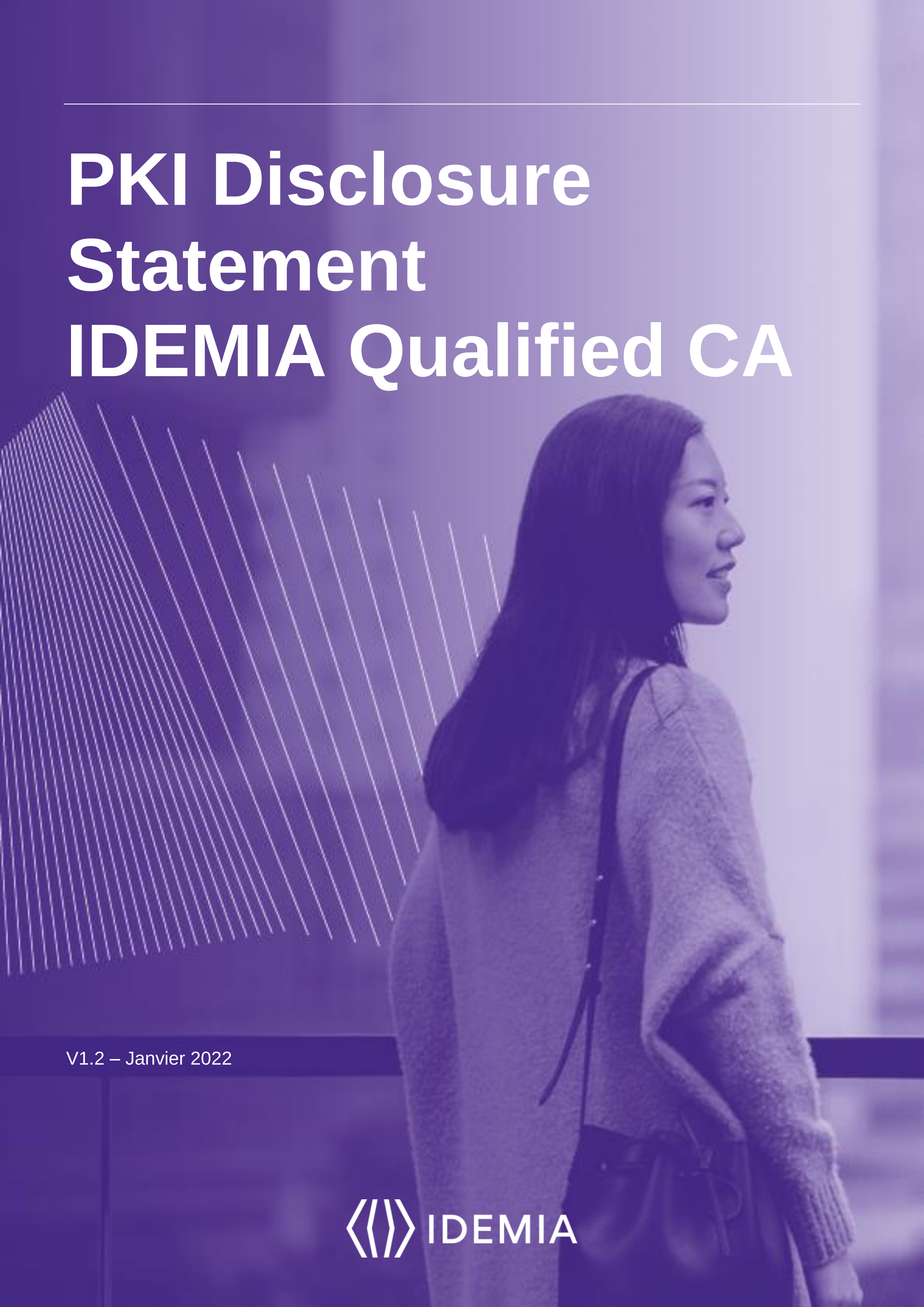


PKI Disclosure Statement IDEMIA Qualified CA

V1.2 – Janvier 2022

Introduction

This document constitutes the PKI disclosure statement (PDS) for the IDEMIA's Qualified CA ("AC qualifiée IDEMIA" in French).

It contains all relevant information about services provided as described in details by Certificate Policy / Certification Practice Statement document (hereinafter CP / CPS).

Version number	Author	Comment
V1.0	PRO	Initial version
V1.1	PRO	Update CPS URL
V1.2	JMD	Transfer to DOCAPOSTE Trust & Sign

1 / TSP Contact Info

This section provides the contact information regarding the PKI.

As of 1 January 2022, the electronic signature activities of IDEMIA have been transferred to DOCAPOSTE Trust & Sign, including the infrastructure and staff in charge of this PKI.

DOCAPOSTE Trust & Sign now operates under an authorization agreement with IDEMIA this PKI for the existing customers under the same terms and conditions as before. This agreement runs until the operations are transferred without service interruption to a new infrastructure under the identity of DOCAPOSTE Trust & Sign.

For any question concerning the operation of the service during this period, you can contact DOCAPOSTE Trust & Sign:

DOCAPOSTE Trust & Sign	
Personne à contacter	PKI Information contact
Adresse postale	DOCAPOSTE Trust & Sign 45-47 Boulevard Paul Vaillant Couturier 94200 Ivry-sur-Seine
Numéro de téléphone	+33 1 56 29 70 01
Adresse email	info@docaposte.fr
Site internet:	http://pki.trust.idemia.io

Revocation requests can be made when:

- The business activity ends with the certification authority or by client's decision;
- Compromise, suspicion of compromise, theft or loss of the means of reconstitution of the private key;
- Non-compliance revealed during audit.

2 / Certificate type, validation procedures and usage

The CA produces the following types of certificates.

Family	OID	Compliance	Subjects and limitation
Time-stamping certificates	1.3.6.1.4.1.54916.1.2.4.1	*ETSI EN 319 411-2 QCP-l*	Only issued to IDEMIA Time-stamping Unit of the IDEMIA qualified Time-stamping Authority.
OCSP	N/A	N/A	Usage limited to the verification of revocation status of the certificates.

Certificate policy is available at the following URL:

Qualified Certificate Policy	http://pki.trust.idemia.io/policies/idemia-eidas-cp-qualified-ca.pdf

2.1 > Time-stamping certificates

These qualified EU certificates (compliant to the *ETSI EN 319 411-2 QCP-l standard*) are exclusively issued to the time-stamping units of the IDEMIA Qualified Time-stamping authority. Each certificate is delivered accordingly to the certificate policy and had a duration of 6 years.

2.2 > OCSP certificates

These certificates are exclusively issued and used by IDEMIA Qualified CA for the signature of the OCSP responses of its OCSP responder. Each certificate is delivered accordingly to the certificate policy and had a duration of 1 year.

3 / Reliance limits

3.1 > Specific Reliance Limits

There are no specific reliance limits on the certificates.

3.2 > Limits regarding certificate usages

Certificate usage is limited to the use cases described in this PDS and the associated CP.

3.3 > Archival period of records

Registration information is kept 7 years after the certificate expiration.

Certificates, CRL (if any) and OCSP responses are kept at least 7 years after their expiration date.

4 / Obligations of subscribers

The subscriber, as an individual or as the representative of the company, has the following obligations:

- Providing correct information for the certificate issuance;
- Consenting to let IDEMIA archiving personal data that are necessary to certificate issuance for the period mentioned above in that document. The subscriber provides also a similar consent for the data necessary for the revocation process and for a transfer to an authorized third party in case of CA end-of-life;
- Notifying the CA in case of loss or comprise of its certificate, its activation data or in case of change of the information stored within the certificate, during the validity period of the certificate;
- Consent to delegate to IDEMIA the operation of its cryptographic device. IDEMIA is then, by delegation, of ensuring the following subscriber's obligation:
    - Obligation to use of the key pair within the limits described in the CP.
    - Prohibition to use the private key for non-authorized usages.
    - Prohibition to use the private key after the expiry of the associated certificate or the revocation of the associated certificate.
    - Obligation to generate and use the private key within a secured cryptographic device or a qualified signature/seal creation device (QSCD), if applicable.

5 / Certificate status checking obligations of relying parties

Certificate users should, before relying on the certificate, check the revocation status of the certificate chain using the OCSP method. The address of the OCSP responder is the following:

OCSP responder	http://pki.trust.idemia.io/ocsp/idemia-eidas-qualified-ca

6 / Limited warranty and disclaimer/Limitation of liability

IDEMIA is not responsible for any damage resulting from the use or linked to the use of its service by the subscriber. The subscriber only is responsible for the use of the service.
IDEMIA is not liable for any damage resulting from an error within the certificate if this error is due to the subscriber or has not been reported by the subscriber to IDEMIA.

7 / Applicable agreements

See Section 2 / Certificate type, validation procedures and usage.

8 / Privacy Policy

Personal data is managed by the TSP and its information systems according to the French and European regulation, in particular, the EU Data Protection Act and the Regulation (EU) 2016/679 of the European parliament and of the council 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, and repealing Directive 95/46/EC (also known as “General Data Protection Regulation”).
Registration information is, among others, personal data.

See section 3.3 > Archival period of records for the retention time of registration information.

9 / Refund Policy

Not applicable.

10 / Applicable law, complaints and dispute resolution

After having contacted the TSP (see Section 1 / TSP Contact Info), in the event of a dispute between the parties arising from the interpretation, application and / or performance of the contract and the failure to reach an amicable agreement between the parties hereto, exclusive jurisdiction is vested in the Nanterre Commercial Court.

The applicable legal system is the French one.

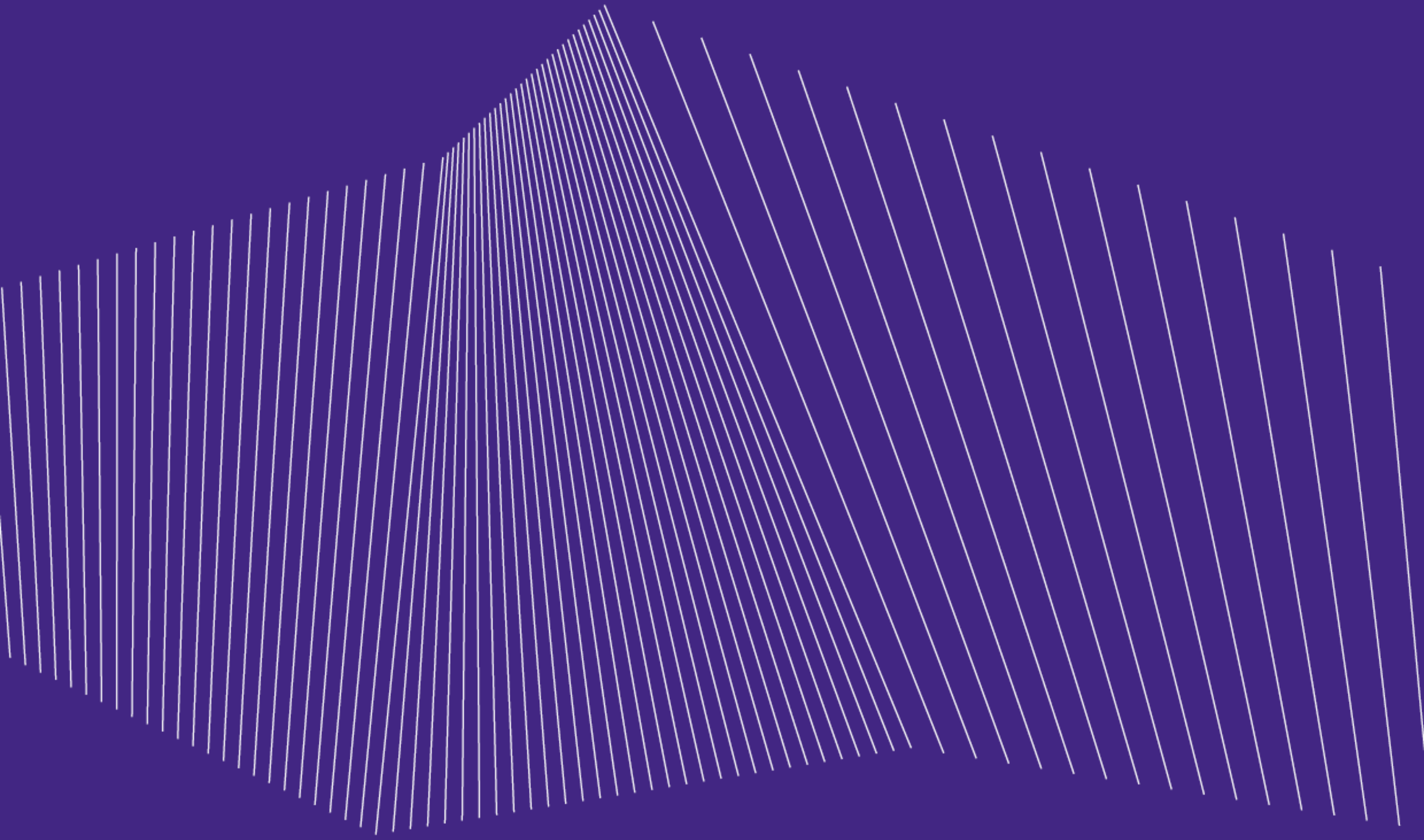
11 / TSP and repository licenses, trust marks, and audit

The list of standards for compliance is described in section 2 / Certificate type, validation procedures and usage.

The CA is declared by the French Supervisory body following its qualification procedure. This qualification is only pronounced after a successful audit performed by an accredited conformity assessment body.

After the decision of qualification, the French Supervisory body publishes the service and associated certificate CA in the trusted list available at the following URL:

FRANCE: Trusted list	www.ssi.gouv.fr/eidas/tl/fr/



IDEMIA

www.idemia.com