CONSEIL SUPÉRIEUR DU NOTARIAT

GENERAL TERMS AND CONDITIONS OF USE OF THE "CLÉ REAL" AND THE ASSOCIATED CERTIFICATES

Version 2.6 applicable from 30 march 2022

1 – PREAMBLE AND SUBJECT

The Conseil Supérieur du Notariat (CSN – the High Council for the French Notariat) offers notaries and their employees a «Clé Real» into which Certificates are imported, making it possible to provide authentication, digital signature and encryption functions for the services offered as part of their relationships between notaries and with their preferred partners. Within this framework, the CSN relies on ADSN to implement, issue and manage the «Clés Real» and Certificates. The conditions of issue and management and, more generally, the life cycle of «Clés Real» and associated Certificates are described in the Certification Policy (CP) of the Certification Authority (CA) established by the CSN and accessible at www.preuve-electronique.org.

The General Terms and Conditions set out the procedures for the issue and use of the «Clé Real», the Certificates and the related functions.
These General Terms and Conditions define the Certification Services via which the CSN provides notaries and their staff with Certificates on «Clé Real».

2 – DEFINITIONS

In addition to the terms defined within the body of this document, the terms used with a capital letter have the meaning ascribed to them in the CP Reference.

CA or Certification Authority designates the Certification Authority that issued one of the certificates present on the «Clé Real». The CA is responsible for keeping a record of applicants for Certificates and of the issue of Certificates. The CA is represented by the CSN.

Authentication (as it appears in this document) means the procedure for checking the identity of the Holder.
Certificate means the digital identity certificate of the Holder issued by the CA that verifies the connection between the identity and the Private Key of a Certificate Holder.

Chain of trust refers to all of the Certificates necessary to validate the origins of a Certificate.

Private Key refers to the part of a key pair kept secret by its Holder which, used in combination with the Public Key, enables a digital signature to be authenticated or created.

Public Key refers to the part of a key pair that enables an authentication or a digital signature to be verified. The Public Key is contained in the Certificate.

«Clé Real» means the Chip, located on a USB Key, totally personal and confidential to each Holder and containing his/her Certificates.

USB Key means a USB reader distributed by ADSN enabling the use of the Chip.

Activation Code means the code issued when the Certification Agent validates the application and given to the Holder in person. The Activation Code is required to initialise the Chip.

PIN Code refers to the password enabling the implementation of the private keys associated with certificates contained in a «Clé Real».

CSN: Conseil Supérieur du Notariat (High Council for the French Notariat).

General Terms and Conditions refers to these general terms and conditions for use of the «Clé Real» and associated certificates, supplemented by the Certification Policies of the CAs issuing the certificates present on the «Clé Real», available at www.preuve-electronique.org.

Applicant File refers to all of the documents associated with an initial «Clé Real» application: a copy of an identity document, the notice of appointment or oath-taking, or any other supporting document from the notary acting in the case, certificate of employment for a worker, the form for collecting the handwritten signature and his seal for a notary, or the form for collecting the handwritten signature and his stamp for an authorised clerk until 31/12/2020, and the paper form signed by the «Clé Real» Applicant and the digital version listed in SACRE.

60 Bd de La Tour-Maubourg - 75007 Paris
Tél. : 01 44 90 30 00 - notaires.fr

LRC means the List of Revoked Certificates certified by the signature of the CA and including the series numbers of Certificates that have been revoked.

Certification Agent means any individual who has been delegated the power to authorise a Certificate application bearing the name of the organisation. [To avoid confusion, it has not been abbreviated to CA in this document.] The President of the CSN validates the «Clé Real» applications from CSN notaries. The CSN's Certification Agents validate «Clé Real» applications from CSN associates and notaries from the Chambers. The Chambers' Certification Agents validate «Clé Real» applications from Chamber staff and notaries from the Company. The Certification Agents from the offices validate «Clé Real» applications from their colleagues.

Holder Number refers to a 10-digit unique number allocated to each «Clé Real» Holder. This number is required to initialise the «Clé Real».

OCSP means Online Certificate Status Protocol.

CP means the Certification Policy of the CA defining the rules with which the CA complies when issuing of Certificates intended to be used when signing authentic instruments.
Chip refers to the strictly personal and confidential smart card, or chip card, issued to each Holder and containing his/her Certificates.

Security Question means the question / answer pairing known only to the holder of the «Clé Real» and enabling his/her authentication for the emergency revocation of the «Clé Real».
CP Reference refers to chapters 1, 2, 3 and 9 of the CP of the CAs issuing the certificates present on the «Clé Real».

SACRE: Suivi Administratif des Clés Real (Administrative Monitoring of the «Clés Real»). Software for the processing of «Clé Real» applications and renewals and which makes it possible to revoke Chips electronically.

Digital Handwritten Signature means the handwritten signature of a notary or authorised clerk that is scanned and then inserted onto the Chip contained in the «Clé Real» when it is initialised.

Holder means any person who has sent the Certification Agent an application to obtain a «Clé Real».

3 – THE ASSOCIATED CERTIFICATES AND FUNCTIONS

3.1 Technical prerequisites

The notarial office guarantees having obtained from its IT partner the assurance that its information system is compliant with the requirements against computer viruses as well as with the regulations relating to the protection of personal data. The notarial office also declares that its software is guaranteed by the software publisher.

3.2 Initialisation of «Clé Real» applications

The Holder logs on to the software for the Administrative Monitoring of the «Clé Real» (SACRE) accessible from the notaries' Intranet at http://intra.notaires.fr. He makes an initial application for a «Clé Real» by notifying his full name, the CRPCEN number of the office or official body, email address and identity card details (type, number, expiry date). The application is accompanied by a digital copy of the paper application form for the «Clé Real», containing these General Terms and Conditions, completed and signed with the required attachments (copies of documentary evidence supporting his identity and status as notary or notary's employee). He selects a password that will be requested when the «Clé Real» is initialised. He is given an application username.

He then, within a maximum period of three months, and during a personal meeting with the Certification Agent (the notary partner or holder from his office for an employee, or the agent of his Departmental or Interdepartmental Chamber for a notary), presents the supporting documents verifying his identity and position as notary and the paper application form for the «Clé Real» that he has scanned and attached to the application in SACRE. The Certification Agent logs on to SACRE, verifies, the identity and status of the applicant and the consistency with the information on the paper application form copied into SACRE with the documents presented by the applicant. Once the checks are complete, the Agent validates the «Clé Real» application electronically in SACRE. He is then given a receipt containing the Activation Code for the «Clé Real» and the Holder Number. The receipt is printed out and given to the Holder. The information it contains is needed for the Holder to initialise the «Clé Real». All of the paper documents provided to the Agent by the Applicant at the meeting will be added at least once a year by the Agent to an act of deposit of summary documents preserved in his records.

When ordering or renewing a «Clé Real», the Holder agrees that his Certificates are available for download.

If an application has still not been validated three months after its registration, the registration will be cancelled in SACRE. The applicant will be notified accordingly and will have to submit a new application.

3.3 Holder's undertaking

The Holder undertakes to send his Certification Agent full, accurate and reliable information in all circumstances, especially when the initial application is made or a renewal is applied for. The Holder guarantees the truthfulness of such information and of all supporting documentation provided. The Holder undertakes to inform the Certification Agent immediately of any changes in the aforementioned information and supporting documents provided. The Holder is solely responsible for his «Clé Real» and PIN Code and for the use of them.

When his «Clé Real» is initialised, once his Certificates have been downloaded, the Holder checks the information relating to his identity included in the Certificates: full name, email address, Holder Number. He then chooses to accept or reject his Certificates. If he accepts the Certificates, he also selects a PIN Code and then a Security Question, as well as, if necessary, his Digital Handwritten Signature and the image of his seal (for a notary) or stamp (for an authorised clerk until 31/12/2020). The CSN or any other Notariat body may not be held liable for an incorrect or inaccurate entry on the Certificates, or for false or inaccurate supporting documents. The information contained in the Certificates is consistent with the details provided by the Holder himself when registering the application.

The Holder undertakes to generate his signature key pair within the «Clé Real».
After initialising the «Clé Real», the Holder undertakes not to export the Private Key associated with his signature certificate outside of his «Clé Real».

The Holder undertakes to not use the private key associated with his signature certificate except electronic signature of electronic documents in professional environment.

The Holder undertake to use the private key associated with his signature certificate only int cryptographic functions calculated inside the «Clé Real».

The Holder undertakes to not use anymore his «Clé Real» in case of compromise CA which has signed his certificates.

3.4 Functions associated with the Certificates

The Holder is responsible for the use of his «Clé Real» and the associated Certificates in both form and content. Use of the «Clé Real» must be restricted to the professional needs of the Notariat, within the framework of the electronic services provided by notaries and their staff in the offices and Notarial Bodies. In particular, the signature certificates contained on the «Clé Real» may only be used to produce electronic signatures. The Holder will be liable for any direct or indirect damage resulting from the use of a «Clé Real» for any purpose other than those provided for in the CP Reference, and any damage resulting from acts that are unlawful, contrary to proper practice or in violation of the rights of third parties in which the use of the «Clé Real» was involved.

4 – DEVELOPMENTS AFFECTING THE «CLÉ REAL» AND THE CERTIFICATES IT CONTAINS

4.1 Validity and renewal of the «Clé Real»

The Chip of a «Clé Real» remains valid until the expiry of the certificates it holds. The certificates are valid for three (3) years, except for CSN certificates generated before the qualification of Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing directive 1999/93/EC, which are valid for two (2) years. During the three months preceding the expiry date of the Chip of the Holder's «Clé Real», an email will be sent automatically to the Holder stating that he is required to renew it before it expires.

On renewal of a «Clé Real» that is nearing expiry, the Holder logs on to the SACRE software, identifying himself with the still valid «Clé Real», and applies to renew the Chip of his «Clé Real» and generate new certificates. The holder must provide the supporting documents necessary for the constitution of his request in a unitary way in order to establish in Sacre the file that he will edit at the end of the course, sign and present during the face to face meeting with his certification agent. In the case of a renewal with an expired «Clé Real», the Holder must follow the same procedure as for an initial application (cf. paragraph 3). However, he will enter only the Holder Number of the current «Clé Real» and will attach the scanned copy of the paper application form for the «Clé Real» completed and signed with the required attachments (copies of documentary evidence supporting his identity and status as notary or notary's employee).

4.2 Blockage of the «Clé Real»

In the event of three successive incorrect entries of the PIN Code, the «Clé Real» will be blocked automatically and permanently. If the Holder wishes to obtain a new «Clé Real», he must follow the same procedure as for a renewal

application with an expired «Clé Real» (cf. paragraph 3).

4.3. Revocation: the consequences.
The Holder is liable for any damage caused to CSN or to third parties by the non-revocation or a late revocation of his Chip. The hotline can be contacted by the individual requesting the revocation to ascertain the circumstances under which a revocation must be requested. The help hotline can be accessed on 0 800 306 212 Service & appel gratuits

The revocation of the «Clé Real»'s Chip leads to the revocation of all the Certificates it contains and in turn leads to the entry of the revoked Certificates on a List of Revoked Certificates (LRC) accessible to the public at www.preuve-electronique.org. The Certificates will be entered on the LRC no later than 24 hours after the revocation request. The Certification Agent and the Holder concerned will be informed of the revocation of the Certificates by email.

The Holder refrains from using his «Clé Real» once he has requested its revocation, or when he learns by email that it has been revoked. The Holder may ask the CSN to give the reasons for the revocation of his «Clé Real». He will receive a reply by registered letter with acknowledgement of receipt. The reason for the revocation is also included in the email sent to him.

If his «Clé Real» has been revoked, the Holder may make a new application for a «Clé Real» by logging on to SACRE.

4.4. Standard revocation.
The Certification Agent of an office will revoke the «Clé Real» of one of his co-workers by logging on to SACRE and following the instructions. He will revoke the Chip of one of his co-workers in the following circumstances:

- the Holder leaves the office;
- the death of the Holder;
- the Holder changes posts;
- the Holder fails to fulfil his obligations.

The Certification Agent of a Chamber will revoke the «Clé Real» of a notary of the Company or of an employee of the Chamber by logging on to SACRE and following the instructions. He will revoke the Chip of one of the Company's notaries in the following circumstances:

- the Holder leaves the organisation;
- the death of the Holder;
- the Holder fails to fulfil his obligations.

The CSN can also revoke the «Clé Real» in the cases listed above, as well as in the following cases:

- the revocation of the CA's Certificate or of one of the Certificates of the CA's Chain of Trust;
- the termination of the General Terms and Conditions;
- a technical problem with the «Clé Real».

4.5 Emergency revocation
Only the Holder may make an emergency revocation of his Chip.
Several possibilities are available to the Holder:

1. The Holder has access to the Notaries' Intranet. He logs on to SACRE and revokes his Chip by following the instructions given by the software.
2. The Holder does not have access to the Notaries' Intranet, but can connect to the Internet. He visits http://revocation-carte-real.notaires.fr and revokes his Chip.
3. The Holder does not have access to the Internet. He carries out his emergency revocation by telephone. He calls the emergency revocation hotline on 0 820 887 763 Service 0,118 € / min + prix appel .

The Holder must perform an emergency revocation of his «Clé Real» in the following circumstances:

- loss or theft of the «Clé Real»;
- compromise or suspected compromise of the «Clé Real» or its contents;
- inconsistency of the information contained (the information or documents are no longer accurate, the Holder is no longer employed by the Notariat or his professional activity or status has changed);
- the Holder's name has changed (e.g. after marriage).

5 – VERIFICATION OF THE CERTIFICATES ISSUED

The users of the certificates contained on the «Clé Real» can check the status of the certificates by using the status information functions provided by the CA.

Third parties using the certificates of the «Clé Real» must check the status of certificates using the certificate status information functions provided by the CA.

The status information functions are available 24 hours a day, 7 days a week by downloading the LRC of the CA who issued the certificate to check on the website www.preuve-electronique.org or using OCSP, only for certificates issued from CA RealSIGN and RealAUTH, on the internet site service ocsp.preuve-electronique.org.

CRLs contain all the certificates of the issuing CA that have been revoked, even after their validity date has been reached.

Similarly, the OCSP service maintains the revocation status of the certificate after it expires.
These services make it possible to check the status of the generated certificates even after expiry of the issuing CA.

6– COMMITMENT RE AVAILABILITY OF SERVICES

The following services are available 24 hours a day, 7 days a week:

- Revocation of the «Clé Real» and of the certificates it contains.
- Verification of the status of the certificates on the «Clé Real».

These services have a redundancy and a recovery plan which guarantee their availability. If the CA envisages a discontinuation of service, ADSN will continue to verify the status of the certificates contained in the «Clé Real».

The following services are available on working days, i.e. Monday to Friday, apart from public holidays, from 08.30 to 19.00:

- «Clé Real» application
- Renewal of the «Clé Real»
- The initialisation of the «Clé Real» and the generation of the certificates it contains.

7 – RESPONSIBILITIES

Each Party undertakes to perform the obligations and commitments incumbent on it under the terms of this document and, without prejudice to the provisions relating to the limits of liability, assumes the consequences arising directly or indirectly from its failure to do so. The Holder is informed that he may make any request for information or explanation from the CSN about these Terms and Conditions, a service referred to in the CP Reference (Point of Contact). The Holder will be notified in advance of any interruption due to maintenance or upgrading; the CSN cannot be held responsible in this case or in case of force majeure. The Holder recognises that the CSN may enlist subcontractors in relation to the performance of its obligations.

The liability of the CSN cannot be invoked if the failure to fulfil its obligations and commitments under the terms of this document, or if they are fulfilled incorrectly, results directly or indirectly from:

- the actions of the Holder;
- the actions of a third party;
- a case of force majeure;
- an interruption for maintenance or upgrading when the Holder has been notified in advance, apart from a case of force majeure;
- an occurrence that is beyond the reasonable control of the CSN, and which could not have been avoided by precautionary measures, alternative solutions or other commercially viable means.

The CSN may not be held liable:

- for the unauthorised or non-compliant use of the «Clé Real», the certificates contained on the «Clé Real», the associated private keys and activation data, or any other equipment or software provided that does not conform to the requirements set out in the document «Norms and Standards of the Notariat's IT system».
- for errors or inaccuracies in the information contained in the certificates, when these errors or inaccuracies result directly from the incorrect nature of the information sent by the person holding or responsible for the certificate.
- any action brought by a third party against the Holder, even if such damage was foreseeable.

8 – LIMITATION OF LIABILITY

The liability of the CSN cannot be invoked if the failure to fulfil its obligations and commitments under the terms of this document, or if they are fulfilled incorrectly, results directly or indirectly from:

- the actions of the Holder;
- the actions of a third party;
- a case of force majeure ;
- an occurrence that is beyond the reasonable control of the CSN, and which could not have been avoided by precautionary measures, alternative solutions or other commercially viable means.

The CSN cannot be deemed liable for the unauthorised or non-compliant use of the «Clé Real», the certificates contained on the «Clé Real», the associated private keys and activation data, or any other equipment or software provided.

The CSN also rejects liability for errors or inaccuracies in the information contained in the certificates, when these errors or inaccuracies result directly from the incorrect nature of the information sent by the person holding or responsible for the certificate.

In any case, the liability of the CSN is limited to direct material damage, with the exclusion of any indirect damage and, in particular, commercial loss, disruption of business, loss of profits, loss of image, loss of turnover, loss of clientele, loss of orders, loss of income, loss of contracts, loss of savings, loss of data, any commercial disruption whatsoever, or action brought by a third party against the Holder, even if this damage was foreseeable at the time of the initial application or renewal.

9 – CONFIDENTIALITY

The «Clé Real» and the PIN Code are strictly confidential. They are reserved for the exclusive use of the Holder.

The Holder agrees to take all security precautions required to this end. Under no circumstances may the Holder disclose, lend or distribute his PIN Code to a third party in any way or allow a third party to become aware of it, or record his PIN Code on any physical medium or software, in particular on paper or in a computer file. The Holder also undertakes not to transfer the «Clé Real». The Holder undertakes to meet this obligation throughout the period of validity of the «Clé Real». Should the Holder fail to meet this obligation, the Certification Agent may revoke the «Clé Real» in accordance with article 4.4.

10 – ARCHIVING

All Applicant Files are archived by the CSN or by a duly appointed third party for the preservation period required in accordance with European Regulation (EU) no. 910/2014 eIDAS. During this period, the Applicant Files may be presented by the CSN further to a requisition order from the competent authorities.

The records of events relating to the management of the «Clé Real» (application, renewal, validation, approval, revocation) are archived in SACRE for 23 years.

In the event of the CSN's activity ceasing, the Applicant Files, which are required to be the subject of an act of deposit received either by the notary in his capacity as Certification Agent or by a third party notary, will be transferred to the departmental archives or to the French national Archives for notaries from the Chambre Interdépartementale des Notaires de Paris (CINP – Interdepartmental Chamber of Paris Notaries), on completion of the legally stipulated period during which they must be preserved by the notary, i.e. 75 years, or in special cases as provided for by decree 79-1037 of 3 December 1979 as amended.

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

Data type	Retention period
Software	**Version n - 1**
Software Configurations	**Version n - 1**
Certificates of AC RealSIGN	**23 years**
LCR & Customer Certificates	**23 years**
Requests and answers OCSP	**10 years**
Technical events	**1 year**
Functional events	**23 years**
Documentation	**10 years**
Registration file (certificate applications)	**75 years**

11 - RETENTION OF EVENT LOGS

The period for the preservation of event logs is:

- one month for systems events;
- one year for technical events;
- twenty-three years for operational events.

12 – SECURITY AND PROTECTION OF PERSONAL DATA

The CSN or an authorised third party ensures the confidentiality of all Applicant Files and possibly of certain events in accordance with the stipulations of the CP Reference. The CSN undertakes to insist that this confidentiality is observed by its employees and any entity acting on its behalf. 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.

The Holder is made aware that the «Clé Réal» and its associated certificates include some of its personal data (essentially related to its identity). 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, Fax: +33 1 44 90 31 42 - 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.

13 – INTELLECTUAL PROPERTY

The use of the «Clé Real» does not confer any right of intellectual property on the Holder.
The CSN retains the ownership of the pertinent rights to all elements, regardless of the medium, such as programmes, archives, data and files belonging to it, provided to the Holder within the framework of the General Terms and Conditions.

14 – PRICES

The prices are shown in Euros and excluding tax, to which VAT is added at the rate in force at the time of invoicing.

15 – DURATION

The General Terms and Conditions come into force on the date of acceptance of the Holder. They continue to apply until the expiry of the «Clé Real», including renewal periods. They shall cease to apply in case of early revocation by one of the Parties under the terms of articles 4.3, 4.4 and 4.5.

16 – POINT OF CONTACT

Postal address:
Membre du bureau du CSN, chargé des technologies de l'information et de la communication
60 Boulevard de la Tour Maubourg
75007 Paris

Telephone: +33 1 44 90 30 00

Email: autorite-certification@notaires.fr

17 - COMPLAINTS

Any complaint must be addressed to the Certification Authority by post or email to the contact details set out in article 16: Point of contact

18 – CERTIFICATION POLICY

These General Terms and Conditions relate to:

- the Certification Policie of the CA RealSIGN (OID 1.2.250.1.78.2.1.3.1.1.4) within the framework of the qualification of Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing directive 1999/93/EC, referenced in the Trusted Service List (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf).
- To the Certification Policies of the CAs RealAUTH (OID 1.2.250.1.78.2.1.3.2.1.1) and RealCIPHER (OID 1.2.250.1.78.2.1.3.3.1.1)
- The active and future certificates of employees will no longer be considered as qualified signature certificates under eIDAS Regulation (910/2014) after the 07/12/2020 in accordance with in accordance with the aforementioned certification policies.

The CSN and ADSN are audited by an accredited company, in concordance with the procedure « Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS » in use, published by ANSSI, to verify that their certification practices conform to the requirements of Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing directive 1999/93/EC.

19 – DISPUTES

The General Terms and Conditions are governed by French law.
IN THE ABSENCE OF ANY LEGAL OR PROFESSIONAL PROVISION TO THE CONTRARY, ANY DISPUTE THAT MAY ARISE BETWEEN THE PARTIES RELATING TO THE FORMATION, PERFORMANCE AND INTERPRETATION OF THESE TERMS AND CONDITIONS AND, IN MORE GENERAL TERMS, ANY DISPUTE CONCERNING THE USE OF THE «Clé Real» SHALL BE BROUGHT BY ONE OF THE PARTIES BEFORE THE COMPETENT COURTS OF PARIS.

20 – EVOLUTIONS COMPARED TO GENERAL TERMS AND CONDITIONS OF USE VERSION 2.4

The differences between this Generals Terms and Conditions of Use of the «Clé Real» version 2.5 and the version 2.4 are:

- §4.1: modifications to the renewal procedures linked to the implementation of the new Sacre course.