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	01
Date of release	06/02/2019
Diffusion	Public

Written by	Aurélie JABTKO
Verified by	Stéphane GASCH
Approved by Stéphane GASCH	

Record of versions	
Version	Nature of the evolutions
01	Creation

Warning

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 subject may freely choose cryptographic media. However, this media must help to ensure exclusive control by the subject on its key pair and on the implementation of the corresponding certificate. The subject contractually commits to ChamberSign France on compliance. Keys pairs of the subjects are not subject to any sequestration or backup. Cryptographic media containing the keys pairs's subjects must ensure the function of authentication or signature for the legitimate subject only and protect the key pair against unauthorized use by third parties. 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: 1.2.250.1.96.1.8.2.6

	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).

	Dans tous ces cas la délivrance d'un nouveau certificat est réalisée de manière identique au processus de délivrance initiale. Seule la phase d'enregistrement peut différer pour un renouvellement. Par exemple seuls quelques documents peuvent ne pas être demandé (acte de nomination du RL notamment). 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 one (1) month. 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 certifiat. 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

ChamberSign
Autorité de certification

1.1.APPENDIX 1. PROTECTION OF PERSONAL DATA

1. PERSONAL DATA

1.2.1.1 PROCESSING OF PERSONAL DATA

1. Personal data collected by ChamberSign France for the purpose of the issuing and preservation of the certificates will only be processed for the purposes for which they were collected.

2. ChamberSign France declares and warrants that the personal data collected in the context of the present conditions as well as the treatments for which it is responsible or, as the case may be, as a subcontractor, are processed in accordance with the provisions of Law no. 78-17 of 6 January 1978 relating to data, the files and freedoms (amended by the law N ° 2018-493 of June 20, 2018 relating to data, files and freedoms and various provisions concerning the protection of personal data) and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46 / EC.

3. The Customer, the Legal Representative, the Agent of Certification and the Subject are informed that in accordance with the regulation in force, ChamberSign France, as a data processor, or according to the case, the subcontractor, implements a processing of personal data concerning them with the following conditions:
- the provision of certification services by ChamberSign France;
- the management of the access and the operation of the certification services provided by ChamberSign France;
- identification of the Subject;
- authentication of the Subject;
- the issuance, preservation, renewal and revocation of the Certificates and the keys pairs;
- compilation of statistics and the measurement of quality and the satisfaction of the certification services provided by ChamberSign France.

4. The collected data are mandatory. Otherwise, ChamberSign France will be able to provide the certification services.

5. ChamberSign France ensures the confidentiality and the security of data collected within the framework of the present ones. Nevertheless, the data contained in the Certificate are by nature public.

6. The data processed by ChamberSign France are not transferred outside the European Union.

7. The collected data are only intended for the authorized services of ChamberSign France. These data could be transmitted to the technical operator of ChamberSign France, which respects the same policy of confidentiality as ChamberSign France. The data are hereby preserved for the duration of the article 22.

8. The Legal Representative, the Certification Agent and the Subject are informed by these general conditions of use that they have a right of access, rectification, deletion, limitation of

treatment, opposition and the right to define guidelines regarding the fate of his or her data after their death, in accordance with the Data Protection Act of 7 January 1978 relating to data, files and freedoms (as amended) as well as to EU Regulation no. 2016/679 of the European Parliament of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

9. These same persons have the right to oppose and limit the processing, the right to the portability of the data, as well as the right to oppose that the data be used for commercial prospecting purposes.

10. In order to exercise their rights, the Legal Representative, the Certification Agent and the Subject may write to the GDPR referent of ChamberSign France by mail accompanied by a copy of an ID signed at the following address: ChamberSign France - 3, Place de la Bourse - 69002 LYON or else:
- By email to the Data Protection Officer at the following address: rgpd@chambersign.fr, it being specified that to secure the authentication, the sending of an electronically signed email is privileged; the sending of a scanned identity document (identity card, passport ...) is forbidden 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, this to avoid any disclosure of personal data.

11. In the event of ChamberSign France's failure to comply with this clause, these persons have the right to lodge a complaint with the National Commission for Data Processing and Freedoms (CNIL).

12. These obligations are also fulfilled in the confidentiality charter, accessible from the ChamberSign website, by clicking on the following link: https://www.chambersign.fr/p-charte-de-confidentialite.html.

2. Sub-contracting

13. In the context of the performance of the certification services, ChamberSign France may be required to process personal data on behalf of the Client.
14. In this context, the Client acts as data processor and ChamberSign France as its subcontractor within the meaning of the regulations applicable in France in the field of the protection of personal data.

15. As such, ChamberSign France undertakes to process the personal data entrusted by the Client in compliance with the applicable regulations in France and in accordance with the contractual terms and conditions agreed by the Client data processor and ChamberSign France.