PKI Disclosure Statement

ChamberSign France CA3 Qualified eID

QNCP-w-gen (QWAC)

Purpose of the document:	This document describes the terms and conditions for the use of QNCP-w-gen level Certificates issued by the Certification Authority ChamberSign CA3 implemented by ChamberSign France as part of its trust services activities
Version	00
Release date	20/02/2025
Type of broadcast	Public

Warning

Theme	Description
Point of Contact:	All information relating to the ChamberSign France Certification Authority is available on its website https://www.chambersign.fr/. It can be contacted in the following ways: - By post at the following address: Le Cours du Midi, 10, Cours de Verdun Rambaud 69002 Lyon. - By telephone on 08 92 23 02 52 (€0.45 including VAT per minute in mainland France only) - By e-mail by completing the contact form for the department concerned, accessible via the following french link: https://www.chambersign.fr/p-nous-contacter/ Certificates may be revoked by authorized persons via their revocation area, accessible via the following link: https://support.chambersign.fr/revocation-certificat-electronique/ Finally, any questions or comments regarding the Certificates Policies can be sent by email to the following address: qualite@chambersign.fr.
Type of certificates issued, associated procedures and uses:	. Keys are generated by certificate holder. The cryptographic device containing the private is under the control of the certificate holder and must be kept secret. Private keys are not subject to any escrow or backup. 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. 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. Certificates issued in accordance with these PDS contain the following OID: 1.2.250.1.96.1.8.2.5. They are defined by the Certificate Policy ChamberSign France CA3 NG Qualified eID.

The certificates identify the following fields for legal entities:

Field	Content
DN	encoded en UTF8String
countryName	ISO on 2 letters (cf. ISO3166-1) of the country of the competent authority with which the entity is officially registered (commercial court, ministry,...)
organizationName	official name of the entity (name of the head office)
organizationalUnitName	National 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
organizationIdentifier	The 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> • LEI<LEI code according ISO17442> • PSD< national payment service provider reference number>
locality	city where the holder's establishment is located
commonName	Corresponds to the name chosen by the applicant, which must not be in the format of a natural person. Example: My Company - Invoicing Department

serialNumber	sequential 4-digit number to handle homonyms By default, the value of this attribute is "0100". 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 "0101" and so on.

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

The information concerning the structure to which the holder is attached is verified during registration (existence, validity, etc.). The certificate holder must provide proof that the domain name for which it wishes to obtain a certificate actually belongs to the entity it represents.
The identity of the holder 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 the public key certified by the CA: generation of the bi-key, under the control and responsibility of the RCC, in a cryptographic device chosen by the holder, sending of the public key to the certificate generation function, downloading of the generated certificate into the device.

The certificate is subject to explicit acceptance by the holder at the time of delivery.

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.

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 1 year. The bi-keys must be periodically renewed in

	order to minimize the risks of cryptographic attacks. 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. A change in the information contained in the certificate also leads to the issue of a new certificate (with renewal of the dual key). 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). All revocation requests are subject to authentication of the applicant and verification of his or her authority for such a request. 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: - 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. The following circumstances may result in the revocation of a certificate covered by these CPs: - the certificate's private key is lost, stolen, unusable (device malfunction), compromised or suspected of being compromised (request by the certificate holder himself); - 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 The causes of revocation are never published.

	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 online), except for revocations resulting from requests to modify the holder's data. 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.
Limitations of use:	Use of the Holder's Private Key and Certificate must remain strictly limited to authenticate web servers. 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. Event logs are kept on site for a period of thirty (30) days if the Client has made a request in paper format. After their generation, they are archived and kept for eleven (11) years. 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. Certificates and CRLs are archived for a period of five (5) years after their expiration. If the Client 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.
Subscriber Obligations:	The Client and his Legal Representative agree to comply with the provisions of these PDS. 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 PDS and that no fraud or error is committed. In this respect, the Client and its Legal Representative shall ensure in particular that the holder: - Communicates the information useful for the creation of the Certificate and the possible modifications during the whole duration of the entire lifespan of the Certificate; - Follows the revocation procedure described in the article "Certificate Revocation"; - keeps the confidential data and the physical device of the Certificate secret and secure.

	The Client and its Legal Representative undertake to provide all useful, accurate and up-to-date information for the creation and management of Certificates. The Client and its Legal Representative agree to inform the Registration 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. The Client and his Legal Representative shall ensure that the certificate is used under the exclusive control of his Holder, and undertake to inform ChamberSign or the relevant Registration Office in the event of loss, theft, compromise of the certificate or disclosure of the PIN code or password. Where applicable, he undertakes to no longer use the compromised Certificate, and ChamberSign reserves the right to revoke it latter. The Client 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. 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. 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. 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. The holder is responsible for verifying the validity of the certificate and the conformity of its use.
Obligations of verification certificates by stakeholders:	Stakeholders verify and respect the use for which a Certificate has been issued. Stakeholders check that the Certificate issued by ChamberSign France is referenced at the level of security and for the trusted service required by the application. For each of the Certificates in the Certification chain, from the Holder's Certificate to the root Certification Authority, the Stakeholders verify the status of the Certificate and in particular the digital signature of ChamberSign France, issuer of the Certificate in question, and check the validity of this Certificate.

	Stakeholders must make sure that the certificate used applies to the domain name of the web service concerned. Stakeholders verify and comply with these obligations as expressed in the applicable Certification Policy. Stakeholders must verify that the certificates on which they are going to base their trust have not been revoked. This verification is done by consulting the CRLs available via the CSF website at the following address: https://support.chambersign.fr/lcr/, or by querying the online certificate status service (OCSP) which includes a "certificate revoked" response after the certificate's end of life date. Revoked certificates remain in the CRL even after their original expiry date. The following circumstances may result in the revocation of a certificate covered by these PDS: - the certificate's private key is lost, stolen, unusable (device malfunction), compromised or suspected of being compromised (request by the certificate holder himself) ; - 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 The causes of revocation are never published.
Limitations of warranties and liability:	ChamberSign France is responsible for the compliance of its Certification Policy with the requirements of the CP-Type. 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. 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.

	ChamberSign France is responsible for maintaining the security level of the technical infrastructure on which it relies to provide its services. ChamberSign France shall not be liable for any damages caused by the use of the Certificate beyond its authorized use. 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. 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. ChamberSign France shall not be responsible for the content of any files or transactions signed or authenticated using the Certificate, and the Client and the Holder shall be solely responsible to third parties for the content of such submissions. 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. ChamberSign assumes no liability or responsibility for Holder's use of a Certificate that does not comply with the provisions of the PDS, including, without limitation, the procedures for verifying the validity of the Certificate during a transaction. 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. 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. If the Legal Representative has purchased one or more physical media, ChamberSign France is only responsible

	for their physical delivery. 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 Client must request the revocation of the Certificate. ChamberSign France shall not be responsible for the use of Holder'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. ChamberSign shall not be liable for any unauthorized use of the Certificate unless the Client, Legal Representative, Certification Agent or Holder has made a revocation request in accordance with these PDS.
Approvals, applicable Certification Policy:	The applicable Certificate Policy is published at: https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Data Protection Policy :	See Appendix 1.
Insurance Policy:	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. 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.
Applicable Law and Dispute Resolution :	In case of difficulty of any kind and before any legal proceedings, the parties undertake to implement a non court dispute resolution procedure. The parties undertake to meet at the initiative of the most diligent party within eight (8) working days of receipt of the letter requesting the non court meeting. The agenda is set by the party initiating the non court meeting. Decisions, if agreed upon, have contractual value. 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. Failing this, jurisdiction is expressly attributed to the French courts.

	The present PDS are governed by French law. This is true for the rules of substance and form, notwithstanding the place of performance of the substantive or accessory obligations.
Publication of information, compliance :	The issued certificates are eIDAS qualified. The root certificate for the CA is available for download from the ChamberSign website. User may verify the Root Certificate's fingerprint on the secure website https://pc.chambersign.fr/ca3/index.html 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. CRL publication points are as follows: http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_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_NG_Qualified_eID http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID The certificate and CRL profiles comply with the ETSI EN 319 412-4 & 319 412-5 standard. The certificates produced contain the following qualified extensions: id-etsi-qcs-QcCompliance id-etsi-qct-web QcEuPDS. The list of certificates of compliance with the standards is available on the website at the following address: https://www.chambersign.fr/attestations-de-conformite-certification/ The national trusted list is available via the following link: https://cyber.gouv.fr/la-liste-nationale-de-confiance

ChamberSign
Autorité de certification

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 ChamberSign, 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. These provisions do not apply to the processing of personal data that ChamberSign may perform as a subcontractor.

4. 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.

5. 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 services, to manage and follow the life cycle of your certificates and bi-keys (issuance, retention, renewal, revocation) to manage access to and the functioning of your Customer Area or to follow our commercial relationship.

6. The information collected is mandatory. Otherwise, Chambersign France will not be able to provide certification services. 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.

7. The subcontractors likely to access your personal data are as follows:
    - Advertising agency based in France, responsible for the transfer of the newsletter by email;
    - Digital Services Company (ESN) based in France, responsible for providing the first level of technical support;
    - IT hosting company based in France, responsible for hosting the ChamberSign website;

- Archiving company based in France responsible for archiving certificate application files for the legally required period of time;
- Chambers of Commerce and Industry that are ChamberSign partners responsible for verifying identities, validating files and issuing certificates;
- Public and private entities that are ChamberSign partners responsible for issuing certificates for their employees, customers or members;
- ChamberSign's trusted service provider partner responsible for providing the signature of the parties when ordering certificates;
- Cheque management service provider responsible for cashing cheques;
- ChamberSign's trusted service provider partner responsible for verifying the validity of identity documents

8. ChamberSign France does not and will not sell your personal data. The data processed by ChamberSign France is not transferred outside the European Union.

9. In accordance with our standards and the present PDS, we keep your data for eleven (11) years from the date of issue of the certificate.

10. In accordance with current regulations, you have the right to access, rectify, delete, limit the processing of your personal data, object to their use, as well as a right to portability and to define guidelines on the fate of your data after your death.

11. 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. 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.

12. In case of reasonable doubt, ChamberSign reserves the right to ask you to provide a copy of your identity document by a secure means, it being specified that this document will not be reused for purposes other than your authentication in the context of the request to exercise your rights, and will not be kept beyond the time required for this purpose.

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, which is an integral part of these PDS, or contact our Data Protection Officer at rgpd@chambersign.fr.

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

1. When User visits our website, cookies are sent to User's computer, tablet or cell phone, subject to the expression of his or her consent from the cookie management banner displayed on the first page visited, and allowing him or her to accept all cookies, refuse them all, or customize their collection. 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 PDS and which User is encouraged to review.