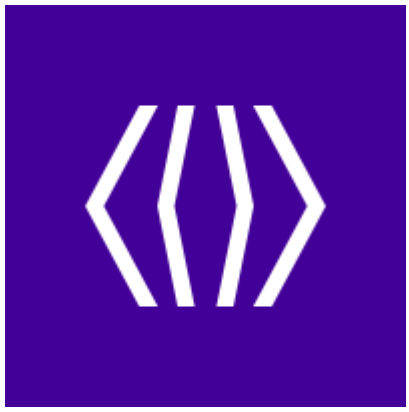
PKI disclosure statements

DICTAO Service CA



Version 1.2
Publication date: 2019-01-31

Section 1. Introduction

This document constitutes the PKI disclosure statement (PDS) for the “DICTAO Service CA” certificates.

Section 2. TSP contact info

> *The name, location and relevant contact information for the CA/PKI (name of responsible person, address, website, info mail, faq, etc.), including clear information on how to contact the TSP (Trust Service Provider) to request a revocation.*

Safran Identity & Security / DSA	
Contact person:	PKI Information contact
Postal address:	IDEMIA Identity & Security France 2, Place Samuel de Champlain 92400 Courbevoie France
Telephone number:	+33 1 78 14 70 00
Email address:	info@idemia.com
Website:	http://trust.dictao.com

Revocation requests can be made when:

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

Section 3. Certificate type, validation procedures and usage

> *A description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage.*
>
> *Any limitations on its use.*

Whether the policy is for certificate issued to the public.
CP being applied (including OID and short summary).

There are several kinds of certificates.

Table 1 – Certificates families

Family	OID	Conformance	Subjects
E-seal	1.2.250.1.195.3.1.1.2	ETSI EN 319411-1 NCP	▪ Legal persons
Timestamping	1.2.250.1.195.3.1.2.2		▪ Timestamping units of the 'DICTAO Service CA' service
OCSP	1.2.250.1.195.3.1.3.1	None	▪ OCSP responder of the 'DICTAO Service CA'

3.1. E-seals certificates

These EU certificates (NCP) are exclusively issued to legal persons to generate "electronic seals" in the sense of the eIDAS Regulation *(Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market)*.

E-seal certificates are used in an online contracting process to digitally sign documents in a PDF format on behalf the legal entity. This process, designed by the delegated registration authority of the TSP, respect the requirements of the conformance.

Each certificate is delivered accordingly to the certificate policy (CP) and had a duration of 3 years.

Certificate policy is available at the following URL: http://trust.dictao.com/pc.html

3.2. Timestamping certificates

These EU certificates (NCP) are exclusively issued to the timestamping units of the DICTAO Service CA.

Requirements are the same as e-seals certificates as described above.

3.3. OCSP certificates

These certificates are exclusively issued and used by the DICTAO Service CA for the signature of the OCSP responses of its OCSP responder.

Section 4. Reliance limits

> *The reliance limits, if any.*

There are no specific reliance limits on the certificates.

> *Indication that the certificate is only for use with digital signatures or seals.*

See previous section.

> *The period of time which registration information and TSP event are maintained (and hence are available to provide supporting evidence).*

Registration information is kept 10 years.

Certificates, CRL and OCSP responses are kept at least 8 years after their expiration date.

Technical logs are kept 7 years.

Section 5. Obligations of subscribers

> *The description of, or reference to, the critical subscriber obligations.*
>
> *The subscriber's obligations […], including whether the policy requires use of a secure cryptographic device.*

In the following, “the owner” is:

- The physical person (certified accountant) whose identity is in the issued certificate (“subject”).
- The physical person related to the legal person whose identity is in the issued certificate (“subject”).

1. Upon registration, the owner must provide genuine and exact information to the TSP.
2. The owner shall use the key pair in accordance with any limitations expressed in the present PDS.
3. The owner shall prevent unauthorized use of his/her subject's private key.
4. The owner shall maintain the subject's private key under the subject's sole control. In particular, he/she must not share the subject’s private key activation code with anyone.
5. The owner shall only generate and use the subject's private key(s) for cryptographic functions within the secure cryptographic device. Doing such

ensures that the subject keys are generated using an algorithm as specified in *ETSI TS 119 312* for the uses of the certified key as identified in the CP, and that key length and algorithm are as specified in *ETSI TS 119 312* for the uses of the certified key as identified in the CP during the validity time of the certificate.

6. The owner shall notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
   - The subject's private key has been lost, stolen, potentially compromised;
   - Control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; or
   - Inaccuracy or changes to the certificate content.
7. Following compromise, the owner will immediately and permanently discontinue to use the subject's private key.
8. The owner will no longer use the subject's private key once he/she has been informed of its revocation or that of the issuing CA.

Section 6. Certificate status checking obligations of relying parties

> *The extent to which relying parties are obligated to check certificate status, and references to further explanation.*
>
> *Information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate.*

Certificate users must, before relying on the certificate, check the revocation status of the certificate chain using one of the following methods.

Table 2 – OCSP responder

OCSP Responder & issuing CA certificate	
Service CA	▪ OCSP : http://trust.dictao.com/ocsp/dictao-service-ca ▪ CA : http://trust.dictao.com/ca/dictao-service-ca.cer

Table 3 – CRL distribution points

CRL distribution point	
Service CA	▪ CRL dp : http://trust.dictao.com/crl/dictao-service-ca.crl

Section 7. Limited warranty and disclaimer/Limitation of liability

Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.

Limitations of liability.

No specific limitation.

Section 8. Applicable agreements

Identification and references to applicable agreements, CPS, CP and other relevant documents; CP being applied.

See Section 3.

Section 9. Privacy policy

A description of and reference to the applicable privacy policy.

The period of time during which registration information is retained.

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 above for the retention time of registration information.

Section 10. Refund policy

A description of and reference to the applicable refund policy.

Not applicable.

Section 11. Applicable law, complaints and dispute resolution

Statement of the choice of law, complaints procedure and dispute resolution mechanisms (anticipated to often include a reference to the International Chambers of Commerce's arbitration services).

The procedures for complaints and dispute settlements.

After having contacted the TSP (see Section 2), 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.

The applicable legal system is the French one.

Section 12. TSP and repository licenses, trust marks, and audit

Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.

If the TSP has been certified to be conformant with a CP, and if so through which scheme.

The link toward the Trusted List of the country within which the TSP is operated.

Tableau 4 – TSP conformance and Trusted List

Service CA	▪ ETSI EN 319 401 ▪ ETSI EN 319 411-1 NCP ▪ Adobe Approved Trust List

AATL technical requirements are available at the following URL:

https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html