

Terms and Conditions of Use

ChamberSign France CA3 Qualified eID

QCP-I-qscd



Purpose of the document:	This document describes the terms and conditions for the use of Certificates issued by the Certification Authority implemented by ChamberSign France as part of its trust services activities
Version	02
Release date	01/04/2022
Type of broadcast	Public

Warning

The present document is a work protected by the provisions of the Code of the Intellectual Property of^{er} July 1, 1992, in particular by those relating to the literary and artistic property and the royalties, as well as by all the applicable international conventions. These rights are the exclusive property of **CHAMBERSIGN FRANCE**. The reproduction, representation (including publication and broadcast), in whole or in part, by any means whatsoever (including electronic, mechanical, optical, photocopying, computer recording), without prior written permission from **CHAMBERSIGN FRANCE** or its assigns, is strictly prohibited.

Rightly, under the terms of Article L.122-4 of the Code of Intellectual Property, *"any representation or reproduction in whole or in part without the consent of the author or his successors or assigns is unlawful.*

By exception, the Intellectual Property Code authorizes, under the terms of Article L.122-5 of the said Code, on the one hand, that *"copies or reproductions strictly reserved for the private use of the copier and not intended for collective use"*; on the other hand, that analyses and short quotations for the purpose of example and illustration.

The representation or reproduction, by any means whatsoever, would constitute an infringement punishable by articles L. 335-2 and following of the Intellectual Property Code.

This document is the property of **CHAMBERSIGN FRANCE AND** may be licensed to any private or public entity for use in its own certification services.

Theme	Description
Point of Contact:	Any questions or comments regarding these CPs can be sent by email to the following address: qualite@chambersign.fr
Type of certificates issued, associated procedures and uses :	<p>Cryptographic media are qualified by the ANSSI to the level required by the eIDAS regulation.</p> <p>Private keys are not subject to any escrow or backup.</p> <p>The cryptographic media containing the private keys are only activated after entering an activation code (PIN code) which is under the full control of the certificate manager and must be kept secret.</p> <p>The activation data corresponds to the PIN codes of the cryptographic media, which are personalized by the Certificate Holders when they personalize their media and which they must not communicate to anyone. The various components of the PKI are not aware of this code at any time.</p> <p>The use is the signature on behalf of a legal entity or an application. The seal allows to attest the identity of the legal entity for which the certificate was issued. It also guarantees the integrity of the data that are signed by the seal.</p> <p>In addition, ChamberSign France may issue Test Certificates. These test certificates are identified as such in their DN by the explicit mention TEST. They are not covered by any warranty by ChamberSign and they must not be used for any other purpose than testing. At the end of the test phases, these certificates are revoked.</p> <p>Certificates issued in accordance with these Terms of Use contain the following OID: 1.2.250.1.96.1.8.2.4</p> <p>The certificates identify the following fields for legal entities:</p> <p>FieldDescription DNencoded in UTF8String countryNamecode ISO on 2 letters (cf. ISO3166-1) of the country of the competent authority with which the entity is officially registered (commercial court, ministry,...) official name of the entity (name of the head office)</p>

organizationalUnitNameNational identifier of the structure among :
-For entities based in Metropolitan France and DOM : 0002 <<SIRET number on 14 characters>>
-For entities based in New Caledonia: S540 <<RIDET number on 9 characters maximum>>.
For other entities based in a country of the European community: S<<ISO3166-1 country code on 3 digits>> <<intra-community VAT number on 14 characters maximum>>
The field can be iterated 3 times
organizationIdentifierThe official registration number of the provider according to [EN_319_412-1] clause 5.1.4. In France, this registration number can also be the prefix "SI:FR-" followed by the SIREN or SIRET number
Identifier of the entity with which the holder is linked
VAT<country code>-<intra-community VAT number>.
-NTR<country code>-<SIREN number>
locality city where the holder 's establishment is located
commonNameFQDN of the service or stamp name
serialNumbersequential 4-digit number to handle homonyms
By default, the value of this attribute is "0001". If a holder with all other DN attributes (countryName, organizationName, organizationIdentifier, organizationalUnitName and commonName) is already registered, the value of the serialNumber attribute for the new holder changes to "0002" and so on.

The certificate request files, containing the public key to be certified, are sealed with the corresponding private key.

The information concerning the structure to which the holder is attached is verified during registration (existence, validity, etc.).

The identity of the cardholder is verified through face-to-face verification of official identity documents.

Following the validation of the certificate application by the PKI registration function, the process consists in handing over to the holder a blank cryptographic medium, uniquely identified and linked to the holder, which will be personalized under the exclusive control of the holder: personalization of the activation code (PIN code), generation of the dual key in the medium, sending of the public key to the certificate generation function, downloading of the generated certificate onto the medium.

	<p>The certificate is subject to explicit acceptance by the holder at the time of delivery.</p> <p>Renewal, if authorized by regulation at the time of expiration of the certificate to be renewed, may be offered online. It must then be done before the expiration date of this certificate. It can only be carried out in the two months preceding this expiration. For the concerned certificates, the renewal is carried out without proceeding again to a face to face. The holder validates online that the information related to the certificate to be renewed is still accurate. For any other subsequent renewal or replacement following a revocation, a new certificate must be ordered following the initial registration procedure.</p> <p>The main reason for issuing a new certificate and the corresponding key pair is that the certificate has reached the end of its validity. The validity period of the certificates is 3 years. The bi-keys must be periodically renewed in order to minimize the risks of cryptographic attacks.</p> <p>A renewal can also be carried out in advance, following an event or an incident declared by the holder, the most frequent being the loss, theft or malfunction of the cryptographic medium.</p> <p>A change in the information contained in the certificate also leads to the issue of a new certificate (with renewal of the dual key).</p> <p>In all these cases the issuance of a new certificate is carried out in the same way as the initial issuance process. Only the registration phase may differ for a renewal. For example, only a few documents may not be required (e.g. the appointment of the LR).</p> <p>All revocation requests are subject to authentication of the applicant and verification of his or her authority for such a request.</p> <p>There is no suspension of certificates. Only the definitive revocation of certificates can be done. ChamberSign France ensures the availability of the revocation status at any time and beyond the validity period of the certificate by implementing the following measures:</p> <ul style="list-style-type: none">- Open-ended publication of revoked certificates in published CRLs;- Compliance of the OCSP response, revoked, in case of solicitation after the end-of-life date of the certificate. <p>The following circumstances may result in the revocation of a certificate covered by these CPs:</p> <ul style="list-style-type: none">- the certificate's private key is lost, stolen, unusable (media malfunction), compromised or suspected of being
--	--



	<p>compromised (request by the certificate manager himself);</p> <ul style="list-style-type: none"> - the information contained in the certificate is no longer valid or no longer consistent with the intended use of the certificate, before the normal expiration of the certificate; - the cryptographic algorithms used are obsolete and are no longer considered secure; - it has been demonstrated that the holder has not complied with the applicable terms and conditions of use of the certificate; - the CA certificate is revoked (which leads to the revocation of the certificates signed by the corresponding private key); - the person responsible for the certificate has changed and has not been replaced <p>The causes of revocation are never published.</p> <p>Revocation requests are processed within 24 hours of receipt of the request, 7 days a week (including weekends and holidays if the revocation is processed by the holder, the certificate manager or the legal representative), except for revocations resulting from requests to modify the holder's data.</p> <p>The revocation management function is available 24 hours a day, 7 days a week. The maximum downtime per interruption (failure or maintenance) of the revocation management function is 2 hours. The maximum total downtime per month for the revocation management function is 8 hours.</p>
<p>Limitations of use:</p>	<p>Customer agrees that ChamberSign France may retain documents relating to the proof of identification control of Registrants for the time periods set forth in the Certificate Policy as well as documents relating to the execution of this Agreement.</p> <p>Event logs are kept on site for a period of thirty (30) days. After their generation, they are archived and kept for seven (7) years.</p> <p>Registration records are archived for a period of eleven (11) years from the date of issuance of the Certificate. If Customer requests a copy of the registration file, Customer will be charged the corresponding cost.</p> <p>Certificates and CRLs are archived for a period of five (5) years after their expiration.</p> <p>If the Customer wishes to have the registration files, Certificates or CRLs stored for a longer period of time, the Customer shall make the necessary arrangements and pay for them himself.</p>
<p>Subscriber Obligations:</p>	<p>The Customer and his Legal Representative agree to comply with the provisions of these TOU.</p>

	<p>The Client and its Legal Representative are responsible for the management of the Certificates issued to the Client's employees, delegates or agents within the framework of the subscription contract, and undertakes to ensure that any Certificate holder complies with the obligations set out in these GCU and that no fraud or error is committed. In this respect, the Client and its Legal Representative shall ensure in particular that the holder :</p> <ul style="list-style-type: none"> -Communicates the information useful for the creation of the Certificate and the possible modifications during the whole duration of the Certificate; -Follows the revocation procedure described in the article "Certificate Revocation"; -keeps the confidential data and the physical medium of the Certificate secret and secure. <p>The Client and its Legal Representative undertake to provide all useful, accurate and up-to-date information for the creation and management of Certificates.</p> <p>Customer and its Legal Representative agree to inform the Home Office of any changes to the information contained in the Certificate and to submit the required supporting documentation without delay. ChamberSign reserves the right to revoke the Certificate.</p> <p>The Customer and his Legal Representative are responsible for the accuracy of the information provided and the completeness of the supporting documents required for the registration of the Certificates.</p> <p>Customer and Customer's Legal Representative acknowledge and agree that the information provided in this regard will be retained and used by ChamberSign to manage Certificates in accordance with the law and in particular the law relating to the protection of personal data.</p> <p>Customer and Customer's Legal Representative acknowledge that they are aware of ChamberSign's Certificate installation requirements. In particular, the Certificate is the subject of a tutorial available on the ChamberSign France website.</p> <p>Customer and its Legal Representative shall select the hardware and software that provides adequate security for their needs for the installation and protection of Certificates and physical media.</p> <p>The holder is responsible for verifying the validity of the certificate and the conformity of its use.</p>
<p>Obligations of verification certificates by stakeholders :</p>	<p>The following circumstances may result in the revocation of a certificate covered by these CPs:</p> <ul style="list-style-type: none"> - the certificate's private key is lost, stolen, unusable (media malfunction), compromised or suspected of being compromised (request by the certificate manager himself); - the information contained in the certificate is no longer valid or no longer consistent with the intended use of the

	<p>certificate, before the normal expiration of the certificate;</p> <ul style="list-style-type: none">- the cryptographic algorithms used are obsolete and are no longer considered secure;- it has been demonstrated that the holder has not complied with the applicable terms and conditions of use of the certificate;- the CA certificate is revoked (which leads to the revocation of the certificates signed by the corresponding private key);- the person responsible for the certificate has changed and has not been replaced <p>The causes of revocation are never published.</p>
Limitations of warranties and liability :	<p>ChamberSign France is responsible for the compliance of its Certification Policy with the requirements of the CP-Type.</p> <p>ChamberSign France assumes all liability for any consequences resulting from the failure of ChamberSign France or any of its components to comply with its Certificate Policy.</p> <p>ChamberSign acknowledges that it shall be liable for proven fault or negligence on its part or on the part of any of its components, regardless of the nature or severity of the fault or negligence, which results in the reading, alteration or misappropriation of Registrant personal data for fraudulent purposes, whether such data is contained in or in transit through the Certificate management applications.</p> <p>ChamberSign France is responsible for maintaining the security level of the technical infrastructure on which it relies to provide its services.</p> <p>ChamberSign France shall not be liable for any damages caused by the use of the Certificate beyond its authorized use.</p> <p>ChamberSign shall not be liable for inaccurate information due to false statements, false documents or failure to inform of changes in the circumstances of the Customer, Registrant, Legal Representative, or Certification Agent at the time of creation or during the life of the Certificate, whether or not the false statement, document or omission is intentional.</p> <p>ChamberSign France assumes no liability or responsibility for the consequences of delays in transmission, alteration, errors or loss of any electronic message, letter or document signed or authenticated.</p>



	<p>ChamberSign France shall not be responsible for the content of any files or transactions signed or authenticated using the Certificate, and the Customer and Registrant shall be solely responsible to third parties for the content of such submissions.</p> <p>In no event shall ChamberSign France be liable for any consequential damages such as, for example, any financial or commercial loss, loss of profit or business interruption, arising out of or in connection with the subscription or use of the Certificates issued by ChamberSign France.</p> <p>ChamberSign assumes no liability or responsibility for Registrant's use of a Certificate that does not comply with the provisions of these TOS, including, without limitation, the procedures for verifying the validity of the Certificate during a transaction.</p> <p>ChamberSign France shall not be responsible for normal wear and tear of computer media, including deterioration of information on said media due to the influence of magnetic fields.</p> <p>ChamberSign France shall not be liable for any damages, including but not limited to, any interruption or malfunction of Certificate User's services and applications.</p> <p>If the Legal Representative has purchased one or more physical media, ChamberSign France is only responsible for their physical delivery.</p> <p>Due to the constant evolution of the technology and the security levels attached to the current reference system, in case of malfunction of the physical medium or its associated pilot software, the Customer must request the revocation of the Certificate.</p> <p>ChamberSign France shall not be responsible for the use of Customer's Private Key, which is the personal responsibility of the Customer. Any damage resulting from the compromise of the Private Key is the responsibility of the Customer.</p> <p>ChamberSign shall not be liable for any unauthorized use of the Certificate unless the Customer, Legal Representative, Certification Agent or Registrant has made a revocation request in accordance with these TOU.</p>
<p>Approvals, applicable Certification Policy:</p>	<p>The applicable Certificate Policy is published at https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf</p>
<p>Data Protection Policy :</p>	<p>See Appendix 1.</p>

<p>Insurance Policy:</p>	<p>ChamberSign France has taken out insurance covering the consequences of its professional civil liability for all bodily injury, material and immaterial damages resulting from its activity.</p> <p>Under the terms of the insurance contract entered into by ChamberSign France, and subject to the limits and conditions of such contract, Registrant shall be entitled to replacement of the lost or stolen Certificate.</p>
<p>Applicable Law and Dispute Resolution :</p>	<p>In case of difficulty of any kind and before any legal proceedings, the parties undertake to implement a conciliation procedure.</p> <p>The parties undertake to meet at the initiative of the most diligent party within eight days of receipt of the letter requesting the conciliation meeting.</p> <p>The agenda is set by the party initiating the conciliation.</p> <p>Decisions, if agreed upon, have contractual value.</p> <p>This clause is legally independent of this contract. It shall continue to apply notwithstanding any invalidity, termination, cancellation or annulment of the present contractual relationship.</p> <p>Failing this, jurisdiction is expressly attributed to the French courts.</p> <p>The present GTU are governed by French law.</p> <p>This is true for the rules of substance and form, notwithstanding the place of performance of the substantive or accessory obligations.</p>
<p>Publication of information, compliance :</p>	<p>The issued certificates are eIDAS qualified.</p> <p>The root certificate for the PKI is available for download from the ChamberSign website.</p> <p>User may verify the Root Certificate's fingerprint on the secure website https://www.keymanagement.chambersign.fr or by contacting ChamberSign France by phone at 08 92 23 02 52 from metropolitan France (rate available on the ChamberSign France website) from 9:00 am to 12:30 pm and from 1:30 pm to 6:00 pm, except on Fridays at 5:00 pm, on business days.</p> <p>CRL publication points are as follows:</p>

http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl
http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl

The CA certificate can be downloaded at the following address
https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.cer

OCSP responders can be accessed at the following addresses:
http://ocsp_ca3.chambersign.fr/ChamberSign_France_CA3_Qualified_eID
http://ocsp_ca3.chambersign.tm.fr/ChamberSign_France_CA3_Qualified_eID

ANNEX 1. PROTECTION OF PERSONAL DATA

1. Personal data

1.1. Processing of personal data

1. ChamberSign believes that privacy is fundamental to our relationship with you. It is important to us to protect your privacy and that of your partners and collaborators, with regard to the information that you entrust to us.
2. The main purpose of this article is to inform you about the collection and use of your personal data by our Association, in the context of the provision of our services. The data collected by Chambersign is strictly necessary to provide our services.
3. In accordance with the European Regulation n°2016/679, known as the General Data Protection Regulation (RGPD) and the provisions of Law n° 78-17 of January 6, 1978, as amended, relating to information technology, files and freedoms, ChamberSign acts as a Data Controller concerning the collection and processing of personal data of users of its services. We are therefore responsible for compliance with the obligations arising from this text.
4. These provisions do not apply to the processing of personal data that ChamberSign may perform as a subcontractor.
5. As such, the personal data collected by ChamberSign France for the purpose of issuing and maintaining Certificates are identity data (last name, first name), as well as data related to your professional life (job title, department, professional email). ChamberSign France does not collect any sensitive data such as religion, trade union membership, racial and ethnic origins, criminal convictions or health-related data.
6. ChamberSign France collects personal data from its customers and processes it for the purposes inherent in providing its certification services. The processing of your personal data is therefore based on the respect of our contractual obligations. In this context, we collect your personal data in order to provide you with our certification services, to manage and follow the life cycle of your certificates and bi-keys (issuance, retention, renewal, revocation) or to follow our commercial relationship.
 - The provision of certification services by ChamberSign France ;
 - Management of access and operation of the certification services provided by ChamberSign France;
 - Identification of the Certificate Holder or the Certificate Manager;
 - Authentication of the Subscriber or the Certificate Manager;
 - Issuance, retention, renewal and revocation of Certificates and Half Keys;
 - Establishing statistics and measuring the quality and satisfaction of the certification services provided by ChamberSign France;
 - Follow-up of the commercial relationship: your data may be used to communicate on the news of ChamberSign France and in particular on the renewal of the products and the innovations proposed, until three (3) years after the end of our commercial relationship.



7. The information collected is mandatory. Otherwise, Chambersign France will not be able to provide certification services.
8. The data collected is only intended for use by ChamberSign France's authorized departments. Some of this data may be transferred to ChamberSign's subcontractors, who follow the same privacy policy as ChamberSign. The data transmitted will be strictly limited to the needs defined for the execution of the subcontractor's mission.
9. ChamberSign France does not and will not sell your personal data. The data processed by ChamberSign France is not transferred outside the European Union.
10. In accordance with the Référentiel Général de Sécurité (RGS Annex A2, Politique de Certification Type " Certificats électroniques de personne ", version 3 du 27 février 2014) and the present GCU, we keep your data for eleven (11) years from the date of issue of the certificate.
11. In accordance with current regulations, you have the right to access, rectify, delete, limit the processing of your personal data and object to their use.
12. In order to exercise your rights, you may contact us by mail with a copy of a signed identification document at the following address ChamberSign France - 10, Cours de Verdun Rambaud - 69002 LYON or by email at the following address: rgpd@chambersign.fr, being specified that to secure the authentication, the sending of an electronically signed email is preferred; the sending of a scanned ID (ID card, passport...) is prohibited in order to guarantee the confidentiality of the data In the absence of an electronic signature, ChamberSign France will authenticate the applicant by any appropriate means, in order to avoid any disclosure of personal data.
13. To learn more about the use of your data and the exercise of your rights under the French Data Protection Act and the RGPD, you can consult our [data protection policy](#) or contact our Data Protection Officer.
14. Furthermore, we inform you that you have the right to lodge a complaint with a control authority (CNIL): <https://www.cnil.fr/fr/agir>.

2. Cookies

15. When User visits our website, cookies are sent to User's computer, tablet or cell phone. In order to better protect User from cookies and to understand their usefulness, ChamberSign has adopted a [Cookie Usage Policy](#) which is an integral part of these Terms and Conditions and which User is encouraged to review.