PKI Disclosure statement

V 1.2

Confidentiality level : public

Datasure

History of document is provided as follows

Numéro de version	Date	Commentaire
1.0	July 9th 2024	Initial document
1.1	Sept. 8th 2024	Minor updates / review direction
1.2	Nov.11th 2024	Scope change Auditor's remarks taken into account

1 TSP Contact Info

Any request related to the service shall be sent to the following address. :

Datasure
Certification Authority
8 rue Alfred Maurel
34120 PÉZENAS, FRANCE

Datasure can also be contacted with the contact form available on the Internet website : https://www.datasure.net

2 Certificate type, validation procedures and usage

2.1 Certificates available

Datasure issues qualified certificates according to European standard ETSI EN 319 411-2 and ANSSI procedure, and certificates related to other standards. Certificates are offered to the general public (private companies, public entities, professionals, private persons, etc.), at the conditions published on the CA website. All certificates are signed with at minimum a hashing function of SHA-256.

2.2 Certificates policy

2.3 Certificate usages

The certificate usage depends on the type of certificate

Case Q1. QCP-n-QSCD (smartcard) 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	The private key associated to the certificate allow to create Qualified Electronic Signature (QES).
Case Q2. QCP-n-QSCD (remote) 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	

Case Q3. QCP-n (software) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	The private key associated to the certificate allows to create Advanced Electronic Signature based on qualified certificate.
Case Q4. QCP-l-QSCD (remote) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	The private key associated to the certificate allows to create Qualified Electronic Seal (Qseal).
Caes Q5. QCP-l-QSCD (smartcard) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Case Q6. QCP-l (software) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	The private key associated to the certificate allows to create Advanced Electronic Signature based on qualified certificate.
Case Q7. QCP-l (timestamping) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	The private key associate to the certificate allows Datasure TSA to issue qualified timestamp.
Case C1. Certificate signature NCP+ natural personal (remote) 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	The private key associated to the certificate allows to create Advanced Electronic Signature.
Case C2. Authentification certificate NCP for organization (software) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	The private key associate to the certificate allows an application to authenticate itself with a TLS.
Case C3. Certificate LCP natural person (remote) 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	The private key associated to the certificate allows to create Advanced Electronic Signature.
Case C4. Certificate LCP Legal person (software) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	The private key associated to the certificate allows to create Advanced Electronic Signature.
Case B1. Biometry certificate (remote) 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	The private key associated to the certificate allows to create Advanced Electronic Signature.

2.4 Validation procedure

The validation procedure depends on the type of certificate

Case Q1. QCP-n-QSCD (smartcard) 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Initial validation procedures include : - French PVID identification scheme
Case Q2. QCP-n-QSCD (remote) 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Initial validation procedures include : - French PVID identification scheme
Case Q3. QCP-n (software) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Initial validation procedures include : - French PVID identification scheme
Case Q4. QCP-l-QSCD (remote) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Initial validation procedures include : - French PVID identification scheme
Casz Q5. QCP-l-QSCD (smartcard) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Initial validation procedures include : - French PVID identification scheme

Case Q6. QCP-l (software) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Initial validation procedures include : - French PVID identification scheme
Case Q7. QCP-l (timestamping) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Internal use for Datasure only
Case C1. Certificate signature NCP+ natural personal (remote) 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Initial validation procedures include : - Remote video identification scheme including Face-match, liveness check and ID document authenticity check.
Case C2. Authentification certificate NCP for organization (software) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Initial validation procedures include : - Remote video identification scheme including Face-match, liveness check and ID document authenticity check.
Case C3. Certificate LCP natural person (remote) 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Initial validation procedures include : - Valid ID document upload
Case C4 Certificate LCP Legal person (software) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Initial validation procedures include : - Valid ID document upload
Case B1. Biometry certificate (remote) 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Authentication with SMS OTP.

3 Reliance limits

Certificate and associated are limited to the usage specified in this PDS and in the CP/CPS.s
Audit logs related to the TSP, including registration information, are stored for 7 years after the expiration of the certificate, in application of ANSSI guidelines.

4 Subscriber obligations

The subscriber shall :

- Communicate exact and up-to-date information when requesting or renewing certificate;
- Respect key usages of the private key and corresponding certificate ;
- Notify the CA in case of change of the information within its certificate;
- Perform, without delay, a revocation request in case of compromise (or suspicion) of the private key or activation data.

Additional obligations applies for certain type of certificates.

Case Q1. QCP-n-QSCD (smartcard) 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	• Use of the QSCD smartcard provided by Datasure • Protect the private key with appropriate means, typically by storing securely the smartcard.;

	• Protect the activation data, in particular by not sharing the PIN Code.
Case Q2. QCP-n-QSCD (remote) 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	• Non applicable. The obligation of QSCD usage is covered by Datasure Signature service.
Case Q3. QCP-n (software) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	• Protect the private key with appropriate means, typically by ensure access control to the PKCS#12 signature file and by choosing a strong password in line with state of art. • The keypair and CSR generation shall be compliant with the recommendation of standard ETSI TS 119 312
Case Q4. QCP-l-QSCD (remote) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	• Non applicable. The obligation of QSCD usage is covered by Datasure Signature service.
Caes Q5. QCP-l-QSCD (smartcard) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	• Use of the smartcard QSCD provided by Datasure • Protect the private key with appropriate means, typically by storing securely the smartcard.; • Protect the activation data, in particular by not sharing the PIN Code.
Case Q6. QCP-l (software) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	• Protect the private key with appropriate means, typically by ensure access control to the PKCS#12 signature file and by choosing a strong password in line with state of art. • The keypair and CSR generation shall be compliant with the recommendation of standard ETSI TS 119 312
Case Q7. QCP-l (timestamping) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	• Subscriber must comply with standard ETSI EN 319421 and timestamping French qualification procedure requirements.
Case C1. Certificate signature NCP+ natural personal (remote) 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	• Non applicable. The obligation of HSM usage is covered by Datasure Signature service.
Case C2. Authentification certificate NCP for organization (software) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	• Protect the private key with appropriate means, typically by ensure access control to the PKCS#12 signature file and by choosing a strong password in line with state of art. • The keypair and CSR generation shall be compliant with the recommendation of standard ETSI TS 119 312
Case C3. Certificate LCP natural person (remote) 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	• Non applicable
Case C4. Certificate LCP Legal person (software) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	• Protect the private key with appropriate means, typically by ensure access control to the PKCS#12 signature file and by choosing a strong password in line with state of art. • The keypair and CSR generation shall be compliant with the recommendation of standard ETSI TS 119 312
Case C5. Biometry certificate (remote) 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	• Non applicable

5 Certificate status checking obligations of relying parties

It is recommended that relying parties, in addition to the validation of the signature, of the eSeal or of the TLS challenge protocol, verify the validity of the issued certificate. Data allowing to verify the validity are provided by Datasure.

Datasure provides :

- The complete certificat chain up to the root CA
- The list of revoked certificates (CRL). CRL are compliant with IETF RFC 5280 standard.

The publication service, under normal circumstances, is available 24/24 and 7/7 under SLA condition depicted in the CP/CPS. In addition to the CRL, Datasure provides an OCSP service.

The relying party using a certificate issued by Datasure shall also check that the certificate is appropriate for the usage intended, in particular, the relying party shall:

- Verify and respect the intended usage of the certificate,
- For each certificate of the chain of trust, for end-entity certificate until the Root CA, verify the electronic signature of the issuing CA and check the validity of the certificate (validity period, revocation status)
- Check and respect the relying parties obligation mentioned in this document and within the CP/CPS.

Technical verification can be done in an automated manner by standard tool such as Acrobat Reader™ or the SD-DSS Open-Source library (provided the EU Commission) or OpenSSL.

6 Limited warranty and disclaimer/Limitation of liability

6.1 Limitation of usage

Datasure does not check the compliancy of its services with the law and Regulation applicable to the subscriber. In particular, Datasure is not accredited to manage healthcare data or sensible data related to National Security. Datasure is not responsible for any usage of the service not in adequation with the applicable Law and Regulations.

6.2 Limit of responsibility

Datasure is not responsible in case of usage not compliant with the conditions expressed in this PDS, the Terms & conditions and the CP/CPS, or any of contractual document between Datasure and the subscriber. In particular, the responsability of Datasure is not engaged in case of divergence of the level provided by the service, as mentioned in the present document, Terms and Conditions and CP/CPS and the security needs expected by the subscriber or relying parties.

Datasure certificates issuance service is limited to the provisioning of a technical service to the subscribers and relying parties. Datasure responsibility cannot be engaged in case of illegal usage or in case of usage non compliance with applicable law and regulations.

Datasure is not responsible of any damage and consequence, direct and indirect, caused by the divulgation by the subscriber of its authentication means or activation data.

Datasure is not responsable for any indirect damage caused by the use of the service. In any case, the responsability is limited to the amount paid for the issuance of the certificate or for the creation of the eSignature or eSeal.

7 Applicable agreements, CPS, CP

The following Certificate policy are associated with the certificates

Case /type of certificate	OID	Applicable Standard / regulation
Case Q1. QCP-n-QSCD (smartcard QSCD)	1.3.6.1.4.1.58753.2.1.1.1.1.1.1	ETSI EN 319411-2 QCP-n-QSCD eIDAS qualification
Case Q2. QCP-n-QSCD (remote QSCD)	1.3.6.1.4.1.58753.2.1.1.1.1.1.3	ETSI EN 319411-2 QCP-n-QSCD eIDAS qualification
Case Q3. QCP-n (software)	1.3.6.1.4.1.58753.2.1.1.1.1.1.2	ETSI EN 319411-2 QCP-n eIDAS qualification
Case Q4 and Q5. QCP-l-QSCD (remote QSCD or smartcard)	1.3.6.1.4.1.58753.2.1.1.1.1.2.1	ETSI EN 319411-2 QCP-l-QSCD eIDAS qualification
Case Q6. QCP-l (software)	1.3.6.1.4.1.58753.2.1.1.1.1.2.2	ETSI EN 319411-2 QCP-l eIDAS qualification
Case Q7. QCP-l (timestamping)	1.3.6.1.4.1.58753.2.1.1.1.1.2.3	ETSI EN 319411-2 QCP-l eIDAS qualification
Case C1 Certificat signature NCP+ natural person	1.3.6.1.4.1.58753.2.1.1.1.2.1.1	ETSI EN 319411-1 NCP+
Case C2. Authentification certificate NCP Legal person (software)	1.3.6.1.4.1.58753.2.1.1.1.2.2.1	ETSI EN 319411-1 NCP

Case C3. Certificat LCP individual (remote)	1.3.6.1.4.1.58753.2.1.1.1.2.1.2	ETSI EN 319411-1 LCP
Case C4. Certificat LCP Legal person (software)	1.3.6.1.4.1.58753.2.1.1.1.2.2.2	ETSI EN 319411-1 LCP
Case B1. Biometry certificate	1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Non applicable

8 Privacy policy

Datasure privacy policy is applicable

9 Refund policy

No refund policy is applicable

10 Applicable law, complaints and dispute resolution

Applicable law are the French Republic law and regulations.
In case of complaints and dispute, parties will try an amicable settlement before starting any suit.
The competent jurisdiction is the Commerce Judicial Court of Béziers (France).

11 TSP and repository licenses, trust marks, and audit

The CA is regularly audited by an accredited body in accordance with standard EN 319 403 to ensure its compliance with the eIDAS Regulation and related standards.

_____