PKI Disclosure Statements

ChamberSign France CA3 Qualified eID

QCP-double_usage

Purpose of the Document:	This document is related to the hierarchy of certification authority ChamberSign France "ChamberSign France CA3". It is the PKI disclosure statement for end-users certificates attached to this hierarchy
Version	00
Date of release	19/02/2021
Diffusion	Public

Written by	Quality Department
Verified by	Technical Department
Approved by Stéphane GASCH	

Record of versions	
Version	Nature of the evolutions
00	Creation

Warning

ChamberSign
Autorité de certification

Statement types	Statement descriptions
TSP contact info:	Any questions or comments about these CPS can be sent by email to the following address: qualite@chambersign.fr
Certificate type, validation procedures and usage:	Each application for a Certificate is subject to a face-to-face meeting between the Subscriber, an EDA agent, a representative of ChamberSign France or a Certification Agent. The subject's cryptographic media are qualified by ANSSI to the level required by the [eIDAS] and [RGS] regulations. The cryptographic media containing the private keys of the subjects are only activated after the entry of an activation code (PIN code) fully controlled by the subjects and which the subjects must keep secret. Cryptographic media containing the private keys of the subjects must perform the authentication or signature function for the legitimate subjects only and protect the private key against any use by third parties. The activation data corresponds to the PIN codes of the cryptographic media, which are defined by the subjects when customising their media and which must remain under their exclusive control. The various components of the PKI have no knowledge of this data at any time. Usages are: - electronic signature data by the subject of the certificate (to sign). Such electronic signature brings, besides the authenticity and integrity of data and signed, the manifestation of consent of the signatory for the content of these data. - authentication of subjects from remote servers or to other people. It may be authentication through access control to a server or application, or origin authentication data within email. Authentication is not a signature on a legal sense because it does not mean that the subject gives his consent to the data exchanged (the non-repudiation guarantee is not available). For information, the use of a dual-use certificate may introduce a potential security risk. This vulnerability depends particularly on the environment implemented by the certificate subject. If the subject's environment is under control and is trusted, then there is no specific security impacts to consider. However, if the environment used is not deemed safe, it is the subject to ensure that the operation he is doing is an authentication operation or a signature operation. The subject must be aware that it is possible to use the certificate to conduct a signature instead of authentication and vice versa. If the subject of the environment is not deemed safe, it is recommended that it ensures both that the key pair is used only for dual-use certificate which was issued to him and secondly that the application implementing the authentication mechanisms or signature uses the fair practice of the certificate. Moreover, ChamberSign France may be forced to issue test certificates. These test certificates are identified as

	such in their DN by the explicit mention TEST. They are covered by any warranty by ChamberSign France and they must never be used for purposes other than for testing purposes. In the late stages of testing, these certificates are revoked. Certificates issued in accordance to these Terms of service contain the following OID: 1.2.250.1.96.1.8.2.8 The certificates identify the following information for natural persons: field Description DN encoded in UTF8String countryName ISO code on 2 letters (see ISO3166-1) of the country of the competent authority with which the entity is officially registered (commercial court, ministry, etc.) organizationName official name of the entity (corporate name of the registered office) organizationalUnitName national identifier of the structure among: • For entities based in mainland France and overseas territories: 0002 << N ° SIRET on 14 characters >> • For entities based in New Caledonia: S540 << N ° RIDET on 9 characters maximum >> • For other entities based in a country of the European Community: S << 3-digit country ISO3166-1 code >> << 14-digit EU VAT number >> The field can be iterated 3 times organizationIdentifier The official registration number of the service provider in accordance with [EN_319_412-1] clause 5.1.4. In France, this registration number may also consist of the prefix "SI: FR-" followed by the number SIREN or SIRET Identifier of the entity with which the subject is linked VAT <country code> - <intracommunity VAT number> • NTR <country code> - <SIREN number> locality city where the subject's establishment is located surName Name of the subject givenName Firstname1 (, firstname2, firstname3 ...) The different names are mentioned in the order indicated on the identity document presented at the time of registration and the copy of which is kept in the registration file. commonName Firstname1 (, Firstname2, Firstname3, ...) NAME The different names are mentioned in the order indicated on the identity document presented at the time of registration and the copy of which is kept in the registration file. title if applicable, function of the subject within its structure

	serialNumber 4-digit sequential number to process homonymy cases By default, the value of this attribute is "0001". If a subject with all other attributes of the DN are identical (countryName, organizationName, organizationIdentifier, organizationalUnitName, and commonName) has already been registered, the value of the serialNumber attribute for the new subject changes to "0002" and so on. Certificate request files, containing the key pair to be certified, are sealed using the corresponding key pair. Information regarding the structure on which the subject is attached are subject to verification upon registration (existence, validity, ...). The identity of the subject or person in charge of certicate is verified through verification of official identity documents during a face-to-face. Following validation of the certificate request file by the registration function, the process consists to give to the subject or the person in charge of the certificate the pulic key signed by the CA: generation of the key pair, under control of the subject or the person in charge of the certificate, into a cryptographic media (software or hardware) chosen by the subject, sending the key pair to the certificate generation function, downloading the generated certificate on the media. The certificate is accepted explicitely by the subject or person in charge of certificates at the delivery time. The subject or the person in charge of certificates accepted his certificate by signing with his new certificate an acceptance form online. The first renewal, if authorized by the regulations at the time of expiry date of the certificate to be renewed, can be performed online if it takes place before the expiry date of the corresponding certificate. The subject or the person in charge of certificates confirms that information related to certificate renewal is always accurate. The next renewal is carried out following the initial registration procedure. The renewal after revocation is carried out according to the initial registration procedure. The main cause for the issuance of a new certificate and the corresponding key pair is the end of validity of the certificate. The validity period of certificates provided by ChamberSign France is three (3) years. The key pairs must be effectively periodically renewed to minimize the risk of cryptographic attack. A renewal can also be made in advance, following a declared event or incident by the subject or the person in

	charge of certificates, the most frequent being the loss, theft or malfunction of cryptographic media. In this case the renewal is, for the subject or the person in charge of certificates, to redo an initial application. A modification of the information contained in the certificate also involves the issuance of a new certificate (with renewal of the key pair). 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. Only a few documents may not be requested (deed of appointment of the legal representative for example). Any revocation request is subject to an applicant authentication and verification of his authority. There can be no certificate suspension. Only the final certificate revocation can be performed. ChamberSign France ensures the availability of the revocation status at any time and beyond the certificate validity period by implementing the following measures: • Publication without a time limit of revoked certificates published in the CSF ; • Compliance of the OCSP response, revoked in case of solicitation after the date of the end of life of the certificate. The following circumstances may cause the revocation of a certificate: • the certificate key pair is lost, stolen, unusable (malfunction of support), compromised or suspected compromise (request of the subject itself) ; • information or attributes of the subject contained in the certificate is no longer valid or no more consistent with the intended use of the certificate, this before the normal expiry of the certificate ; • cryptographic algorithms used are obsolete and are no longer considered safe ; • it has been shown that the subject has not respected the applicable terms of use of the certificate ; • the CA certificate is revoked (which results in the revocation of certificates signed by the corresponding key pair) ; • the subject no longer meets the professional requirements (cessation of activity, death). The causes of revocation are never published. Revocation requests are processed within 24 hours after receiving the request, 7 days / 7 (weekends and holidays included if the revocation is processed by the subject, the person in charge of certificates or natural person mandated to represent the subject), excluding consecutive revocations to requests for modification of the subject

	data. The revocation management function is available round the clock, 7 days a week. The maximum duration of downtime per interruption (failure or maintenance) of the revocation management function is 2 hours. The maximum total duration of downtime per month of revocation management function is 8 hours.
Reliance limits :	The Client agrees that ChamberSign France retains documents for proof of identification control of the subject for the periods provided in the Certificate Policy and the documents relating to the conclusion of this contract. The 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. The original registration files are archived with archivers third party for a period of eleven (11) years from the issuance of the certificate. If Client's request to obtain a copy of the registration dossier, the Client will be charged the corresponding cost. Certificates and CRLs are archived for a period of seven (7) years after their expiry. If the Client wishes that the registration files, the Certificates or the CRLs are kept for a longer period of archiving, he will have to make the necessary ones and to take the cost himself at his charge.
Obligations of subscribers:	The Client and its Legal Representative undertake to respect the provisions of the PDS. The Client and its Legal Representative are responsible for the management of Certificates issued to employees, delegates or agents of Client under the subscription agreement and undertake to ensure that any Certificate's subject violating obligations under the Terms and that no fraud or error is committed. As such, the Client and its Legal Representative will ensure in particular that the leader: - communicates via the contact point identified herein, the information to create the certificate and any changes during the duration of the certificate; - respects the revocation procedure described in Article 9 Revocation of the Certificate; - keeps secret and secure way, confidential data and the physical support of the Certificate. The Client and its Legal Representative undertake to provide all relevant information, accurate and updated for the creation and management of certificates. The Client and its Legal Representative undertake to inform the home Registration Authority of any changes to

	information contained in the certificate by mail with the required supporting documents without delay. The previous certificate will be revoked and a new certificate containing the updated information will be issued. The Client and its Legal Representative vouch for the accuracy of the information provided and completeness of the supporting documents required for registration of the Certificates. The Client and its Legal Representative recognize and accept that the information provided thereunder are kept and used by ChamberSign France to manage certificates as provided by law and in particular those relating to the protection of personal data. The Client and its Legal Representative acknowledge being informed of the conditions of installation of Certificates ChamberSign France. In particular, the certificate is the subject of a tutorial available on the website of ChamberSign France. The Client and its Legal Representative choose hardware and software offering security in line with their requirements for the installation and protection of Certificates and physical media.
Certificate status checking obligations of relying parties:	Acceptors certificates must verify the non-revocation of the certificates on which they will base their confidence. This verification is done by checking the CRL available via the website ChamberSign France, or by querying certificate status online service (OCSP) that incorporates a response "revoked certificate" from the date of end of life certificat. The revoked certificates are still present in the CRL even after their original expiration date. The service is available 24 hours / 24 and 7 days / 7 via the website ChamberSign France. The maximum duration of downtime per interruption (failure or maintenance) of the information based on the status of certificates is 4 hours. The maximum total duration of downtime per month of the information function on certificate status is 16 hours. The maximum response time of the OCSP service received a query on the status of a certificate is 10 seconds from the receipt of the request by the server.
Limited warranty and disclaimer / Limitation of liability:	ChamberSign France is responsible for the compliance of its Certificate Policy, the requirements issued by the model of CPS. ChamberSign France assumes any harmful consequences resulting from non-compliance with its Certificate Policy by itself or one of its components.

	ChamberSign France acknowledges liability in case of proven misconduct or negligence of itself or one of its components, whatever their nature and severity, which would result in reading, alteration or misuse of personal data subjects for fraudulent purposes, these data are contained in transit or in the Certificates 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 can not be held liable for damage caused by use of the Certificate beyond the limits of the authorized use. Responsibility of ChamberSign France can not be held liable for inaccurate information due to false declarations, false documents or no information of changes in the situation of the Subject, the Legal Representative, or natural person mandated to represent the subject when creating or valid certificate, which the false declaration, false documents or the omission is intentional or not. ChamberSign France assumes no obligation or responsibility for the consequences of delays in transmission, alteration, errors or loss of any email, letter or document, signed or otherwise authenticated. ChamberSign France does not in any way be held responsible for the contents of files or transactions signed or authenticated using the certificate, the Client and the subject is only vis-a-vis third parties responsible for the content of these shipments. ChamberSign France will in no case liable for indirect damage such as, for example, any financial or commercial loss, loss of income or operating, finding their origin or resulting subscription or inherent in the use of certificates issued by ChamberSign France. ChamberSign France assumes no obligation or liability for the use by the Holder of a Certificate not in accordance with the PDS, especially regarding the validity of control procedures certificate during a transaction. Otherwise, ChamberSign France can not be responsible for phenomena related to normal wear of computer media, including the deterioration of the information given on the said media due to the influence of magnetic fields.

	ChamberSign France can not be held liable for such damage related to a disruption or malfunction of services and applications for Certificates User. If the Legal Representative has acquired one or more physical media, ChamberSign France is responsible only for their physical deliverance. Due to the constant evolution of technology and levels of security attached to the standards in force in case of malfunction of the physical media or its associated driver software, the Client must request revocation of the Certificate. ChamberSign France can not be responsible for the use of subject Private Key, who has personal responsibility. Any damage related to the Compromise of the Private Key is the Client. ChamberSign France can not be held liable due to illicit use of the Certificate once the Client, the Legal Representative, the Certification Agent or the subject has not made a revocation request in accordance with the Terms.
Applicable agreements, SPC, PO Box :	The applicable certification policy is published at the following address: https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Privacy policy :	See Appendix 1
Refund policy :	ChamberSign France has subscribed for all of the physical, material and immaterial arising from its business insurance covering the consequences of professional liability. Under the insurance contract by ChamberSign France, and the limits and conditions of this contract, the subject will benefit from the replacement of lost or stolen certificate.
Applicable law, complaints and dispute resolution:	In case of difficulty of any kind and before any legal proceedings, the parties undertake to implement a conciliation procedure. The parties agree to meet at the initiative of either party within eight days from receipt of the letter requesting conciliation meeting. The agenda is set by the party that takes the initiative of reconciliation. The decisions, if adopted by mutual agreement, guaranteed.

	This clause is legally independent of this Agreement. It continues to apply despite the possible invalidity, resolution, termination or extinction of these contractual relationships. Otherwise, jurisdiction is assigned to the French courts. These Terms are governed by French law. This is so for the substantive rules and the rules of form and this, notwithstanding the places of performance of the substantive or accessory obligations.
TSP and repository licenses, trust marks and audit:	Certificates issued qualified eIDAS. The root certificate of the PKI be downloaded from the website ChamberSign. The user can check the fingerprint of the root certificate on the https://www.keymanagement.chambersign.fr secure site or by contacting ChamberSign France by phone. CRL publishing points are: 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 the following address: https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.cer The OCSP responders can be accessed at: http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_Qualified_eID http: // ocsp-ca3. chambersign.tm.fr/ChamberSign_France_CA3_Qualified_eID

1.1.APPENDIX 1. PROTECTION OF PERSONAL DATA

1. PERSONAL DATA

1.2.1.1 PROCESSING OF PERSONAL DATA

1. For ChamberSign France, the protection of personal data is fundamental because it reflects the relationship we have with you. It is important to us to protect your privacy and that of your partners and collaborators, with regard to the information 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, within the framework of the provision of our services. The data collected by Chambersign is therefore strictly necessary for the performance of our services.

3. In accordance with the European Regulation n°2016/679 known as the General Regulation on Data Protection (RGPD) and the provisions of Law n° 78-17 of January 6, 1978 as amended, relating to data processing, data files and liberties, ChamberSign acts as Data Controller concerning the collection and processing of personal data of the users of its services. We are therefore responsible for compliance with the obligations arising from this text.

4. The present stipulations do not concern the processing of personal data that ChamberSign may be required to operate as a subcontractor.

5. As such, the personal data collected by ChamberSign France for the purposes of issuing and storing the Certificates are identity data (surname, first name), as well as data relating to your professional life (function, service, 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 the personal data of its customers and processes it for purposes inherent to the provision of its certification services. The processing of your personal data is therefore based on compliance with our contractual obligations. In this context, we collect your personal data in order to provide you with our certification services, to manage and monitor the lifecycle of your certificates and bi-keys (issue, conservation, renewal, revocation) or to monitor our commercial relationship.
- The provision of certification services by ChamberSign France;
- The management of access and operation of the certification services provided by ChamberSign France;
- The identification of the Certificate Holder or Certificate Manager;
- Authentication of the Certificate Holder or Certificate Manager;
- Issuance, conservation, renewal and revocation of Certificates and Key Bi-keys;
- The establishment of statistics and the measurement of the quality and satisfaction of the certification services provided by ChamberSign France;
- The follow-up of the commercial relationship: your data may be used to communicate on ChamberSign France news and in particular on the renewal of products and new products offered, up to three (3) years from 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 authorized services. Part of this data may be transmitted to ChamberSign France's subcontractors, who respect the same privacy policy as ChamberSign France. The transmitted data 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 also not transferred outside the European Union.

10. In application of the General Security Standard (RGS Annex A2, Certification Policy Type "Electronic Certificates of Persons", version 3 of February 27, 2014) and these Terms and Conditions, we keep your data for eleven (11) years from the date of issue of the certificate..

11. In accordance with the Regulations in force, you have a right of access, rectification, deletion, limitation of processing and opposition.

12. In order to exercise your rights, you can contact us by mail with a copy of a signed identity document at the following address ChamberSign France- 10, Cours de Verdun Rambaud - 69002 LYON or by e-mail at the following address: rgpd@chambersign.fr, it being specified that to secure the authentication, the sending of an e-mail signed electronically is privileged; the sending of a scanned identity document (identity card, passport...) is prohibited in order to guarantee the confidentiality of the data. In the absence of an electronic signature, ChamberSign France will proceed to the authentication of the applicant by any appropriate means 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. In addition, we inform you that you have the right to file a complaint before a supervisory authority (CNIL): https://www.cnil.fr/fr/agir.

2. Cookies

15. When the User visits our website, cookies are sent to his/her computer, tablet or cell phone. In order to better protect the User from cookies while understanding their usefulness, ChamberSign has adopted a Cookie Usage Policy which is an integral part of these Terms and Conditions, which can be viewed on our Site and which the User is expressly invited to view.