Manager is the CSN's ISSM or his/her designated representative, under the direct supervision of the president of the CSN.

5.2.1.2. RA

The Registration Authority manager is the KMI application manager.
The technical tasks of registration and validation are the responsibility of ADSN and, more directly, the KMI Administrator.
Two roles are formalised within this context and held by the KMI Administrator:

- The registration officer is responsible for checking the information contained in the certificate request, and then approving the request

- The revocation officer is responsible for processing revocation requests

5.2.1.3. CSO

A **monthly CSN-ADSN security monitoring committee** is formed, responsible for the operational application of the CP through the implementation of the measures defined in the CPS [R3], in particular concerning the CSO. The Steering Committee conducts risk analyses on the area under its control, decides the risk management strategy, and validates and monitors the corresponding action plans. It conducts internal audits on its component and monitors the implementation of the necessary corrective measures.

The requests for timestamp certificates are validated during the key ceremony, which involves:

- The representative of the REALTS CA
- The representative of the notaries' TSA
- The Certificate Manager
- The Security Manager
- The master of ceremonies
- The KMI Administrator
- The process server

The **Security Manager** is responsible for implementing security practices. This role is filled by different individuals responsible for software security or physical security. The ISSM, responsible for the overall security of the CSO, is the president of ADSN.

The system administrator is in charge of the installation, configuration and maintenance of the KMI's trust systems.

The system operator is in charge of the day-to-day work on the KMI, in particular the backups and restorations.

The system auditor is able to access and analyse the log files of the KMI components.

The KMI Application Manager is responsible for the definition, implementation, management and monitoring of software security measures in regard to the network and the application. To achieve this, he/she relies on the system administrators.

The KMI Administrator is responsible for ADSN applications with the **System Administrator** trust role. He/she enters certificate requests on the KMI and validates them during a key ceremony. The KMI Administrator also enters certificate revocation requests under the supervision of the security manager.

Secret holders are also defined for the REALTS CA. Each possesses part of the secret required to activate the HSM holding the CA's private key.

5.2.2. Number of people required per task

Any sensitive task is carried out by at least two people. To reconstruct the CA’s secret requires 3 people to come together from among 5, each of whom hold a part of the secret.

5.2.3. Identification and authentication for each role

Identification and authentication measures are put in place to support the implementation of the access control policy and the traceability of operations; the access control policy restricts access to individuals authorised to carry out administrative operations and generate keys within the trust infrastructure.

The roles assigned are notified in writing to those concerned in the job description.

5.2.4. Roles requiring a separation of duties

Some trust roles are distinct and separate from any other trust role. An exclusion list is kept in [R3]. A single individual may only have one trust role.
An individual holding a trust role may also hold part of a secret. A secret holder may only hold one part of a secret.

5.3. Security measures concerning staff

5.3.1. Qualifications, competences and authorisations required

Any individual who occupies a role identified as sensitive is subject to a confidentiality and conflict of interest clause managed by ADSN. Furthermore, those with a trust role must declare on their honour that they have not committed any cyber-crime offence.
The CSO ensures that staff appointments to sensitive posts correspond to their professional competences. In particular, CSO staff take training courses at least once a year on IT threats and information system security practices.

Supervisory staff have the appropriate expertise and are familiar with security procedures.

All staff members with trust roles are informed of their responsibilities (job description) and the procedures related to the security of the system and staff monitoring.

5.3.2. Background checks

Background checks are made on all staff appointed to sensitive posts.

5.3.3. Initial training requirements

Staff receive training in software, equipment and internal operational procedures. This mainly concerns CSO staff working on the KMI components, but also involves training for operators in the use of the KMI.

5.3.4. Ongoing training requirements and frequency of courses

Staff must be given information and training when any change is made to the systems, procedures and organisations, where these changes impact their work.

Staff receive training in incident management and are familiar with incident reporting procedures.

5.3.5. Frequency and sequence of rotations between different assignments

N/A

5.3.6. Sanctions in case of unauthorised actions

The sanctions for unauthorised actions are set out in the internal regulations applicable to sensitive roles held by CSO and CA staff.

5.3.7. Requirements for staff of external service providers

Requirements for staff of external service providers are contract-based.

5.3.8. Documentation provided to staff

The security rules are communicated to staff when they take up their post, in accordance with the post they have been assigned to. All staff appointed to an operational role in the Key Management Infrastructure are informed of the corresponding procedures.

5.4. Data-building procedures for auditing

5.4.1. Type of event to be recorded

It is necessary to record the following events:

- system events relating to the various KMI components (start-up of servers, network access, etc.), whether on the active website or the backup website
- technical events relating to the KMI component applications, on the active website or the backup website
- functional events relating to the KMI component applications (certificate request, validation, revocation, etc.), on the active website or the backup website
- events linked to the signature keys and CA certificates (generation (key ceremony), backup / recovery, revocation, renewal, destruction, etc.)
- The transmission of the certificates to the CMs and, on a case-by-case basis, explicit acceptances / rejections by the CMs;
- The publication and updating of information related to the CA (CP, CA certificates, etc.)
- The operations carried out

These logs help guarantee the traceability and accountability of the actions taken (timestamping, assignment of the employee).

5.4.2. Frequency of processing the event logs

The event logs are used:

- On a daily basis as part of the automated control process
- Systematically in the case of an abnormal event

5.4.3. Retention period of the event logs

The retention period of the event logs is as follows:

- one month for system events
- one year for technical events
- in accordance with legal obligations for functional events

5.4.4. Protection of event logs

The event logs may only be accessed by authorised CSO staff. They may not be modified without authorisation; alerts are triggered if the logs or the parameters defining the content of the logs are modified.

5.4.5. Backup procedure for the event logs

The backup procedures for the event logs involve daily delta backups, and global backups on a weekly basis.

5.4.6. Event log collection system

The events recorded within the KMI are centralised in an SIEM.

5.4.7. Notification to the event manager of the recording of an event

N/A

5.4.8. Assessment of vulnerabilities

System and technical event logs are monitored on a permanent and daily basis to enable vulnerabilities to be anticipated and alert reports to be submitted if/when they are identified. This monitoring is conducted by automated processes for the detection of anomalies.

The monitoring of the functional event logs is carried out by request in the event of a dispute, or for a behaviour analysis of the KMI.

A monthly review of abnormal events is conducted by the CA's by means of a monthly CSN-ADSN security monitoring committee.

5.5. Data archiving

5.5.1. Types of data to be stored

The following data are to be stored:

- executable software and configuration files
- CP, CPS and GTCU
- Certificates and CRLs published
- Registration files
- Timestamp certificate generation requests
- Event logs

5.5.2. Archive retention period

The following table shows the archive retention periods for each type of data

Type of data	Retention period
Software	Version n – 1
Software configurations	Version n – 1
REALTS CA certificates	23 years
CRLs & Client certificates	23 years
OCSP requests and responses	23 years
Technical events	1 year
Functional events	23 years
Documentation	10 years
Registration file (certificate requests)	23 years
CM registration form	23 years

5.5.3. Protection of the archives

Whatever their medium, the archives are securely protected and are only accessible to authorised persons. These archives are readable and usable throughout their life cycle.

The CSO takes all necessary steps to ensure archives are retained for the statutory period in accordance with the legal requirements concerning the provision of evidence. The retention period and the methods used are described in [R3].

5.5.4. Archive backup procedure

The archives are backed up in a secure manner, some being subject to dual logging. The methods and resources used for the backup ensure that the elements cannot be easily deleted or destroyed.

5.5.5. Data timestamping requirements

The timestamping of event log data is synchronous, apart from off-line operations. To this end, KMI components are synchronised on a single server synchronised with world time.

5.5.6. Archive collection system

N/A

5.5.7. Archive recovery and verification procedure

The recovery and verification of the archives can be conducted within a period that conforms to the use of the certificates issued. A period of 7 working days is necessary to recover the archives.

5.6. Change of CA keys

The lifetime of the REALTS CA keys is 8 years. The lifetime of certificates issued by the REALTS CA is 3 years. The REALTS CA keys must be renewed no later than 4 years and 1 day after the generation of the CA keys.

5.7. Compromise and disaster recovery

5.7.1. Procedure for reporting and processing incidents and compromises

Procedures and methods of reporting and processing incidents (raising awareness, staff training, analysis of the different log files) are in use.

A major incident – e.g. loss, suspicion of compromise, compromise or theft of certificate management private key – is immediately notified to the CA and the ANSSI. If necessary, the certificate revocation is published as quickly as possible by any means necessary.

5.7.2. Recovery procedure in case of corruption of IT resources (equipment, software and/or data)

A continuity plan is established making it possible to comply with the availability requirements of the different components of the KMI.

5.7.3. Recovery procedures in case of corruption of a component's private key

In the event a CA key is compromised, the corresponding certificate. Will be immediately revoked Action to take in the event the secret elements of the other components are compromised are addressed in the business continuity plan.

The information below concerns the compromise of an algorithm or an associated parameter, such as the CRC algorithm used in the certificates or the length of the key of the certificates.

The CSA and, more particularly, the CSO keep abreast of cases of compromise of the aforementioned elements by means of bodies like the ANSSI.

When informed of a compromise impacting the certificates of the CAs or the timestamp certificates, the CA and the CSO form a crisis unit to determine the actions to be taken to restore service as soon as possible.

The timeframe for effective resumption of activity in the event of a compromise is 14 days.

5.7.4. Business continuity following a disaster

The CSO is in a position to continue to operate in accordance with the disaster recovery plan [R2].

5.8. End of life of the KMI

5.8.1. Transfer or termination of activity affecting the CA and the CSO

The CSN only envisages the termination of its Certificate Authority activity in the event of a qualified and independently effective electronic signature system being established. The CSN is not envisaging the transfer of its Certificate Authority activity.

In the event that ADSN terminates its CSO activity at the request of the CSN, ADSN will initiate the procedure [R8] and maintain the availability of the timestamp certificates verification function.

In the event that ADSN transfers its CSO activity to another company at the request of the CSN, the archiving of the event logs as described in chapter 5.4, as well as the archiving of the certificates and information relating to the certificates used will make it possible to guarantee a constant level of trust. The CA will then organise the takeover of the CSO activities by a new operator [R9].

5.8.2. Termination of activity affecting the CA activity of the CSN

In case of an interruption of service, the following requirements will be taken into account:

1. The private key for issuing certificates will not be transmitted in any circumstances;
2. All necessary steps will be taken to destroy it or render it inoperative;
3. The CA certificate will be revoked;
4. All certificates issued that remain valid will be revoked and the corresponding CMs will be notified;
5. The CA will communicate to the point of contact identified on http://ssi.gouv.fr the principles of the action plan implementing the technical and organisational resources intended to cope with a termination of activity or to organise the transfer of activity. In particular, it will state the archiving arrangements made (for keys and information about certificates) to guarantee this function throughout the period initially provided for in its CP. The CA will communicate the terms of the changes made to the ANSSI, in accordance with the different KMI components concerned. The CA will assess the impact and list the consequences (legal, financial, functional, technical, communicational, etc.) of this event. It will present an action plan intended to eliminate or reduce the risk for the applications and the inconvenience for the CMs and certificate users;
6. The CA will keep the ANSSI informed of any additional obstacle or delay encountered as the process continues.

In the event of an interruption of the CA's activity due to a renewal of the CA chain or a total termination, the CSN undertakes to manage the upkeep of the status of certificates in the following way:

- a final CRL whose expiry date will be positioned at the value 99991231235959Z
- a final OCSP response will be pre-generated for each certificate issued, containing an expiry date positioned at the value 99991231235959Z

These elements are published and available 7 years after the end of validity date of the associated ACs.
The pre-generated OCSP responses are activated to respond at the latest before the end of validity of the REALTS CA certificate

5.8.3. Termination of activity affecting the RA activity of the CSN

In the context of this CP, the RA activity is provided directly by the CA.

6. Technical security measures

6.1. Generation and installation of key pairs

6.1.1. Key pair generation

6.1.1.1. REALTS CA keys

See CP of NOTARIES OF FRANCE CA [R6]
The REALTS CA keys are generated during the key ceremony.

6.1.1.2. Holder keys generated by the CA

N/A

6.1.1.3. Holder keys generated by the holder

The keys are generated directly on the HSM of the timestamp unit before storing the certificate.

6.1.2. Transmission of the private key to its owner

N/A

6.1.3. Transmission of the public key to the CA

When the key pair has been generated on the equipment which will host the certificate, the public key is transmitted in a file in format PKCS#10.

6.1.4. Transmission of the CA's public key to certificate users

The public keys verifying the signature of the CA are distributed to certificate users using a method that guarantees end-to-end data integrity and authentication of origin.

6.1.5. Key sizes

The REALTS CA keys have a size of 4096 bits.
The end certificate keys have a size of 2048 bits and 3072 bits for keys generated after January 1, 2024.

6.1.6. Verification of the generation and quality of key pair parameters

Cf. profiles document [R5].

6.1.7. Objectives of uses of the key

The use of the CA's private key and the associated certificate is limited to the signing of certificates and CRLs, as defined in the description document of the certificates and the CRLs [R5].
The CA's private key is only used in a secure environment.
The private keys of the timestamp units are used exclusively for signing requests for timestamp tokens for the CSN's timestamping services.

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

6.2.1. Standards and security measures for the cryptographic modules

6.2.1.1. Cryptographic module of the CA

The CA's cryptographic module for the generation and implementation of signature keys meets the requirements set out in the regulations.

The cryptographic module for certificate signing must not be handled without authorisation during its transport.

The cryptographic module for the signing of certificates and revocation notifications must not be handled without authorisation during its storage.

The cryptographic module for the signing of certificates and revocation notifications operates in the conditions stipulated by the supplier.

The CA signature cryptographic module has a "Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI..

6.2.1.2. Cryptographic modules of timestamp certificates

The timestamp units have their own cryptographic module, identical to those of the CA ("Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI.).

6.2.2. Control of private keys by several people

6.2.2.1. Cryptographic module of the CA

The CA’s private key is controlled by at least two people.

6.2.3. Private key escrow

The private keys of the CA and holders are not held in escrow.
The private key of the timestamp units is not held in escrow.

6.2.4. Backup copy of the private key

The private key of the REALTS CA must have a backup copy.
The private keys of certificates issued by the REALTS CA do not have backup copies.

6.2.5. Storage of the private key

The private key of the REALTS CA is stored in the archives.
The private keys of the timestamp units are not stored.

6.2.6. Transfer of the private key to / from the cryptographic module

6.2.6.1. Transfer of the CA’s private key

The private key can only be transferred to the backup HSM: this transfer requires the presence of at least two people and must be carried out in such a way that there is no sensitive information on the server.

6.2.6.2. Transfer of the private key of a timestamp certificate

The private key cannot be transferred.

6.2.7. Storage of the private key in the cryptographic module

6.2.7.1. Storage of the CA’s private key

The CA’s private key is stored in the cryptographic module in the security conditions defined by "Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI..

6.2.7.2. Storage of the private key of a timestamp certificate

The private key of a timestamp certificate is stored in the cryptographic module in the security conditions defined by "Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI..

6.2.8. Activation method of the private key

6.2.8.1. Activation of the CA's private key

The CA's private key may only be activated by the individual authorised to do so, and at least two other people must be present.

6.2.8.2. Activation of the private key of a timestamp certificate

The private key of a timestamp certificate may only be activated by the individuals authorised to do so, and at least two other people must be present.

6.2.9. Deactivating the private key

6.2.9.1. Deactivation of the CA's private key

The private key is deactivated from the cryptographic module.

6.2.9.2. Deactivation of the private key of a timestamp certificate

The deactivation of the private key of a timestamp unit is linked to the deactivation of the timestamping context configured. Once deactivated, the private key in question will no longer be usable.

6.2.10. Method of destruction of private keys

6.2.10.1. Deactivation of the CA's private key

The private key is destroyed from the cryptographic module with the aid of commands described by the editor. Once destroyed, the previously generated secret elements cannot subsequently be used.

6.2.10.2. Destruction of the private key of a timestamp certificate

The private key is destroyed from the cryptographic module in accordance with the specifications of the editor of the HSM solution implemented.

6.2.11. Security assessment level of the cryptographic module

6.2.11.1. Cryptographic module of the CA

The CA's cryptographic modules has a "Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI..

6.2.11.2. Cryptographic module of a timestamp certificate

The cryptographic modules has a "Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI..

6.3. Other aspects of the management of key pairs

6.3.1. Archiving of public keys

The public keys of the CA and holders are archived as part of the certificate archiving policy.

6.3.2. Lifetime of key pairs and certificates

The signing keys of the REALTS CA have a lifespan of eight years, as do the certificates.
The signing keys of the timestamp certificates have a lifespan of one year, and the certificates have a lifespan of three years.

6.4. Activation data

6.4.1. Generation and installation of the activation data

6.4.1.1. Generation and installation of the activation data corresponding to the CA’s private key

See CP of NOTARIES OF FRANCE [R6]

6.4.1.2. Generation and installation of the activation data corresponding to the private key of the timestamp certificates

N/A

6.4.2. Protection of the activation data

The activation data of the CA’s keys are only delivered to the authorised individual.

6.4.3. Other aspects related to the activation data

N/A

6.5. Security measures for the IT systems

6.5.1. Technical security requirements relating to the IT systems

6.5.1.1. Identification and authentication

The systems, applications and databases uniquely identify and authenticate the users. Any interaction between the system and a user is only possible after they have been successfully identified and authenticated. For each interaction, the system can establish the identity of the entity.

The authentication information is stored in such a way that it can only be accessed by authorised users.

Access to certificate management interfaces requires a strong authentication based on at least two factors.

6.5.1.2. Control of access

The profiles and rights of access to the CSO’s equipment are defined and documented, as are the procedures for the registration and de-registration of users.

Under no circumstances may an unauthorised individual access the components of the ECSP without being accompanied by an authorised individual.

The systems [Applications and databases] can distinguish between and administer the access rights of each user on the items subject to access rights, for one user, for a group of users, or for both. It is possible to:

- Completely deny users or groups of users access to an item;
- Restrict a user’s access to an item to operations that do not modify the item;
- Grant rights of access to an item by descending to the granularity level of the individual user.

An individual who is not an authorised user may not grant or withdraw access rights to an item. Likewise, only authorised users may introduce new users, or remove or suspend existing users.

The media used by the authorised representative of the CSO are employed in accordance with the requirements of the classification plan.

6.5.1.3. Administration and operation

The use of utility programs is restricted and controlled.

The operational procedures of administration and operation of the KMI are documented, monitored and regularly updated.

The start-up conditions (initial security configuration of the servers) are documented. The settings implemented make it possible to strengthen the security level of systems by applying tightening-up measures. The security measures are described in the CPS [R3].

The end-of-life conditions (destruction and scrapping) of the equipment are documented in order to guarantee the non-disclosure of the sensitive information they hold.

All of the KMI's sensitive materials are subject to a maintenance procedure to guarantee the availability of the functions and information. The procedures are documented.

The staff involved in these procedures are formally appointed.

Measures are applied to monitor maintenance actions.

6.5.1.4. Integrity of the components

Detection and prevention measures are implemented on all the components of the ECSP to provide protection against malware.

The components of the local network (CSO) are maintained in a physically secure environment; periodic checks of conformity to their configuration are made.

Regular penetration and vulnerability detection tests are carried out on all the technical components of the CSO.

6.5.1.5. Flow security

Security measures are implemented to guarantee the authentication of origin, integrity and confidentiality, if appropriate, of the data exchanged between entities involved in the process.

6.5.1.6. Logging and auditing

Activity can be monitored through the events logs. All events related to system security are logged. The details of the events concerned are described in the CPS [R3].

The systems are synchronised with UTC time to the nearest second.

6.5.1.7. Supervision and control

Permanent supervision is carried out and alert systems installed to detect, record and respond rapidly to any unauthorised and/or irregular attempt to access resources (hardware and/or software).

6.5.1.8. Raising awareness

Appropriate measures to raise the awareness of ECSP users are implemented.

When a security breach is detected on a CSO component, the individuals affected are made aware of the impact of the breach and an action plan is defined to cover the breach within a reasonable time.

6.5.2. Security assessment level for the IT systems

N/A

6.6. Security measures linked to systems development

The development and test infrastructures are separate from the operational infrastructures of the KMI.

The criteria for the reception and validation of new IT systems, upgrades and new versions are established, and suitable tests of the system are conducted before it is received and put into production.

A capacity plan is established to ensure the proper processing of certificates issued by the CA.

6.6.1. Measures associated with security management

The KMI is monitored in regard to the installation of the CSO security management system. The steering committee manages the passing of information to the CA, which is notified of any significant change.

Any upgrades to the components must be documented in the operational procedures.

6.6.2. Security assessment level of the life cycle of the systems

Monthly CSN-ADSN security monitoring committee make it possible to ensure that the security level is maintained and any improvements are made.

6.7. Network security measures

The measures put in place conform to the risk analysis conducted on the IT system [R1].

Network communications carrying confidential information are subject to protective measures against bugging. The corresponding network components are hosted in a secure environment.

Periodic scans are conducted to detect vulnerabilities on the ECSP equipment accessible from the Intranet or Internet.

Security gateways are set up to protect the local component of the IT system from unauthorised access from the Intranet and Internet.

The redundancy of access on the ECSP services on the Internet is guaranteed.

6.8. Timestamping / dating system

Cf. 5.5.5.

7. Profiles of certificates, OCSP and CRLs

The profiles of certificates and CRLs are described in a dedicated document entitled “description of certificates and CRLs” [A4].
This document is published by ADSN on its website and at https://www.preuve-electronique.org.

7.1. Certificate profiles

7.1.1. Version no.

7.1.2. Certificate extensions

7.1.3. OID of the algorithms

7.1.4. Form of names

7.1.5. Name constraints

7.1.6. OID of the CPs

7.1.7. Use of the policy constraints extension

7.1.8. Policy qualifiers semantics and syntax

7.1.9. Processing semantics for the critical CP extensions

7.2. Certificate revocation list profile

7.2.1. Version number

7.2.2. CRL extensions and CRL entry extensions

7.3. OCSP profile

The OCSP service conforms to RFC 6277 and RFC 2560.
The service is accessible on the servers of the ADSN IT system and on the Internet.

7.3.1. Version number

The OCSP request and response are in version 1.

7.3.2. OCSP extensions

OCSP request:

- It is necessary to complete the RequestorName field of the OCSP request with the name of the calling application.
- The cyclic redundancy checks (CRC) provided in the OCSP request must be calculated using the algorithm SHA256 or SHA512, depending on the content of the request.

OCSP response:

- The response contains the name of the CA signatory.

8. Compliance audit and other assessments

8.1. Frequencies and/or circumstances of the assessments

A check for compliance with the CP when the system is implemented, or subsequent to any significant modification, is carried out in the form of an annual internal audit.

8.2. Identities: role of the assessors

The assessor is careful to ensure that the policies, statements and services are correctly implemented and to detect cases of non-compliance that could compromise the security of the service provided.

8.3. Relations between the assessors and the assessed entities

The assessor is appointed by the CA. He/she is independent of the CA, the RA and the CSO.

8.4. Scope of the assessments

The assessor makes regular compliance checks of the implementation of:

- the certification policies
- the certification practices statements
- the implementation services

8.5. Actions taken on completion of the assessments

On completion of a compliance check, the audit team gives the CA a notification that can be “pass, fail or to be confirmed”.

In the event of a fail, the audit team passes its recommendations to the CA; the CA can decide which measures to implement.

In the event of a “to be confirmed” result, the audit team identifies and prioritises the areas of non-compliance; it is up to the CA to suggest a schedule to correct the non-compliances; a subsequent inspection will make it possible to lift the non-compliances previously identified.

In the event of a pass, the CA confirms to the inspected component its compliance with the requirements of the CP.

8.6. Communication of results

In the case of a CA qualification, the audit results are made available to the body in charge of the qualification.

9. Other professional and legal issues

9.1. Scheduled charges

The CA may impose charges for:

- The issue or renewal of certificates
- The provision of a directory listing the certificates

The provision of CRLs is never billed.

9.2. Financial liability

9.2.1. Insurance cover

Risks likely to engage the liability of the CSN are covered by an appropriate insurance policy.

9.2.2. Other resources

The CSN confirms it has an adequate financial guarantee specifically allocated to the cover of financial risks.

9.2.3. Cover and guarantee concerning the user entities

No specific requirement.

9.3. Confidentiality of professional data

9.3.1. Scope of the confidential information

The CSN and the CSO prepare an inventory of all information assets and perform a classification to define the protection requirements consistent with needs.
In particular, the following information is treated as confidential:

- The private keys of holders and CAs
- The activation data
- The event logs
- The registration files of the CMs

9.3.2. Information that does not qualify as confidential information

N/A

9.3.3. Responsibilities in regard to the protection of confidential information

The CSN undertakes to process the confidential information gathered in accordance with the laws and regulations in force.

9.4. Data protection

9.4.1. Data protection policy

Technical, procedural and organisational measures are established to guarantee the protection of personal data collected at the time of registration.

9.4.2. Personal information

Personal data are data of a personal nature gathered concerning the CM (no personal data in the timestamp certificates). This relates to the CM commitment file containing certificate issue / renewal / revocation requests (including copies of identity documents and reasons for revocation), and data for physical access (badge) to premises / DC hosting of KMI components / timestamping and video recordings.

9.4.3. Non-personal information

No specific requirement.

9.4.4. Responsibilities in regard to the protection of personal data

The CSN or a third party appointed by the CSN ensures the confidentiality of any requestor folder and possibly of certain events as stipulated in this CP. The CSN undertakes to request to any entity intervening for itself as well as its employees to enforce the level of confidentiality expected.

The CSN undertakes to take and maintain the necessary measures to ensure the security and confidentiality of any application file, in accordance with the provisions of Regulation (EU) 2016/679 of 27 April 2016 [A6].

The execution and management of the General Conditions imply the implementation of a processing of personal data to whose the Holder consents and of which the CSN is responsible. In accordance with applicable regulations, the Holder is informed that the communication of his data is mandatory and necessary to take into account his certificate application, to ensure its management and its life cycle.

According to Regulation (EU) 2016/679 of 27 April 2016, the holder can access his data in soliciting:

- The data controller, the Higher Council of Notaries, Certification Authority, 60 boulevard de La Tour-Maubourg, 75007 PARIS - Tel: +33 1 44 90 30 00 - mail: author -certification@notaires.fr, or
- The data protection officer of the CSN, cil-csn@notaires.fr - 95 avenue des logissons, 13107 VENELLES Cedex.

If necessary, the holder may also request the rectification or deletion of data concerning him, obtain the limitation of the processing of these data or oppose it for legitimate reason, except in cases where the regulations do not allow the exercise of this rights.

If, after contacting the data controller or data protection officer, the data subject considers that his rights are not respected or that the processing does not comply with the data protection rules, he may submit a complaint online or by post to a supervisory authority.

9.4.5. Notification and consent for use of personal data

N/A

9.4.6. Conditions for disclosure of personal information to judicial or administrative authorities

Records can be made available as legal proof of certification if required.

9.4.7. Other circumstances concerning the disclosure of personal information

No specific requirement.

9.5. Intellectual and industrial property rights

The provision of service by the CSN may not be interpreted as leading to the transfer of any intellectual property right whatsoever.

9.6. Contractual interpretations and guarantees

9.6.1. Certificate authorities

The CSN is responsible for:

- the validation and publication of the CP,
- the validation of the CPS and its conformity to the CP,

- the conformity of the certificates issued to this CP,
- the compliance with all the security principles by the different components of the KMI, and for the associated controls.

The CSN is responsible for any damage resulting from a failure to comply with this document by itself or any of the components of the KMI.

Unless it can be clearly demonstrated that it has committed no intentional fault or negligence, the CSN is responsible for any prejudice caused to any natural person or legal entity that reasonably relies on the certificates issued in each of the following cases:

- The information contained in the certificate does not correspond to the information provided at the time of registration
- After the certificate had been issued, no verification was made as to the possession of the corresponding private key by the holder
- The CA or CSO did not record the revocation of a certificate and/or publish this information in accordance with its commitments.

The CSN is not liable for any prejudice caused by a use of the certificate exceeding the limits imposed on its use.

Finally, the CSN assumes liability for any fault or negligence in the precautions to be taken in regard to the confidentiality of the personal data confided to it by the holders.

9.6.2. Registration service

Cf. above

9.6.3. CM

The managers of certificates issued for the timestamp units of the CSN are required to familiarise themselves with and approve this Certification Policy.

9.6.4. Certificate users

Certificate users must check the status of a certificate from the distribution points of the CRL defined in this CP.
To this end, they may request the point of contact defined in paragraph 1.5.2 to provide the CRL and the CA certificates applicable at the time of the check, if the latter are not publicly accessible.
The operation consists of checking that:

- The serial number of the certificate concerned does not appear in the applicable CRL

- The certificate used was correctly issued by the applicable certification chain.

9.6.5. Other participants

No specific requirements

9.7. Limit of liability

The CSN refuses liability for any damage resulting from the use of key pairs for any purpose other than those intended.

The CSN also refuses liability for any damage resulting from errors or inaccuracies in the information contained in the certificates, when these errors or inaccuracies result directly from the inaccuracy of the information communicated by the Certificate Manager.

9.8. Indemnities

N/A

9.9. Validity and early expiry of the CP

9.9.1. Period of validity

This document is applicable until the last certificate issued under the terms of this CP reaches the end of its lifespan.

9.9.2. Early expiry

Other than in exceptional circumstances related to security, developments concerning this document do not require the revocation of certificates already issued.

9.9.3. Effects of expiry and clauses that remain applicable

N/A

9.10. Individual notifications and communications between the participants

In the event of a change of any kind in the composition of the KMI, the CSN will validate the change by means of a technical assessment and will analyse the impact in terms of security and quality of service.

9.11. Amendments to the CP

9.11.1. Amendment procedures

The CSN undertakes to ensure that any change made to this document is consistent with the objectives of compliance with the regulatory requirements for ECSP certification.

9.11.2. Notification process and timeframe for amendments

No specific requirement.

9.11.3. Circumstances in which the OID must be changed

Any significant change in the CP which will have a major impact on the certificates already issued will be accompanied by a change of OID.

9.11.4. Notification to users

Any new version of this Certification Policy will be notified on the website https://www.preuve-electronique.org intended for holders and utility applications.

This notification will precede any issue of an end certificate in accordance with the requirements of the new Certification Policy.

9.12. Dispute resolution provisions

In accordance with the legislation and regulations in force, the conditions of the certificates issued are defined by this Certification Policy.

9.13. Competent courts

This Certification Policy is subject to French law.

Any dispute concerning the validity, interpretation or performance of this Certification Policy will be submitted to the competent courts of the Paris Court of Appeal.

9.14. Compliance with legislation and regulations

This PC conforms to the legislation and regulations shown in chapter 10 in regard to the management of CA certificates.

9.15. Miscellaneous provisions

9.15.1. Comprehensive agreement

No specific requirement.

9.15.2. Transfer of activity

Cf. chapter 5.8

9.15.3. Consequences of an invalid clause

No specific requirement.

9.15.4. Application and waiver

No specific requirement.

9.15.5. Force majeure

Cases of force majeure are considered to be those generally used by the French courts, particularly in the case of an unstoppable, overwhelming and unforeseeable event.

9.16. Other provisions

N/A

9.17. General Terms and Conditions of Use

N/A

10. Associated documents

10.1. Applicable documents

[A1]	RFC 3647. Internet X509 PKI certificate policy and certificate practice statement framework
[A2]	Decree of 26 July 2004 relative to acknowledgment of certification service providers and the official recognition of the evaluation bodies
[A3]	European Regulation eIDAS 910/2014
[A4]	Notarial Certification Infrastructure. Description of certificates and CRLs
[A5]	ISO/IEC 9594. Distinguished Name
[A6]	Regulation (EU) 2016/679 of 27 April
[A7]	Law no. 2008-696 of 15 July 2008 on archives
[A8]	EN 319401 “General Policy Requirements for Trust Service Providers”
[A9]	EN 319411-1 “General requirements”
[A10]	EN 319411-2 “Requirements for trust service”
[A11]	EN 319412-1 “Overview and common data structures”
[A12]	EN 319412-3 “Certificate profile for certificates issued to legal persons”

10.2. Reference documents

[R1]	Risk analysis
[R2]	Management of the disaster recovery plan
[R3]	Certification Practices Statement of the REALTS CA
[R5]	Description of the certificates and CRL of the Notaries of France CA chain
[R6]	Certification Policy of the NOTARIES OF FRANCE Ca
[R8]	Termination of activity procedure
[R9]	Transfer of CSO activities

11. Annex 1: Security requirements for the CA's cryptographic module

11.1. Requirements for security objectives

The cryptographic module used to generate certificates and CRLs satisfies the following security requirements:

- Guaranteeing the confidentiality and integrity of the private signature keys of the CA throughout their life cycle and their destruction at end of life
- Being able to identify and authenticate its users
- Limiting access to its services in accordance with the user and the role assigned to it
- Being able to carry out a series of tests to check that it is functioning correctly and to enter a safe state if an error is detected
- Enabling the creation of a secure electronic signature to sign the certificates generated by the CA, which does not reveal the private keys of the CA and which cannot be forged without knowledge of the private keys
- Creating audit records for each modification concerning security
- If a function for the backup and restoration of the CA's private keys is provided, guaranteeing the confidentiality and integrity of the backed up data and claiming at least a double-checking of the backup and restoration operations
- Detecting attempts to tamper with data and entering a safe state when an attempt is detected

11.2. Certification requirements

The module is certified in accordance with the above requirements, and has been rated ("Common Criteria Certificate" label, according to the ANSSI Scheme and the protection profiles recognized by ANSSI.).

12. Editions

Version / Edition	Date	Issuer	Approver
0.1	11/08/2017	ADSN	Members of the CSN board
1.1	16/05/2019	ADSN	Members of the CSN board
1.2	29/09/2020	ADSN	Members of the CSN board
1.3	21/01/2021	ADSN	Members of the CSN board
1.4	18/10/2022	ADSN	Members of the CSN board
1.5	12/03/2024	ADSN	Members of the CSN board
1.6	11/02/2025	ADSN	Members of the CSN board