PKI Disclosure Statement

CERTIFICATION AUTHORITY

« CDC - LEGALIA » AUTHENTICATION OR SIGNATURE

Version	Date	Description	Authors	Society
1.8	21/0/2017	Creation in compliance with eIDAS	Vincent COUILLET	Caisse des Dépôts

Document Classification	Reference
Public broadcasting	OID : 1.2.250.1.5.1.1.1.2.3
	OID : 1.2.250.1.5.1.1.1.3.3

Table of Contents

1. INTRODUCTION

Caisse des Dépôts et Consignations (CDC) has positioned itself as an electronic certification service provider for its employees (Groupe Caisse des Dépôts) and its Clients, offering services for digital trust, allowing client to secure all their electronic exchanges. Certificates of CDC employees and Clients are generated by different Certification Authorities, depending on the "CDC - RACINE" root certification authority. The whole constitutes a hierarchy of certification.

This document is the CDC-LEGALIA PKI Disclosure Statement. This document is not a substitute for AC CDC – LEGALIA's CP / CPS, which defines all the PKI commitments and practices for Enterprise and / or Administration type stakeholders with an Authentication profile (OID 1.2 .250.1.5.1.1.1.2.3) or a Signature profile (OID 1.2.250.1.5.1.1.1.3.3). The purpose of this document, in accordance with the applicable standard, is to summarize the main points of CA CDC - LEGALIA 's practices for certificate holders and third parties.

2. CONTACT POINTS

Requests for information or questions concerning the Certification Authority should be addressed to the Application Manager:

- By mail: Caisse des Dépôts - Responsible for electronic certificates - DRCI - 56, rue de Lille - 75356 PARIS 07 SP FRANCE
- By e-mail: igc@caissedesdepots.fr

To contact the Registration Authority:

- By mail: Caisse des Dépôts - AE "CDC – LEGALIA" - DCB - 15, quai Anatole France - 75356 PARIS 07 FRANCE
- By e-mail: ae-dbr@caissedesdepots.fr
- By phone: +33 (1) 58 50 58 58

The points of contact are also specified in the contract forms and in the Terms and Conditions.

3. CERTIFICATE TYPE, VALIDATION PROCEDURE AND USE OF CERTIFICATES

Certificate Family	Public Certificate	OID	Description
Qualified electronic signature	**yes**	1.2.250.1.5.1.1.1.3.3	**Qualified electronic signature certificate, as defined in the eIDAS European Regulation and in accordance with ETSI TS 319 411-2 QCP-n-QSCD. Certificates issued on token Qualified as QSCD material by ANSSI, with creation of keys on the token by the CSP. RSA keys of size 2048 bit and validity of the certificate of 3 years. Key use is limited to the qualified electronic signature.**
Authentication NCP+	**yes**	1.2.250.1.5.1.1.1.2.3	**Certificate of authentication conforming to ETSI TS 319 411-1 NCP + issued on token hardware qualified QSCD by ANSSI, with creation of keys on the token by the CSP. RSA keys of size 2048 bit and validity of the certificate of 3 years. Use of the key limited to authentication.**

4. UTILIZATION LIMITS

Any use other than the ones described in the CP / CPS and the above section are prohibited.

Certificates shall not be used beyond their period of validity

For legal and regulatory compliance purposes, the traces of the operations carried out by CDC - LEGALIA are retained. In particular:

- The registration files are kept for 10 years.
- The issued certificates and information status (CRL, OCSP) are kept at least 8 years after their expiry date.
- The technical traces ensuring the accountability of the shares are kept 7 years after their generation.

5. OBLIGATIONS OF CERTIFICATE HOLDERS

The obligations of the holders are described in the subscription agreement as well as in the CP / CPS. We recall them below for information purposes (the obligations contained in the subscription agreement and in the CP / CPS).

- THE SUBSCRIBER undertakes to comply with the procedures described in the e-mail sent by the AUTHORITY OF CERTIFICATION for the withdrawal of the CERTIFICATE. It undertakes to respect the following rules:
    - Protect his USB KEY or his CHIP CARD by the PIN CODE he defined himself when withdrawing his CERTIFICATE.
    - Do not entrust a third party with the PIN CODE, lend it to a third party or let a third party know about it.
    - Regularly change the PIN CODE of the CERTIFICATE.
    - Keep the PIN CODE secret after its change and protect its PIN CODE from any COMPROMISE by loss, theft or computer capture. THE SUBSCRIBER commits to ensure the security of the computer station on which it uses the CERTIFICATE.
    - Use its CERTIFICATE within the scope of the applications defined in the Certification Policy.
    - Inform the CERTIFICATION AUTHORITY in the event of a known or suspected COMPROMISE of its private key and any alteration, loss or theft of its USB KEY or CHIP CARD and immediately request the REVOCATION OF THE CERTIFICATE by specifying the name, Name and e-mail address of the SUBSCRIBE concerned by the incident.
    - Do not include its PIN CODE on any physical medium, such as paper.
    - Perform the procedures in accordance with the User's Manual which has been sent by email with PIN.
    - Store your USB KEY or CHIP CARD after using the CERTIFICATE in a secure manner to avoid any risk of identity theft.
- SUBSCRIBER agrees to respect the technical prerequisites described in Annex V of the contract.
- The SUBSCRIBER acknowledges being informed that, in general, the AUTHORITY OF CERTIFICATION does not ensure the archiving of signed documents and messages using a CERTIFICATE issued by the AUTHORITY OF CERTIFICATION.
- The SUBSCRIBER undertakes to provide all relevant information during the creation of the CERTIFICATE and during the period of validity of the CERTIFICATE. The information provided must be accurate and accompanied by the supporting documents provided for in this document.
- The SUBSCRIBER is responsible for informing the THIRD USER of the obligation to verify the CERTIFICATE and the SIGNATURE associated with the exchange, the message and the electronic document.
- THE SUBSCRIBER is fully responsible for the use of its USB KEY or its SMARTCARD, its PIN CODE. THE SUBSCRIBER recognizes and accepts the

transactions thus initiated and their characteristics, the proof of which is constituted by the electronic registration.

- The SUBSCRIBER undertakes to verify that the USB KEY or the SMARTCARD on which he will use his CERTIFICATE is approved by the CERTIFICATION AUTHORITY.
- The Subscriber agrees to use his certificate only for the purpose for which it is intended (Authentication or Signature).
- THE SUBSCRIBER undertakes to take all appropriate measures to ensure the security of the USB KEY or the SMARTCARD in his custody.
- In the event of a malfunction of the electronic certificate medium at the time of its initialization, in accordance with the provisions of the CA - CDC LEGALIA ad hoc operating manual, the SUBSCRIBER undertakes to contact the TECHNICAL ASSISTANCE OF THE CERTIFICATION AUTHORITY as soon as possible.
- Any modification of information indicated as compulsory at the time of registration must be notified in writing to the AUTHORITY OF CERTIFICATION and accompanied by the required supporting documents.
- THE SUBSCRIBER agrees to cease using a CERTIFICATE following the expiry of the CERTIFICATE, following a request for REVOCATION or following the notification of the REVOCATION of the CERTIFICATE, for whatever reason.
- THE SUBSCRIBER undertakes to revoke the CERTIFICATE, specifically if one of the following reasons is realized:
    - Information concerning him, appearing in the CERTIFICATE, become inaccurate (e-mail address, name, etc.).
    - Change of function rendering the use of the CERTIFICATE unnecessary.
    - Suspicion of fraudulent use.
    - Failure to comply with the rules governing the use of the CERTIFICATE, as set out above.

The application for REVOCATION of the CERTIFICATE will be made by:

- Online at the URL specified in the contract.
- Written in accordance with the model provided in the form "REVOCATION TYPE OF CERTIFICATE FORM" downloadable on the site http://www.caissedesdepots.fr/confiance.html. By e-mail or by phone to the REGISTRATION AUTHORITY

6. OBLIGATIONS OF USERS AND CERTIFICATE VERIFICATION

The obligations of the holders are described in the subscription agreement as well as in the CP / CPS. We recall them below for information purposes (the obligations contained in the subscription agreement and in the CP / CPS).
The persons or entities for which documents signed by a certificate produced in the course of the service
1.can verify the validity of the electronic signature and the certificate used to create the signature and all the elements of the certification chain up to the root certificate. In particular, they must check the status of each of the chain's certificates and ensure that they have not been revoked.

2.Take into account all limitations, in particular limitations of use, as described in the CGUs annexed to the contract as well as in the Certification Policy / Declaration of Associated Certification Practices and, where applicable, any Contractual agreements limitations between CDC -LEGALIA and the certificate user.

To this end, CDC - LEGALIA publicly makes all the elements available to all certificate users (certificate chain, CRL, links to the OCSP servers) making it possible to verify the validity of the certificates issued to the following address: http://www.caissedesdepots.fr/confiance

7. GARANTEE AND RESPONSIBILITY LIMITATIONS

These limitations are set out in the Terms & Conditions annexed to the subscription agreement. The main limitations are recalled here to indicate

- The CDC is not responsible for the preservation or protection of the private key of the SUBSCRIBER, who is solely responsible for this. Consequently, all damages related to the COMPROMISE of the private key of a SUBSCRIBER are the responsibility of the CLIENT.
- The CDC undertakes to make every effort to ensure that its site is accessible at all times and that the integrity of the information relevant to the audit is protected. However, the CDC reserves the right, without its liability being engaged, to suspend access to the said site when it considers that an event likely to affect its functioning or integrity so requires for the duration necessary for the planned intervention.
- Under no circumstances shall the CDC intervene in any way whatsoever in the relations between the CLIENT and the SUBSCRIBERS holding CERTIFICATES, or between the CLIENT and the CERTIFICATES' THIRD PARTIES.
- Subject to applicable public policy provisions, the CDC shall not be liable for any unauthorized or unauthorized use of certificates, associated private keys and activation data, CRLs and any other equipment or software available. In particular, the CDC denies responsibility for any damage resulting from:
  - Use of key pair for a purpose other than those provided for;
  - The use of revoked or expired certificates;
  - The non-revocation of a certificate involving the use of the certificate and the bi-key by an unauthorized third party;
  - A case of force majeure as defined by the French courts.
- The CDC also disclaims its liability for any damage resulting from errors or inaccuracies in the information contained in the certificates where such errors or inaccuracies result directly from the erroneous nature of the information communicated by the Holder or the Certification Representative

8. APPLICABLE DOCUMENTS

The applicable documents are:

- CP / CPS of CDC - LEGALIA CA
- Subscriber agreement including the Terms & Conditions

These documents are available at the following address.
http://www.caissedesdepots.fr/confiance

9. PRIVACY POLICY

Personal data relating to the CERTIFYING REPRESENTATIVE or SUBSCRIBER transmitted and held by the CDC may not be disclosed without the prior consent of the data subject. However, they may be communicated to the subcontractor or to any subsidiary of the CDC, in compliance with the provisions of law number 78-17 of January 6 1978.

10. REFUND POLICY

No special requirements.

11. APPLICABLE LAW

This service is subject to French law.
In matters relating to a contract, any dispute concerning the validity, interpretation or performance of this Certification Policy shall be submitted to the relevant courts within the jurisdiction of the Paris court of appeal.

12. CONFORMITY AUDIT

The Certification Authority is audited in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2 on a regular basis by an accredited independent assessment body (see Section 8 of the CP / CPS).