General Terms and Conditions of Use

REALTS CA

Version	Date	Description	Authors	Company
1.0	02/12/2015	Original draft	Y. THOMASSIER	REAL.NOT
1.1	08/09/2017	eIDAS additions	Y. THOMASSIER	REAL.NOT
1.2	08/12/2017	Addition after review by the legal department	Y. THOMASSIER	REAL.NOT
1.3	16/05/2019	Informations regarding archiving and change REAL.NOT in ADSN	M. Bontrond / M. PORPORAT	CSN / REAL.NOT

Status of document	Classification
Approved	PUBLIC
OID of the document	
1.2.250.1.78.2.1.3.5.1.3	

CONTENTS

1 INTRODUCTION

1.1 Definitions

Agence Nationale de la sécurité du Système d'Information (ANSSI): the French Network and Information Security Agency.

Certificate Authority (CA) Entity that generates and issues electronic certificates. In the context of this document, the role of CA is assumed by the CSN, or any third party that would act in its place in accordance with its Certification Policy.

Conseil Supérieur du Notariat (CSN): the High Council of French Notaries – the body responsible for trust services on behalf of the Notariat. In particular, the CSN is the Certificate Authority defined by these GTCU.

Certification Practices Statement (CPS): certificate issuing practices associated with a Certification Policy

Key Management Infrastructure (KMI): technical infrastructure for the management of key pairs and electronic certificates.

Certificate Revocation List (CRL): a list electronically signed by the CA that contains all the identifying details of the certificates that have been revoked.

Lightweight Directory Access Protocol (LDAP): Protocol for accessing and maintaining directory information services.

Object Identifier (OID): unique number identifying an item (document, procedure, process, etc.)

Online Certificate Status Protocol (OCSP): Internet protocol used to validate the status of an X509 digital certificate.

Certification Service Operator (CSO): project management of the certificate issuing service, states the certification practices and issues the end certificates.

Certification Policy (CP): set of rules, identified by a name (OID), defining the requirements which a CA must satisfy when generating certificates.

Electronic Certification Service Provider (ECSP): individual in charge of the production and delivery of electronic certificates. The role of the ECSP is assumed by the CSN.

Certificate Manager (CM): ADSN employee responsible for managing the signing certificates of the timestamp units.

Request For Comments (RFC): numbered series of official documents describing the technical aspects of the Internet or various IT hardware.

1.2 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 produce paperless authenticated deeds and, more generally, to secure all of their communications.

A certification structure has been established for this purpose. This document constitutes the General Terms and Conditions of Use of the certificates issued by the REALTS CA (hereinafter referred to as the "GTCU-REALTS"). The certificates issued by the REALTS

CA are exclusively intended for the timestamp units of the timestamping service implemented by ADSN on behalf of the CSN, which is the timestamping authority.

The objective of this document is to summarise the CSN's undertakings, as the CA, as regards the issue and management of electronic certificates, as well as the obligations of the other participants. The details of these requirements are described in the REALTS Certification Policy (CP), which can be consulted on the website https://www.preuve-electronique.org.

This document is supplemented by a Certification Practices Statement (CPS).

The CPS sets out the mechanisms and procedures implemented to achieve the security objectives of the CP.

1.3 Identification of the document

These General Terms and Conditions of Use of the REALTS CA are identified, in the documentary database of the ADSN trust infrastructure, by a unique identification number, the OID. 1.2.250.1.78.2.1.3.5.1.3.

Other more explicit elements (name, version number, date of update) also help to identify it.

2 GENERAL TERMS AND CONDITIONS OF USE OF THE CERTIFICATION SERVICE OF THE REALTS CA

These GTCU-REALTS are based on the template set out in annex A of the standard EN 319411-1 (version 1.1.1).

Point of contact	Member of the CSN board, responsible for information and communication technologies 60 Boulevard de la Tour Maubourg 75007 Paris 01 44 90 30 00
Types of certificate, validation procedures and usage restrictions	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 tokens. Only the first profile is concerned by these GTCU-REALTS. The class 0 certificates issued by the REALTS CA may be used for timestamp signatures for the CSN's timestamp servers. The certificate issued by the REALTS CA is under the responsibility of a Certificate Manager (CM) formally identified during a key generation ceremony for a new Timestamp Unit (TU). To obtain a certificate, 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 timestamp 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. Technically the request for a certificate is originally made by the KMI administrator via a tracked internal request from an identified CM for timestamp certificates. The renewal of a certificate issued by the REALTS CA requires a new request, which follows the same process as the

	original request. A request to revoke a certificate may come from the CM or from an authorised individual within the CA's organisation and is processed by the KMI Administrator.
Restrictions on use	Class 0 certificates may not be used for any purpose other than those defined in the line: "Types of certificate, validation procedures and usage restrictions".
Archiving	The archive retention periods for each type of data are as follows: - CRL and client certificates: 23 years - OCSP request and response: 23 years - Technical events: 1 year - Functional events: 23 years - Registration file (paper applications for certificates): 23 years - RC registration form: 23 years
Obligations of the subscriber	The subscriber is represented by the CM of the signing certificate of a timestamp unit, who undertakes: - To request the generation of a key pair only through the process of generating a new time stamping environment of the AH. - To ensure that the signing certificate generated corresponds to the request from the timestamp unit in question. - To ensure that this certificate is installed on the correct timestamp unit. - To monitor the life cycle of the certificate and initiate the annual renewal procedure, or revocation procedure if necessary (compromise of the private key associated with the signing certificate, compromise of a timestamp unit, compromise of the private key of the REALTS CA).
Obligations of the REALTS CA	The CSN is responsible for: • the validation and publication of the CP of the REALTS CA; • the validation of the CPS of the REALTS CA and its conformity to the CP; • the conformity of the certificates issued to the REALTS CP; • the compliance with all the security principles by the different components of the KMI, and for the associated controls. In case of a major incident (e.g. loss, suspicion of

	compromise, compromise or theft of a certificate management private key), the incident must immediately be notified to the ANSSI (supervision-eIDAS@ssi.gouv.fr). 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. In case of the discontinuation of the activity of the CA or the timestamping services, the corresponding certificates of the timestamp units will be revoked. 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.
Checking the status of certificates	The user of a certificate is required to verify the status of certificates, including those of the corresponding chain of trust (Regulated professions CA, Notaries CA, REALTS CA). The REALTS CA provides users with an updated CRL, published on the REAL network in the CRL publication directory by LDAP (annuaire.real.notaires.fr), and online on the website https://www.preuve-electronique.org and an associated OCSP service. The CRL contains the extension "ExpiredCertsOnCRL" and stores the serial numbers of all revoked certificates, even those that have expired. 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 keeps the revocation status of the certificate available after it has expired.

	If the OCSP request contains a request for a serial number not issued by the REALTS CA, the OCSP will include in the responding response the status "unknown" if the REALTS CA is still valid, and "unauthorized" if it has expired. In the event of the end of life of the REALTS CA, the CSO will generate: - 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 If the CSN stops the activity of the REALTS CA, it undertakes to keep the CRLs and pre-generated OCSP responses available.
Limit of guarantee and liability	The CSN may not be held liable for the unauthorised or non-compliant use of the certificates, associated private keys and activation data, CRLs or any other equipment or software provided. 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. The CSN may not be held liable for any damages resulting from a claim by a third party, loss of clientèle, interruption of work or any other damage, particularly indirect damage or commercial loss.
Applicable agreements and certification practices	The Certification Policy describing the requirements with which the REALTS CA expects to comply and the corresponding Certification Practices Statements are published on the following website: https://www.preuve-electronique.org. The OID of the Certification Policy is: 1.2.250.1.78.2.1.3.5.1.1 The OID of the Certification Practices Statement is: 1.2.250.1.78.2.1.3.5.1.2
Confidentiality policy	The CSN and the CSO must 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 the end certificates and of the

	REALTS CA; • The activation data; • The event logs; • The registration forms of the CMs.
Insurance policy	Risks likely to engage the liability of the CSN are covered by an appropriate insurance policy.
Applicable law and resolution of disputes	The activities of the REALTS CA are governed by European regulations. All disputes and litigation arising from the interpretation and implementation of this document will be subject to the jurisdiction of the competent courts of the Paris Court of Appeal.

Audit and certification	The REALTS CA does not hold formal certifications. Nevertheless, the practices implemented conform to the supply of timestamp certificates for a qualified timestamping service within the meaning of REGULATION (EU) No. 910/2014 Of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
	The following documents are published by the CA:
	- Certification Policy: https://www.preuve-electronique.org
	- General Terms and Conditions of Use: https://www.preuve-electronique.org
	- Certificate Revocation List:
	  ○ ldap://annuaire.real.notaires.fr:389
	  ○ ldaps://annuaire.real.notaires.fr:636
	  ○ https://www.preuve-electronique.org/certificats-revoques.html
	- OCSP Server: ocsp.preuve-electronique.org