CERTIFICATION AUTHORITY CDC - LEGALIA

CERTIFICATION POLICY

AUTHENTICATION TEMPLATE

OR

SIGNATURE TEMPLATE

Version	Date	Description	Author	Company
0.1	04/08/2009	Certification Policy	Alain BOUILLE	Caisse des Dépôts
1.0	23/11/2009	Definition of CA names	Alain BOUILLE	Caisse des Dépôts
1.1	02/04/2010	Change of OID	Cédric CLEMENT	Caisse des Dépôts
1.2	28/05/2010	Update after first deployments	Cédric CLEMENT	Caisse des Dépôts
1.3	22/07/2010	Unification of authentication or signature CPs	Cédric CLEMENT	Caisse des Dépôts
1.4	01/12/2010	Update following RGS audit	Cédric CLEMENT	Caisse des Dépôts

Document classification	Reference
Public circulation	Authentication OID: 1.2.250.1.5.1.1.1.2.2 Signature OID: 1.2.250.1.5.1.1.1.3.2

CONTENTS

1 INTRODUCTION

1.1 General presentation

The Caisse des Dépôts et Consignations (CDC) has positioned itself as a provider of electronic certification services for its employees, customers and partners, offering digital trust support services to enable them broadly to make all their exchanges secure. The certificates of CDC's employees, partners and customers are generated by various Certification Authorities dependent on the root Certification Authority "CDC RACINE". Together these authorities constitute a certification hierarchy.

This certification policy defines the requirements relating to the CA CDC - LEGALIA for Corporate and/or Administration type Holder certificates with an **Authentication** profile (OID 1.2.250.1.5.1.1.1.2.2) or a **Signature** profile (OID 1.2.250.1.5.1.1.1.3.2).

This document has been drawn up on the basis of the standard state Certification Policy (v2.3). The Certification Authority CDC - LEGALIA is qualified under the Référentiel Général de Sécurité (RGS) (General Security Database) at level **.

1.2 Identification of document

Authentication profile

For authentication certificates, the OID number of this document is **1.2.250.1.5.1.1.1.2.2**. The OID number of this document obeys the following naming principles:

- Iso(**1**)
- member-body(**2**)
- f(**250**)
- type-org(**1**)
- cdc (**5**)
- Direction des Risques et du Contrôle Interne (Risk and Internal Control Department) (**1**)
- Digital trust programme (**1**)
- Certification Policies (**1**)
- CDC - LEGALIA Certification Policy - Authentication (**2**)
- Version (**2**)

In the event of subsequent changes to this document, the OID number will be modified as regards its latest "Version" value and become 1.2.250.1.5.1.1.1.2.**3** in its next revision.

Signature profile

For signature certificates, the OID number of this document is **1.2.250.1.5.1.1.1.3.2**. The OID number of this document obeys the following naming principles:

- Iso(**1**)
- member-body(**2**)
- f(**250**)
- type-org(**1**)
- cdc (**5**)
- Direction des Risques et du Contrôle Interne (Risk and Internal Control Department) (**1**)
- Digital trust programme (**1**)
- Certification Policies (**1**)

- CDC - LEGALIA Certification Policy - Signature (**3**)
- Version (**2**)

In the event of subsequent changes to this document, the OID number will be modified as regards its latest "Version" value and become 1.2.250.1.5.1.1.1.3.**3** in its next revision.

1.3 Entities intervening in the PKI

1.3.1 Certification Authority

The Certification Authority is the Caisse des Dépôts et Consignations (CDC), duly represented by its head, the Director General of the CDC. Within the framework of this activity, he may, if he wishes, delegate this function to a person of his choice. In particular, the ISSO (Information System Security Officer) of the CDC benefits from this delegation. The ISSO of the CDC is the head of the Certification Authority.

The Certification Authority is responsible for the application of this Certification Policy. The CA is responsible for the certificates signed in its name and for the whole of the public key infrastructure (PKI) it has set up.

In particular, the CA is responsible for the following functions:

- Application of the Certification Policy,
- Registration of Holders,
- Issuing of certificates,
- Certificate management,
- Publication of the Certificate Revocation List (CRL),
- Logging and archiving of events and information relating to the functioning of the PKI.

The CA performs these functions directly or wholly or partly delegates or subcontracts them. In all cases, the CA remains responsible for them.

1.3.2 Delegated Registration Authority

The Registration Authority (RA) is responsible for certificate life cycle management. It validates Holders' applications. It guarantees the identity of the Holders to whom it issues certificates.

Because of the diversity of the Customers of the CA CDC - LEGALIA (see the definition of a "Customer" in paragraph 1.6.2), the CA CDC - LEGALIA may use several Delegated Registration Authorities.

A Delegated Registration Authority acts as the Registration Authority within a given perimeter. This perimeter may include the Holders of one or more Customers.

The reciprocal obligations between the Certification Authority and each Delegated RA are described in a "CA - RA Agreement" signed by the head of the Certification Authority and by the representative of the Customer responsible for the Delegated RA.

The organisation, processes and tools of each Delegated RA are the same. The players potentially differ between Delegated RAs.

The players of a Delegated RA are the Registration Operators. They are appointed by the Application Manager. They guarantee the functioning of the RA and are therefore responsible for managing the life cycle of the Certification Authority's certificates, within the perimeter of the Delegated RA.

The players of the Delegated RA are authenticated by certificate during access to the Registration Authority's interfaces. For this purpose, they must apply for a certificate from the CA CDC - FIDELIA.

Each Delegated RA performs the following functions:

- Management of certificate applications;
- Triggering of the generation of certificates with the CSP;
- Checking of the identity of future Company Authorized Representatives and validation of their appointment;
- Checking of the identity of future Holders;
- Validation of registration files;
- Validation of certificate revocation requests;
- Participation in certificate renewal;
- Archiving of registration files;
- Level 2 support for Holders.

The only Delegated RA of the CA CDC - LEGALIA is the DBR RA: it manages the perimeter of the Holders of the "business line" Customer DBR SP2. Delegated RAs may be operated by Customers of cross-company entities. In particular, the DBR RA is operated by the business line Customer DBR SP2.

1.3.3 Certificate Holders

A Certificate Holder is an individual, acting within the framework of his professional activities, who holds a certificate issued by the CA CDC - LEGALIA. This certificate is used for authentication when accessing business resources (OID 1.2.250.1.5.1.1.1.2.2) or for electronic signature within the framework of business uses (OID 1.2.250.1.5.1.1.1.3.2).

1.3.4 Certificate users

The certificate users are the authentication, electronic signature and signature validation services which use the Holders' certificates. This concerns business applications.

1.3.5 Other participants

1.3.5.1 Components of the PKI

The technical components enabling the functions of the PKI to be operated are presented in the CPS.

1.3.5.2 Certification Service Provider (CSP)

The CSP is responsible for operating a certification service managing the whole life cycle of the Certificates, in accordance with the CPs. For the CDC, the Technical Operator is Keynectis, managed by INFORMATIQUE CDC (ICDC) by delegation from the CA. A contract is drawn up between the Caisse des Dépôts, INFORMATIQUE CDC and Keynectis for the technical supply of the certification service.

The CSP's personnel may need to use certificates for authentication or signature purposes on the components which it controls. These certificates are not to be confused with those of the Holders and are not issued by the CA CDC - LEGALIA. In this case of application, we shall speak of certificates of the components of the CSP and the procedures for management of these certificates are described in the related certification policies.

1.3.5.3 Company Authorized Representative

The Company Authorized Representative is an individual duly identified and accredited by the RA. The Company Authorized Representative checks the (individual) identity of

Holders on behalf of a Registration Authority. He is also involved in the certificate application or revocation request process on behalf of the Holders. He is part of the organisation to which the Holders he is responsible for belong. He is designated by the legal representative of the Holders' organisation, and has powers to represent their organisation in dealings with the Certification Authority.

1.4 Use of certificates

1.4.1 Applicable areas of use

1.4.1.1 Holders' key pairs and certificates

The certificates issued by the CA CDC - LEGALIA are usable exclusively for authentication operations (OID 1.2.250.1.5.1.1.1.2.2) or signature operations (OID 1.2.250.1.5.1.1.1.3.2) carried out by the certificate users as defined in paragraph 1.3.4. Any other use is made under the sole responsibility of the Certificate Holder.

The CA CDC - LEGALIA does not issue certificates for other populations and for other uses. The certificates of the other components of the Public Key Infrastructure (CSP administration certificates) are issued by another certification authority.

The key pairs associated with the Holders' certificates are in "hardware" format: the key pairs are protected in a physical medium. The physical medium is personal and specific to the Holder. This physical medium is supplied by Gemalto. It belongs to the "MultiApp ID IAS ECC on NXP component" range. It is described as "SSCD qualified". It guarantees the security of exchanges relating to the use of the key pair from the physical medium.

1.4.1.2 CA and component key pairs and certificates

The certificate of the CA CDC - LEGALIA is issued by the CA CDC RACINE and is usable exclusively for:

- Signing Holder certificates;
- Signing CRLs.

1.4.2 Prohibited areas of use

The certificates of this CP cannot be used outside authentication or signature operations performed in the context of applications explicitly authorised by the CDC or which have been authorised beforehand by the representatives of the CA. The CDC may not be held responsible for use of a certificate by a Holder on an application which is not explicitly authorised.

1.5 CP management

1.5.1 Entity managing the CP

The CDC is responsible for managing the CP via the Risk and Internal Control Department (DRCI).

1.5.2 Contact point

Requests for information or comments on this Certification Policy must be sent to:

Responsable du Service de Certification
Caisse des Dépôts – Direction du Risque et du Contrôle Interne
56 rue de Lille – 75 007 Paris
igc@caissedesdepots.fr

Questions for the Registration Authority must be sent to the following e-mail address, for the DBR Delegated RA: ae-dbr@caissedesdepots.fr
The telephone number to contact the DBR RA is: +33 (1) 58 50 58 58.
The postal address of the DBR RA is:

Caisse des Dépôts
AE CDC - LEGALIA – DBR – Bureau B235
15 Quai Anatole France – 75 356 PARIS

1.5.3 Entity determining the compliance of a CPS with this CP

The CDC is responsible for the internal operations to check the compliance of the CPS with the CP.

1.5.4 Procedures for approval of compliance of CPS

Approval of the compliance of the CPS with the Certification Policy is declared by the Head of the Certification Authority.

1.6 Definition and acronyms

1.6.1 Acronyms

The acronyms used in this CP are as follows:

ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information*
CA	Certification Authority
CISSI	*Commission Interministérielle pour la SSI* (Interministerial Commission for ISS)
CP	Certification Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DGME	*Direction Générale de la Modernisation de l'Etat* (General Directorate for Modernisation of the State
DN	Distinguished Name
ECS	European Committee for Standardisation
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISS	Information System Security
ISSO	Information System Security Officer
PKI	Public Key Infrastructure.
LAR	*Liste des certificats d'AC Révoqués* (CA Certificate Revocation List)
MC	*Mandataire de Certification* (Company Authorized Representative)
OC	*Opérateur de Certification* (Certification Operator)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PP	Protection Profile
PSCE	Prestataire de Services de Certification Electronique (Electronic Certification Service Provider)
RA	Registration Authority
RSA	Rivest Shamir Adelman
SP	*Service de Publication* (Publication Service)
SSCD	Signature Secure Creation Device
TSA	Time Stamping Authority
URL	Uniform Resource Locator

1.6.2 Definitions

Agent - Individual acting on behalf of an administrative authority.

User applications - Application services using the certificates issued by the Certification Authority for purposes of authentication, encryption or signature of the Holder of the certificate or purposes of authentication or stamping for the server to which the certificate is attached.

Authentication - Process used to check the stated identity of a person or of any other entity, or to guarantee the origin of data received.

Administrative authorities - This generic term refers to state administrations, local governments, public establishments of an administrative nature, the bodies managing social security systems and other bodies responsible for the management of an administrative public service.

Certification Authority (CA) - Within a PSCE, a Certification Authority is responsible, in the name and under the responsibility of this PSCE, for the application of at least one Certification Policy, and is identified as such, as the issuer ("Issuer" field in the certificate), in the certificates issued under this Certification Policy. In this CP, the term PSCE is not used outside this chapter and chapter I.1 and the term CA is otherwise the only term used. It refers to the CA responsible for the application of the Certification Policy, meeting the requirements of this CP, within the PSCE wishing to obtain qualification of the corresponding family of certificates.

Registration Authority – This authority checks the identification information of the future Holder of a certificate, and if necessary other specific attributes, before passing on the corresponding application to the appropriate department of the PKI, in accordance with the services rendered and the organisation of the PKI (see below). The RA is also responsible, when necessary, for re-checking the Holder's information during renewal of his certificate.

Delegated RA – Registration Authority managing the Holders in a given perimeter.

Time Stamping Authority – Authority responsible for managing a time stamping service (see standard time stamping policy [RGS_A_12]).

Key pair – A key pair is a pair consisting of a private key (which must be kept secret) and a public key necessary for using encryption techniques based on asymmetric algorithms.

Electronic certificate - Electronic file certifying that a key pair belongs to the individual or legal entity or hardware or software element identified, directly or indirectly (by an alias), in the certificate. It is issued by a Certification Authority. By signing the certificate, the CA validates the link between the identity of the individual or legal entity or hardware or software element and the key pair. The certificate is valid for a given period specified in the certificate. In this CP, the term "electronic certificate" refers only to a certificate issued to an individual and concerning an authentication key pair (OID 1.2.250.1.5.1.1.1.2.2), or signature key pair (OID 1.2.250.1.5.1.1.1.3.2), unless specified otherwise (CA certificate, certificate of a component, etc.).

Trust chain - All of the Certificates necessary to validate the genealogy of a Certificate Holder's Certificate.
In a simple horizontal architecture, the chain consists of the Certificate of the Certification Authority which issued the certificate and that of the Certificate Holder.

Customer: entity benefiting from the PKI. This entity uses the CDC's PKI and one or more Delegated RAs to cover its certificate needs, for given users and Holder populations which are within its area of responsibility.

CA Steering Committee – steering body of the Certification Authority. It comprises five people who play a security role.

Component - Platform operated by an entity and consisting of at least a computer workstation, an application and, if necessary, a means of encryption and playing a defined role in the operational implementation of at least one function of the PKI. The entity may be the PSCE itself or an external entity linked to the PSCE contractually, by regulations or hierarchically.

General Terms of Use (GTU) – Summary of the authorised use of a certificate and of the Holder's obligations, in accordance with the Certification Policy of the CA. The GTU must be known to the Holder.

"CA - RA Agreement" - document defining the reciprocal obligations between the Certification Authority and a Customer operating a Delegated RA

Certification Practices Statement (CPS) - A CPS identifies the practices (organisation, operational procedures and technical and human resources) which the CA applies in the supplying of its electronic certification services to users in compliance with the certification policy or policies which it has undertaken to follow.

Authentication system – This is the hardware and/or software system used by the Holder to store and use his private authentication key.

Secure Signature Creation Device (SSCD) - Hardware or software designed to implement the electronic signature creation data, which meets the requirements defined by the regulations

Registration file – set of documents enabling the RA to validate the registration application of a future Holder. The registration file of the CA CDC - LEGALIA for a Holder comprises the signed application form, a photocopy of the future Holder's identity document certified as a "true copy of the original" together with the signed General Terms of Use. It should be noted that the registration file of a Company Authorized Representative contains additional documents (described in paragraph 3.2.3.3).

Entity – Refers to an administrative authority or an enterprise in the broadest sense, i.e. also private legal entities such as associations.

Renewal window – period of time during which a certificate can be renewed. This period starts a few months before the expiry date of the certificate. The length of the renewal window is defined in this CP (paragraphs 4.6 and 4.7).

Certificate generation function - This function generates (creation of the format and electronic signature with the CA's private key) the certificates on the basis of the information passed on by the Registration Authority and the Holder's public key obtained either from the Holder or from the Holder secret element generation function, if it is the latter function which generates the Holder's key pair.

Holder secret element generation function - This function generates the secret elements intended for the Holder, if the CA is responsible for this generation, and prepares them for their submission to the Holder (e.g. personalisation of the smart card to be supplied to the Holder, secure letter with the activation code, etc.). Such secret elements may be, for example, the Holder's key pair itself, the (activation / unlocking)

codes associated with the Holder's private key storage device, or temporary codes or keys enabling the Holder to carry out the process of generation / collection of his certificate remotely.

Revocation management function - This function processes revocation requests (particularly identification or authentication of the applicant) and determines the actions to be conducted. The results of the processing are circulated via the certificate status information function.

Publication function – This function makes available to the various parties concerned the general terms, policies and practices published by the CA, the CA certificates and any other relevant information intended for Holders and/or certificate users, apart from certificate status information. It may also, depending on the CA's policy, make available the valid certificates of its Holders.

Holder delivery function – This function delivers to the Holder at least his certificate and, if necessary, the other elements supplied by the CA (Holder's device, Holder's private key, activation codes, etc.).

Certificate status information function - This function supplies certificate users with information on the status of certificates (revoked, suspended, etc.). This function may be implemented according to a mode involving publication of updated information at regular intervals (CRL, LAR) and also if necessary according to a real time query/response mode (OCSP).

Application form - Form required for registration of a Holder. It must be filled in and signed by the future Holder. It contains information on the Holder's identity and organisation.

Crypto Service Provider *(*CSP) – Program enabling use of the cryptographic functions of a certificate's physical medium.

HSM (Hardware Security Module) – Encryption box in which the public and private keys of the Certification Authorities are stored.

Public Key Infrastructure (PKI) - Set of components, functions and procedures dedicated to the management of cryptographic keys and their certificates used by trust services. A PKI may consist of a certification authority, a certification operator, a centralised and/or local Registration Authority, certification agents, an archiving entity, a publication entity, etc.

Certificate Revocation List (CRL) - List containing the identifiers of revoked or invalid certificates.

Company Authorized Representative - The Company Authorized Representative is designated by and placed under the responsibility of the client entity. He is in direct contact with the RA. He carries out on its behalf a number of checks concerning the identity and if necessary the attributes of this entity's Holders (he carries out in particular the face-to-face meeting for identification of the Holders when such a meeting is required).

Reason for revocation – Circumstance which may be the cause of the revocation of a certificate. The reasons for revocation are detailed in paragraph 4.9.1.

OID - Unique digital identifier registered in accordance with the ISO registration standard to designate a specific object or class of objects.

Authorised person - This is a person other than the Holder and the Company Authorized Representative who is authorised by the CA's Certification Policy or by a contract with the CA to conduct certain actions on the holder's behalf (request for revocation, renewal, etc.). Typically, in an enterprise or an administration, this may be a hierarchical superior of the Holder or a human resources manager.

Certification Policy (CP) - Set of rules, identified by a name (OID), defining the requirements with which a CA complies in the setting up and supply of its services and indicating the applicability of a certificate to a particular community and/or a class of applications with common security requirements. A CP can also, if necessary, identify the obligations and requirements concerning other persons involved, particular Holders and certificate users.

Certificate Holder – The individual identified in the certificate who is the holder of the private key corresponding to the public key which is in this certificate.

Electronic certification service provider (PSCE) - Any person or entity who is responsible for the management of electronic certificates throughout their life cycle with respect to the Holders and users of these certificates. A PSCE can supply various families of certificates corresponding to different uses and/or different levels of security. A PSCE comprises at least one CA but may comprise several CAs depending on its organisation. The various CAs of a PSCE may be independent from each other and/or bound by hierarchical or other links (Root CA / Child CAs). A PSCE is identified in a certificate for which it is responsible via its CA which has issued this certificate and which is itself directly identified in the "issuer" field of the certificate.

Security product - A software or hardware device whose use is required to implement security functions necessary for the protection of a dematerialised item of information (in an exchange, a processing operation and/or the storage of this information). This generic term covers in particular electronic signature devices, authentication devices and confidentiality protection devices.

Application promoter - Person responsible for a public service accessible by electronic means.

Qualification of an electronic certification service provider - The [RGS Decree] describes the procedure for qualification of PSCOs (trust service providers). As a PSCE is a specific PSCO, the qualification of a PSCE is an act by which a certification body certifies the compliance of all or part of the electronic certification offer of a PSCE (family of certificates) with certain requirements of a Standard CP for a given level of security and corresponding to the service concerned by the certificates.

Qualification of a security product – Act by which the ANSSI certifies the capacity of a product to provide, with a given level of robustness, the security functions concerned by the qualification. The qualification certificate indicates if necessary the ability of the product to participate in the performing, at a given level of security, of one of more functions dealt with in the [RGS]. The qualification procedure for security products is described in the [RGS Decree]. The [RGS] specifies the three qualification processes: elementary level qualification, standard level qualification and reinforced level qualification.

Renewal of a Certificate - Operation carried out at the request of a Certificate Holder or at the end of the period of validity of a Certificate which consists in generating a new Certificate identical in every way to the previous one apart from the validity dates and the public key.

Application Manager of the CA CDC - LEGALIA - The Application Manager is responsible for the implementing of the Certification Policy and the PKI Certification Practices Statement on the application for which he is responsible. His responsibility covers all of the functions performed by this application and the corresponding performances.

Head of the Certification Authority – Person physically representing the Certification Authority.

Revocation of a Certificate - Operation resulting in the removal of the CA's guarantee concerning a given Certificate, before the end of its period of validity.
A revocation request may be made as a result of various types of events such as compromise of a key pair, change of information contained in a certificate, etc.
The revocation operation is considered to have been completed when the certificate in question is published in the Certificate Revocation List. The certificate is then unusable.

Physical medium (or encryption medium) - smart card or cryptographic key with USB port which may contain key pairs and certificates.

Information system – Any set of resources used to produce, process, store or transmit information exchanged electronically between administrative authorities and users and between administrative authorities.

Identity document - national identity card, passport or residence permit (for foreign nationals) serving to prove the identity of a future Holder to the RA.

User - Individual acting on his own behalf or on behalf of a legal entity and conducting electronic exchanges with administrative authorities.

Note - An employee of an administrative authority who conducts electronic exchanges with another administrative authority, is, from the latter's point of view, a user.

Certificate user - Entity or individual receiving a certificate and relying on it to check an electronic signature received from the Holder of the certificate.

Certificate validation - Operation to check the status of a Certificate or a certification chain.

2 RESPONSIBILITIES CONCERNING MAKING AVAILABLE OF INFORMATION WHICH MUST BE PUBLISHED

2.1 Entities responsible for making available of information

The CA is responsible for the making available of information which must be published. Operationally, this function is performed under the responsibility of the Certification Service Manager.

2.2 Information which must be published

The information published by the CA CDC - LEGALIA is as follows:

- This Certification Policy;
- The General Terms of Use;
- The forms necessary for certificate management: registration application, revocation request;
- The Mandate necessary for the appointment of a new Company Authorized Representative;
- The "CA - RA Agreement" defining the reciprocal obligations between the Certification Authority and a Customer operating a Delegated RA.
- The points of contact with the Certification Authority or the Delegated RA.

The CSP publishes the following elements:

- The profiles of the certificates and CRLs (see paragraph 7);
- The Certificate Revocation List (CRL);
- The URL for self-service revocation of certificates;
- The certificate of the Certification Authority CDC - LEGALIA;
- The thumbprint of the certificate of the CA CDC - LEGALIA.

The thumbprint of the certificate of the CA CDC - LEGALIA is (algorithm SHA-256):
E7 FC 14 CF ED F7 F5 3F 9D 6B AB 80 79 F5 29 E9 C7 07 4C 06 58 21 5A CA 87 17 1B E1 AA 8F 54 F4

2.2.1 Publication of Certification Policy

This CP is published on the website:
http://www.caissedesdepots.fr/uploads/media/pc-legalia-en.pdf

2.2.2 Publication of CA certificate

The certificate of the Certification Authority is published on:

- For the CA CDC - RACINE: http://www.caissedesdepots.fr/uploads/media/cdc-racine.crt
- For the CA CDC - LEGALIA: http://www.caissedesdepots.fr/uploads/media/cdc-legalia.crt

2.2.3 Publication of CRL

The certificate revocation list (CRL) is published on:
http://igc-crl.caissedesdepots.fr/cdc/legalia.crl

It is also accessible via an OCSP service:
http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/

These URLs are also indicated in the Holders' certificates.

2.3 Publication lead times and frequencies

2.3.1 Frequency of publication of Certification Policy

The Certification Policy is reviewed at least every two years, and updated if necessary in accordance with the provisions described in section 9.12.1. The Certification Policy is published as soon as it is validated, within a maximum period of 24 hours.

2.3.2 Frequency of publication of CA certificate

The CA certificate is circulated within a maximum period of 24 hours following its generation.

2.3.3 Frequency of publication of CRL

CRLs are published every 24 hours. The status of certificates can be obtained via the CRL and via an OCSP service.

2.3.4 Availability of published information

The CSP's electronic certification service is available round the clock. The level of availability of the service (including certificate issuing and revocation) is 99 % on a monthly basis, and a continuous unavailability of the service (incident of seriousness level 1) may not exceed 6 hours in operational working hours and 8 hours in non-working hours. These provisions, and this service guarantee, are guaranteed by the CSP and constitute contractual obligations for the CSP with respect to the CA.

2.4 Control of access to published information

Published information is made available for reading to the whole User community. The CPs, CA certificates and CRLs are made available internationally for reading.

Additions, deletions and changes are restricted to authorised persons in the CA. Edit mode access to certificate status information publication systems (adding, deleting and modification of published information) is strictly limited to the accredited internal functions of the PKI, via strong access control.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Name types

The names used comply with the specifications of the X.500 standard. In each X509v3 certificate the issuing CA (issuer) and the Holder (subject) are identified by an X.501 type "Distinguished Name" (DN), the exact format of which is specified in section 7 describing the profile of the certificates. The distinguished name takes the form of an "X.501 name" type "UTF8 string".

3.1.2 Need for use of explicit names

The names to distinguish Holders are explicit and contain the necessary information to identify Holders, located in the "Subject – DN" field of the certificate, such as the Holder's surname, first name and organisation. This information is collected by the Company Authorized Representative during the Holder identity check phase.

The name (CN field) is that of the Holder as indicated in the identity documents. The information contained in the "Subject – DN" field of the certificate is described explicitly below:

- C (CountryName) field: the country in which the Holder's organisation is registered;
- O (OrganizationName) field: the corporate name of the organisation represented by the Holder, as indicated in the company registration certificate;
- OU (Organization Unit) field: the SIREN or SIRET number of the organisation represented by the Holder;
- CN (Common Name) field: the Holder's name in "Given name SURNAME" form (if required, the Holder's second given name may be added if it appears on the identity documents).

3.1.3 Holder aliases

The certificates concerned by this CP may in no case be anonymous. Maiden name type aliases are accepted only if they are indicated on the official identity documents supplied at the time of registration.

3.1.4 Rules for interpretation of the various forms of names

The names used for Holders are sufficiently explicit and do not require any particular interpretation.

All the characters are in "printable string" format, i.e. without accents or characters specific to French and in accordance with the X.501 standard. For hyphenated given names and surnames, the hyphen is used as a separating element.

Example:

DN = {C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=Jean-Michel DUPONT}

3.1.5 Uniqueness of names

The RA will resolve any homonym problems and guarantees the uniqueness of the names used for the Holders' certificates. The uniqueness key of a certificate within the CA CDC - LEGALIA is the e-mail address of the Holder combined with the DN (Distinguished Name) field and the KeyUsage.

The e-mail address is positioned in the certificate in field RFC 822 (*Subject Alternative Name*). By definition an e-mail address is unique within a structure. The DN field, containing the SIREN/SIRET number of the organisation to which the holder is attached, guarantees the uniqueness key if Holders in different structures have the same e-mail address.

The inclusion of the KeyUsage in the uniqueness key guarantees differentiation between a signature certificate and an authentication certificate possessed by the same Holder.

In the event of homonyms in the "Given name SURNAME" pairing, within the same organisation, the RA will also enter the Holder's second given name in the CommonName (CN) attribute of the certificate.

The given names presented must be presented in the same order as on the identity document and separated by a comma without any space either before or after the comma, followed by a space, followed by the holder's surname.

Example:
DN = {C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=Michel,Paul DUPONT}

3.1.6 Identification, authentication and role of registered trademarks

The RA shall check with reasonable care the right of use of registered names and trademarks by the applicant.

3.2 Initial validation of identity

3.2.1 Method to prove possession of the private key

The CA checks the possession of the private key by the Certificate Holder before certifying the public key. During the certificate application process, the Holder generates his key pair in his physical medium and supplies the CA with proof of possession of his private key (request PKCS#10) corresponding to the public key contained in his certificate application.

3.2.2 Validation of the identity of an organisation

See chapter 3.2.3.

3.2.3 Validation of the identity of an individual

3.2.3.1 Registration of a Holder [PRIVATE INDIVIDUAL]

Not applicable.

3.2.3.2 Registration of a Holder [ENTERPRISE] / [ADMINISTRATION] without Company Authorized Representative

Not applicable.

3.2.3.3 Registration of a Company Authorized Representative

The registration of a Company Authorized Representative involves the following steps:

- **Signing of a Mandate** and supply of additional documents **by the Legal Representative.**
- **Signing of the General Terms of Use** and of the Mandate by the future Company Authorized Representative.
- **Validation of the identity** of the Company Authorized Representative by the Delegated RA in a face-to-face meeting.
- **Archiving** of all the documents in the registration file.

The future Company Authorized Representative downloads the following documents on the Caisse des Dépôts' institutional website:

- Mandate of the Certification Agent. This must be dated less than 3 months previously.
- General Terms of Use (GTU). It should be noted that the GTU contain the Certification Agent's commitments:
    - Commitment concerning checking of applicants' files.
    - Commitment concerning notification of his departure.

The future Certification Agent fills in these documents and signs them. The future Certification Agent goes to meet the Legal Representative to get him to sign the Mandate. The Legal Representative must return the signed Mandate to the future Certification Agent together with two additional documents:

- Attestation of unique identification of the enterprise (company registration certificate or Certificate of Identification in the Répertoire National des Entreprises et de leurs Établissements (National Directory of Businesses and their Establishments) or registration in the Trades Register).
- Legal Representative's attestation.

The documents cited collectively constitute the registration file.

The future Certification Agent goes to the premises of the RA, with the registration file, and meets a Registration Operator face-to-face.

The Registration Operator validates the registration file. To do so, he checks:

- The completeness of the Registration file:
    - Certification Agent's mandate. The mandate designates the Certification Agent. It must be jointly signed by the Legal Representative and the Certification Agent. It must be dated less than 3 months previously.
    - General Terms of Use.
    - Attestation of unique identification of the enterprise.
    - Legal Representative's attestation.
- The signature of the Legal Representative on the mandate.
- The signature of the future Certification Agent on the mandate and the General Terms of Use.
- The consistency between the information indicated in the Mandate and the supporting documents supplied.

The Registration Operator photocopies an identity document belonging to the Holder. The Registration Operator and the Holder sign this photocopy, adding the words "Certified true copy of the original". This photocopy is added to the registration file.

The Registration Operator archives the registration file.

3.2.3.4 Registration of a Holder [ENTERPRISE] / [ADMINISTRATION] via a Certification Agent

The registration of a Holder involves the following steps:

- **Application.**
- **Validation of the Holder's identity**.

These two steps are the subject of this paragraph.

- Validation of the application.

The methods of validation of the Holders' identity are defined for each Customer, in the "CA - RA Agreement". The Customer, via the Certification Agent, vouches for the reliability of the identity communicated by the Holder to the RA at the time of registration.

In all cases, the application and the validation of the Holder's identity take place in the manner described below. The future Holder goes to meet the Certification Agent to make his certificate application. The Certification Agent checks the Holder's identity in a face-to-face meeting. For this purpose, the Holder presents an identity document. The Certification Agent photocopies the Holder's identity document, and adds the words "Certified true copy of the original". The Certification Agent and the Holder sign this photocopy. The Certification Agent gets the Holder to fill in the application form. The Holder signs the form. The Holder signs the General Terms of Use.

These documents collectively constitute the Holder's registration file:

- Application form signed by the Holder.
- General Terms of Use signed by the Holder.
- Photocopy of an identity document signed by the Certification Agent and the Holder.

The Certification Agent sends the registration file to the RA.

3.2.4 Unverified Holder information

Not applicable.

3.2.5 Validation of the applicant's authority

For the CA CDC - LEGALIA, the applicant is always the future Holder.

The RA, and by delegation the Certification Agent, check that the applicant has the necessary powers to make this application. This check is carried out on the basis of the information supplied in the certificate application, and according to the rules specific to the Business Line, which the RA will have validated by the persons in charge of the Certification Authority before implementation.

3.2.6 CA cross-certification

The CA has no recognition agreement with a CA outside the security domain to which it belongs. Nevertheless, the CA will recognise all other external CAs which have the status referenced "CFONB", "RGS" or "PRIS".

In this case, if another CA make an agreement request, or if the persons in charge of the CA CDC - LEGALIA express the need to establish a recognition agreement with another CA, the CA steering committee will conduct a series of investigations (audits / risk analysis) to determine whether the CA to be recognised issues certificates of the same quality, with the same level of security, as those of this CA CDC - LEGALIA.

In particular, the CDC may expect CAs requesting a certification agreement to comply with the certificate formats stipulated by the following standards:

- IETF RFC 5280;

- IETF RFC 3739 and ETSI - TS 101 862 for qualified certificates.

3.3 Identification and validation of a key renewal request

A new certificate cannot be supplied to the Holder without renewal of the corresponding key pair.

3.3.1 Identification and validation for a standard renewal

The Holder is informed of the forthcoming expiry of his certificate by e-mail 90, 30 and 15 days before expiry. Copies of these notifications are sent to the RA.

3.3.1.1 Case of first renewal

The RA bases itself on the registration file supplied at the time of the first application and archived for identification and validation of the renewal request. The Holder must reply to a notification from the RA to validate the renewal. He will then receive a collection URL and a collection code in two separate e-mails, to carry out the renewal.

3.3.1.2 Case of second renewal

In the second renewal, the procedure for identification and validation of the renewal request is the same as the initial registration procedure (see paragraph 3.2).

3.3.2 Identification and validation for a renewal after revocation

Following the definitive revocation of a certificate, for whatever reason, the procedure for identification and validation of the renewal request is the same as the initial registration procedure (see paragraph 3.2).

3.4 Identification and validation of a revocation request

A request for revocation of a certificate issued by the RA CDC - LEGALIA may be made by the following players:

- The Holder or a Certification Agent;
- The Registration Authority of the CA CDC - LEGALIA;
- A Legal Representative of the Holder's entity;
- The Head of the CA CDC - LEGALIA.

Any person making a revocation request is authenticated.

- The Holder is authenticated via his revocation code chosen at the time of the certificate application.
- The Certification Agent is authenticated on the basis of a handwritten signature by comparison with the signature in his registration file.
- The Registration Operator is authenticated via his certificate issued by the CA CDC - FIDELIA.
- The Legal Representative is authenticated on the basis of a handwritten signature using a signature card.
- The Head of the CA is authenticated by the RA (face-to-face meeting, handwritten signature, signed e-mail).

Remark 1: the Holder is identified by the person making the request via the following information:

- If the Holder is the person making the request: the identifier used may be the Holder's e-mail address or the content of the Holder's CN field.
- Otherwise: the Holder must be identified via his surname, given name and e-mail address.

Remark 2: when the applicant is the Certification Agent or the Legal Representative, he must be identified via the following information:

- Surname, given name, name of the company to which he belongs and work telephone number.

4 OPERATIONAL REQUIREMENTS CONCERNING THE LIFE CYCLE OF CERTIFICATES

4.1 Certificate application

4.1.1 Origin of a certificate application

A certificate may be applied for by a Certification Agent alone, duly mandated for this entity, in the event of prior consent of the future Holder.

This application must undergo checking and validation by the RA before issuing of the electronic certificate.

4.1.2 Process and responsibilities for drawing up a certificate application

The registration of a Holder involves the following steps:

- **Application.**
- **Validation of the Holder's identity**.

These two steps are described in paragraph 3.2.3.4. This paragraph details certain points mentioned in paragraph 3.2.3.4.

- Validation of the application: this step is described in paragraph 4.2.1.

The certificate application must be based on a registration file. This file comprises:

- The application form signed by the Holder.
- The General Terms of Use signed by the Holder.
- A photocopy of an identity document signed by the Certification Agent and the Holder.

The application form contains the following information:

- The reference of the contract between the CA and the Customer to whom the Holder belongs.
- The future Holder's contact details:
  - Surname and given name;
  - Work e-mail address;
  - Postal address.
- The revocation code chosen by the Holder, which he will have to use in the event of loss or compromise of his physical medium. The Holder must comply with the password policy which is detailed in the application form;
- The date and the Holder's signature (on paper).

The registration file must be passed on to the RA for validation.
It may be submitted in paper form or in electronic form. The electronic form may involve scanning of the previously signed paper documents.

4.2 Processing of a certificate application

4.2.1 Execution of application identification and validation processes

The registration of a Holder involves the following steps:

- Application.
- Validation of the Holder's identity.

These two steps are described in paragraphs 3.2.3.4 and 4.1.2.

- **Validation of the application**: this step is described in this paragraph.

Prerequisites: the Registration Authority has received the registration file.

Within this RA, a data entry operator takes charge of the application and enters the Holder's information on the CSP's interfaces, using the information indicated in the application form. This triggers the sending of a notification to the RA indicating that a new application needs to be validated.

A validation operator carries out the validation of the application, checking:

- The consistency of the application with the Certification Agent's mandate.
- The completeness of the Registration file
- The consistency between the information entered in the application form and the Registration file.
- **Remark**: the documents in the registration file must be dated less than 3 months previously.

If these requirements are met, the validation operator validates the application on the CSP's interfaces.

- If not, the Registration Operator indicates that the Registration file is invalid. This triggers the sending of an e-mail to the generic mailbox of the Delegated RA. The Holder will be required to make another trip.

The validation of the application triggers the following on the PKI:

- Sending of a notification to the RA indicating the validation of the application.
- Sending of a notification to the Holder containing the personalised collection URL.
- Sending of a notification to the Holder containing the collection code.
- Sending of a notification to the Holder containing the revocation code.

The Registration Operator sends the physical medium to the future Holder by mail.

- Note 1: the physical medium is associated with a default PIN code. This initial PIN code will have to be changed by the Holder before collection.
- Note 2: concerning the letters sent:
    - They may be sent in a batch of similar letters to the Certification Agent. It is the Certification Agent who supplies them to the Holders.
    - OR they may be sent directly to the Holder at the address indicated in the application form.

Under these conditions, the Holder will be able to collect his certificate in self-service mode (under the additional condition that the technical prerequisites are met on his workstation).

The RA is responsible for establishing the follow-up of certificate applications and assignments. This follow-up must allow identification of:

- The Holders attached to an agent;
- The status of current certificate applications;
- The status of issued certificates.

The RA carries out this follow-up by keeping the paper documents which have been passed on to it by the agents.

4.2.2 Acceptance or rejection of application

The application is validated by a Registration Operator on the CSP's technical interfaces: the application may be accepted or rejected. In the event of rejection, the RA informs the Holder of this, giving the reasons for rejection.

4.2.3 Time required to draw up the certificate

Following validation of the application by the RA, the time required to draw up the certificate essentially depends on the Holder, who initiates the collection of this certificate. When the Holder triggers the procedure for collection of his certificate, the following operations are then carried out automatically:

- Generation of the Holder's keys on his encryption medium (USB key or Smart card);
- Creation of a file in PKCS#10 format for the certificate application (CSR);
- Secure transmission of the certificate application to the CA;
- Signing of the certificate application by the CA;
- Installing of the Holder's certificate on the physical medium.

This sequence of operations requires less than one minute.

4.3 Issuing of the certificate

4.3.1 CA actions concerning the issuing of the certificate

The issuing of the certificate by the CA to the Holder is carried out in self-service mode by the Holder.

Remark: if he has received a new physical medium, the Holder must change his PIN code. Certificate collection cannot be carried out with an initial PIN code.

Once the Holder has received the collection notifications (three separate letters containing the collection URL, the collection code and the revocation code) and his physical medium (if applicable), he carries out the collection of the certificate himself. This involves the following steps:

- The Holder accesses the connection URL.
- The Holder changes the PIN code of his physical medium (complying with the password policy associated with this physical medium).
- The Holder enters his collection code.
- The Holder enters his new PIN code to trigger electrical personalisation of the certificate.
- Electrical personalisation takes place as follows:
    - Generation of the Holder's keys on his physical medium;
    - Creation of a file in PKCS#10 format for the certificate application;
    - Secure transmission of the certificate application to the CA;
- The CA signs the certificate and hands it over to the Holder: the certificate is generated and automatically installed on the physical medium.
  Note: the certificate is also installed at the same time in the Holder's browser.
- Following the generation of the certificate, the Certification Authority sends a confirmation notification to the RA and to the Holder.

The time allowed for the Holder to carry out collection is limited to two months. If the applicant exceeds this two-month period, he must make a new application, following the same procedure as for the initial application.

4.3.2 Notification by the CA of the issuing of the certificate to the Holder

After issuing of the certificate, a notification is sent to the Holder (with a copy being sent to the RA).

4.4 Acceptance of the certificate

4.4.1 Certificate acceptance procedure

The certificate is tacitly accepted by the Holder 7 days after the installing of his certificate on his encryption medium (USB key or smart card). In the event of a claim made by the Holder, the certificate is revoked by the RA and the Holder is invited to make a new application for issuing of a certificate.

4.4.2 Publication of the certificate

Certificates are not published after issuing.

4.4.3 Notification by the CA to the other entities of the issuing of the certificate

The CA informs the RA of the issuing of a certificate to a Holder by sending an e-mail notification. The RA updates its certificate follow-up by annotating the effective issuing of the certificate in the corresponding Holder's registration file. In addition, the RA may be informed of the issuing of the certificate by consulting the list of certificates created via the CSP's technical interfaces.

4.5 Use of the key pair and the certificate

4.5.1 Use of the private key and the certificate by the Holder

The Holder undertakes, by signing the application form and the General Terms of Use, to use his certificate only for purposes of authentication (OID 1.2.250.1.5.1.1.1.2.2) or signature (OID 1.2.250.1.5.1.1.1.3.2), on target applications defined in paragraph 1.4.1. Any other use is prohibited, and entails the Certificate Holder's liability. This use is indicated explicitly in the extensions of the certificates (see chapter 7).

4.5.2 Use of the public key and the certificate by the certificate user

See previous chapter and chapter I.4: certificate users must strictly comply with the authorised uses of certificates.

4.6 Renewal of a Certificate

For the CA CDC - LEGALIA, there is no certificate renewal in the RFC 3647 sense, involving only changing of the validity dates. Only the issuing of a new certificate following a change of key pair is authorised.

This CP requires certificates and the corresponding key pairs to have the same lifetime. There can therefore be no renewal of certificates without renewal of the key pair.

4.6.1 Possible reasons for renewal of a Certificate

Not applicable.

4.6.2 Origin of a renewal request

Not applicable.

4.6.3 Procedure for processing of a renewal request

Not applicable.

4.6.4 Notification to the Holder of the drawing up of the new certificate

Not applicable.

4.6.5 Procedure for acceptance of the new certificate

Not applicable.

4.6.6 Publication of the new certificate

Not applicable.

4.6.7 Notification by the CA to the other entities of the issuing of the new certificate

Not applicable.

4.7 Issuing of a new certificate following change of key pair

4.7.1 Possible reasons for change of key pair

The key pairs issued for the Holders' certificates by the CA CDC - LEGALIA have a service life of 3 years. The issuing of a new certificate before the end of the service life can only be the consequence of a revocation or a renewal request. The renewal window is a period of 3 months before the expiry date of the certificate.

4.7.2 Origin of an application for a new certificate

If the application for a new certificate follows a revocation, the origin of the application is the Holder, the Registration Authority or the Certification Agent.

If the application for a new certificate is made within the framework of a certificate renewal request, the origin of the application is the Holder.

The Holder receives notifications of the forthcoming expiry of his certificate from the RA from the beginning of the renewal window. The Holder receives three notifications. The Holder must confirm his renewal request to the RA by return e-mail. Beyond the expiry date of the certificate, he will have to make a new application (see paragraph 4.1).

4.7.3 Procedure for processing an application for a new certificate

The procedure for processing an application for a new certificate is the same as the initial application procedure (see paragraph 4.2) in the following cases:

- The application for a new certificate follows a revocation.
- The application is for a second renewal.

In the case of a first renewal, the procedure for processing an application for a new certificate is as follows:

- Following receipt of an expiry notification and e-mail confirmation from the Holder, a Registration Operator takes charge of the application.

- **Remark**: the Holder specifies whether or not he wishes to change his physical medium. It is recommended to change the physical medium at the time of the second renewal.
- The Registration Operator (data entry operator role) makes a renewal request on the CSP's technical interfaces.
- A validation operator validates the application.
- The validation of the application triggers:
  - Sending of a notification to the RA indicating the validation of the application.
  - Sending of a notification to the Holder containing the collection URL.
  - Sending of a notification to the Holder containing the collection code.
  - Sending of a notification to the Holder containing the revocation code.
- The Holder collects his certificate as described in paragraph 4.3.

Remark: the first renewal process does not require the step of validation of the Holder's identity.

4.7.4 Notification to the Holder of the drawing up of the new certificate

Same as for application (paragraph 4.3.2).

4.7.5 Procedure for acceptance of the new certificate

Same as for application (paragraph 4.4.1).

4.7.6 Publication of the new certificate

Same as for application (paragraph 4.4.2).

4.7.7 Notification by the CA to the other entities of the issuing of the new certificate

Same as for application (paragraph 4.4.3).

4.8 Modification of the certificate

Modifications of CA certificates are not authorised.

4.8.1 Possible reasons for modification of a certificate

Not applicable.

4.8.2 Origin of a certificate modification request

Not applicable.

4.8.3 Procedure for processing a certificate modification request

Not applicable.

4.8.4 Notification to the Holder of the drawing up of the modified certificate

Not applicable.

4.8.5 Procedure for acceptance of the modified certificate

Not applicable.

4.8.6 Publication of the modified certificate

Not applicable.

4.8.7 Notification by the CA to the other entities of the issuing of the modified certificate

Not applicable.

4.9 Revocation and Suspension of certificates

4.9.1 Possible reasons for a revocation

4.9.1.1 Holders' certificates

The following circumstances can lead to the revocation of a Holder's certificate:

- the Holder's information indicated on his certificate is no longer in accordance with the identity or the use stipulated in the certificate (for example after a change in the Holder's entity following a transfer);
- the Holder or the organisation to which he belongs has not met the obligations resulting from this CP and indicated in the General Terms of Use;
- an error (intentional or otherwise) has been detected in the Holder's registration file;
- the Holder's private key is suspected of being compromised, is compromised, has been lost or has been stolen;
- the PIN code of the Holder's physical medium is suspected of being compromised, is compromised or has been forgotten;
- the Holder, the Legal Representative of the entity, the Certification Authority or the Registration Authority request revocation of the certificate (particularly in the case of destruction or impairment of the Holder's private key and/or his physical medium);
- death of the Holder or discontinuation of the activity of the Holder's entity;
- termination or normal expiry of the Contract relating to the electronic certification services;
- a major technological change requiring the generation of new key pairs (key lengths too short, hashing algorithms compromised).
- Revocation of a CA certificate in the trust chain.

When one of the above circumstances arises and the CA has become aware of it, the certificate concerned is revoked and the serial number placed in the new Certificate Revocation List (CRL).

4.9.1.2 Certificates of a component of the PKI

The following circumstances trigger revocation of the certificate of a component of the PKI (particularly the certificate of the CA used for signing of the Holder certificates and the CRLs):

- Suspected compromise, compromise, loss or theft of the component's private key;
- A decision to change a component of the PKI following detection of a non-conformity in the procedures applied within the component with it following a negative qualification or compliance audit);
- Discontinuation of the activity of the entity operating the component.

4.9.2 Origin of a revocation request

4.9.2.1 Holder certificates

The persons / entities who can request the revocation of a Holder certificate are as follows:

- The Holder;
- The Registration Authority of the CA CDC - LEGALIA;
- A Legal Representative of the Holder's entity;
- The Certification Agent of the Holder concerned.
- The Head of the CA CDC - LEGALIA.

The Holder is informed of the persons / entities liable to make a revocation request for his certificate at the time of his registration.

4.9.2.2 Certificates of a component of the PKI

Revocation of the certificate of the CA CDC - LEGALIA can be decided only by the Head of the CA or by judicial authorities following a court ruling.

Revocation of the certificates of the other components is decided by the entity operating the component (the RA or the CSP) concerned, which must inform the CA of it without delay.

4.9.3 Procedure for processing of a revocation request

4.9.3.1 Revocation of a Holder certificate

The requirements for identification and validation of a revocation request, made offline or online by the revocation management function, are described in chapter 3.4.

Revocation requests from Holders may be made:

- Online via an interface made available by the Certification Service Provider. The login URL for Holders is:
  - Authentication certificates (OID 1.2.250.1.5.1.1.1.2.2): https://igc-rev.caissedesdepots.fr/GroupeCDC/CDC/LEGALIA-AUTH:I
  - Signature certificates (OID 1.2.250.1.5.1.1.1.3.2): https://igc-rev.caissedesdepots.fr/GroupeCDC/CDC/LEGALIA-SIGN:I
- By mail using a form addressed to the DBR RA.

Revocation requests from the Certification Agent, the Holder's Legal Representative or the Head of the CA are handled by the Delegated RA. They must be made by mail using a form addressed to the DBR RA.

The practical information enabling this revocation to be carried out whatever the channel (online, by telephone or by e-mail) is available on the Caisse des Dépôts' institutional website at: http://www.caissedesdepots.fr/en/trusted-services-program.html

The process for self-service revocation by the Holder is as follows:

- The Holder logs in at the URL for revocation. This URL is indicated in a notification received by the Holder after validation of the certificate application. This notification also contains the revocation code which was chosen by the Holder in the application form.
- The Holder enters his revocation code.
- The Holder selects the certificate to be revoked and a reason for revocation.
- This triggers revocation by the CA. The serial number of the revoked certificate will appear in the next CRL published.
- The Holder and the RA receive a notification of the revocation.

- The operation is recorded in the event logs.

The process for revocation by the RA is as follows:

- A Registration Operator logs in to the CSP's interfaces. He authenticates himself using his certificate.
- He searches for the Holder using his e-mail address.
- The Registration Operator selects the certificate to be revoked together with a reason for revocation and sends the revocation request.
- This triggers revocation by the CA. The serial number of the revoked certificate will appear in the next CRL published.
- The Holder and the RA receive a notification of the revocation.
- The operation is recorded in the event logs.
- The operation is taken into account only during working days and hours.

The process for revocation by the Certification Agent, the Legal Representative, the Head of the CA or the Holder (identified in the paragraph below as the applicants) is as follows:

- The applicant logs in to the Certification Authority's publication website: http://www.caissedesdepots.fr/en/trusted-services-program.html
- The applicant downloads a revocation form.
- The applicant prints the form, fills it in and signs it.
  - Note: the Holder is identified by his e-mail address.
- The Legal Representative passes on the form to the RA.
- The RA takes charge of the request. The Registration Operator validates the signature of the applicant: Legal Representative, Certification Agent, Head of CA or Holder.
- If the request is from an authorised applicant (see above list), the Registration Operator follows the "process for revocation by the RA" presented above.
- The operation is taken into account only during working days and hours.

Remark: the Holder follows this process if the self-service revocation function is unavailable.

Remark: the reasons for definitive revocation of certificates are not published in the CRL.

4.9.3.2 Revocation of a certificate of a component of the PKI

Requests for revocation of one of the components of the CA are to be made to the Head of the Certification Authority, who will carry out the usual checks to qualify this request.

4.9.3.2.1 Case of the CA

In the event of a request for revocation of the CA's certificate, it will inform the RAs as quickly as possible. These RAs will in turn inform all the Certification Agents concerned as quickly as possible that the CA certificates issued on their behalf are no longer valid. The Certification Agents will have to inform the Certificate Holders, indicating to them explicitly that their certificates are no longer valid because one of the certificates in the certification chain is no longer valid. In parallel with the RAs, the CA must inform the CSP of the revocation of the CA's certificate.

4.9.3.2.2 Case of the RA

In the event of revocation of a certificate of one of the Registration Operators of the CA CDC - LEGALIA, the Head of the Delegated RA will make sure that there are still enough Registration Operators to guarantee CA service continuity.

4.9.3.2.3 Case of the CSP

In the event of revocation of a certificate of one of the departments of the CSP, the CSP must inform the CA of this as soon as possible and detail the impacts associated with this revocation for the CA.

4.9.4 Time granted to the Holder to make the revocation request

As soon as the Holder (or an authorised person) is aware that one of the possible reasons for revocation under his responsibility has arisen, he must make his revocation request without delay.

4.9.5 Time taken for processing of a revocation request by the CA

4.9.5.1 Revocation of a Holder certificate

The CA makes every effort to ensure that the maximum processing time between the revocation request and actual revocation is as short as possible.

Operationally, the online revocation management function is available round the clock. The Holder can access this service himself to carry out revocation of his certificate. In this case, revocation is immediate. The serial number of the revoked certificate will appear in the following CRL.

For the other modes of revocation, revocation requests are processed during working days and hours by the RA's personnel. This arrangement is agreed on if the certificate users are operational only during working days and hours.

In general, the Keynectis electronic certification service is accessible round the clock. The level of availability of the service (including the certificate revocation system) presents an unavailability of less than 4 hours per month, and a continuous unavailability of the service (incident of seriousness level 1) may not exceed 1 hour in working and non-working hours of operation.

4.9.5.2 Revocation of a certificate of a component of the PKI

In the event of revocation of a CA certificate, the CA informs the CSP which immediately revokes the certificate. This revocation then takes effect as soon as the serial number of the certificate appears in the CRL.

4.9.6 Requirements for checking of revocation by certificate users

The Users of the certificates issued by the CA CDC - LEGALIA (as defined in paragraph 1.3.4) must check the status of the Certification Authority's certificate, and of the certificates constituting the certification chain. The method used depends on the Holder and the constraints associated with the user applications.

By default, the Certificate Revocation List is made available in the form of a "CRL" file. The CRL publication URL is indicated in the CRLDP field of the certificate.

An online certificate status check service is also available at: http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/.

4.9.7 Frequency of drawing up of CRLs

CRLs are drawn up and published on the Internet every 24 hours. Information concerning the revocation status of a certificate is immediate in the OCSP service.

4.9.8 Maximum time taken for publication of a CRL

CRLs are made public and visible internationally within a maximum period of 24 hours. The period between completion of the generation of the CRL and its publication is less than 30 minutes. Information concerning the revocation status of a certificate is immediate in the OCSP service. Within this framework there is therefore no delay between the actual revocation of a certificate and the availability of this information to Users.

4.9.9 Availability of a system for online checking of the revocation and status of certificates

The CA CDC - LEGALIA uses an online certificate status check service (OCSP). This service enables a certificate to be checked in real time on each use of the certificate. This service is accessible round the clock. The level of availability of the service is 99 % on a monthly basis (unavailability less than 8 hours per month), and a continuous unavailability of the service (incident of seriousness level 1) may not exceed 2 hours in working and non-working hours of operation.

4.9.10 Requirements for online checking of revocation of certificates by certificate users

See 4.9.6.

4.9.11 Other available means of information on revocations

Not applicable.

4.9.12 Specific requirements in the event of compromise of the private key

For Holder certificates, the entities authorised to make a revocation request must do so as soon as possible after becoming aware of the compromise of the private key.

Requests for revocation of one of the components of the CA are to be made to the Head of the Certification Authority, who will carry out the usual checks to qualify this request.

In the event of revocation of a certificate of one of the Registration Operators of the CA CDC - LEGALIA, the Head of the RA will makes sure that there are still sufficient people representing the RAs, to ensure CA service continuity.

In the event of a request for revocation of the CA's certificate, he will inform the RAs concerned as quickly as possible. These RA will in turn inform all the Holders concerned as quickly as possible, indicating to them explicitly that their certificates are no longer valid because one of the certificates in the certification chain is no longer valid.

4.9.13 Possible reasons for a suspension

Not applicable: certificate suspension is not a service which is performed.

4.9.14 Origin of a suspension request

Not applicable.

4.9.15 Procedure for processing of a suspension request

Not applicable.

4.9.16 Limits of period of suspension of a certificate

Not applicable.

4.10 Certificate status information function

4.10.1 Operational characteristics

CRLs are published in v2 format and accessible on the Internet in the form of a list visible internationally to everyone.

4.10.2 Availability of the function

The certificate status information function is available round the clock. In general, the Keynectis electronic certification service is accessible round the clock. The level of availability of the service (including the publication service concerning certificate status) is 99 % on a monthly basis (unavailability less than 8 hours per month), and a continuous unavailability of the service (incident of seriousness level 1) may not exceed 2 hours in working and non-working hours of operation.

4.10.3 Optional systems

An OCSP service is available at http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/. This service allows the status of a certificate to be checked in real time and on each authentication or on each signature.

4.11 Termination of the relationship between the Holder and the CA

Termination of the relationship between the Holder and the CA is a reason for revocation.

4.12 Key sequestration and recovery

No key sequestration is carried out.

4.12.1 Policy and practices for recovery by sequestration of keys

Not applicable.

4.12.2 Policy and practices for recovery by encapsulation of session keys

Not applicable.

5 NON-TECHNICAL SECURITY MEASURES

The requirements presented in this chapter result from the risk management strategy defined by the steering committee of the Certification Authority. Details concerning the conditions for implementation of these requirements are given in the CPS.

5.1 Physical security measures

5.1.1 Geographical location and construction of sites

The geographical location of the sites does not require any particular measures regarding risks such as earthquakes, explosions or volcanic or flooding risks.

5.1.2 Physical access

Physical access to the functions for generation of certificates, generation of the Holder's secret information and revocation management is strictly limited to the persons authorised by name.

Physical access to the components of the CA supporting these functions is limited solely to authorised persons by the setting up of a physical security perimeter enabling separation of roles between the various persons involved. Access traceability is guaranteed.

Outside working hours, physical intrusion detection measures are implemented. Physical security measures are also introduced to limit access to sensitive media (key media, registration file, CPS and application documents).

5.1.3 Power supply and air conditioning

Backup measures are implemented to ensure that a power cut or an air conditioning failure do not affect the commitments made by the CA in terms of availability (management of revocations and information relating to certificate status in particular).

5.1.4 Vulnerability to water damage

The definition of the security perimeter takes water damage risks into consideration. Means of protection are implemented to guard against residual risks (e.g. burst pipes).

5.1.5 Fire prevention and protection

The fire prevention and fire-fighting means enable meeting of the commitments made by the CA in terms of availability (management of revocations and information relating to certificate status in particular) and archiving durability.

5.1.6 Media storage

The means of storage of the supports enable meeting of the commitments made by the CA in terms of restitution and archiving durability.

5.1.7 Withdrawal of media from service

Media considered to be sensitive in terms of confidentiality undergo destruction procedures or may be reused in an identical operational context for the same level of sensitivity.

5.1.8 Off-site backup

To enable post-incident resumption of service in accordance with the commitments made by the CA, off-site backups of critical information and functions are made. The

confidentiality of the information and the integrity of the backed-up applications are guaranteed in the same way on the operational site and on the backup site. This concerns the revocation management and certificate status information functions in particular.

5.2 Procedural security measures

5.2.1 Trusted roles

To ensure the security of the CA, a Steering Committee is set up, responsible for operational application of the CP through the implementing of the measures defined in the CPS.

The Steering Committee conducts or orders the conducting of the risk analyses on the perimeter for which it is responsible, decides on the risk management strategy and validates and follows up the corresponding action plans. It orders the conducting of the internal audits on its component and monitors the introduction of the necessary corrective measures.

The CA Steering Committee comprises five people, each having a role in the management of the Certification Authority's security.

The five functional trusted roles are as follows:

- **Security manager**: responsible for the implementation of the Certification Authority's security policy. He manages control of physical access to the equipment of the CA's systems. He is qualified to consult the archives and is responsible for analysis of the event logs to detect any incident, anomaly, attempted compromise, etc. He is responsible for certificate generation and revocation operations.
- **Application Manager**: The application manager is responsible for the implementing of the Certification Policy and the PKI Certification Practices Statement on the application for which he is responsible. His responsibility covers all of the functions performed by this application and the corresponding performances.
- **System engineer** - He is responsible for the start-up, configuration and technical maintenance of the CA's computer systems. He carries out technical administration of the CA's systems and networks.
- **Operator** - An operator within the CA operates the applications for the functions performed by the CA, within the framework of his attributions.
- **Controller**- Person designated by a competent authority and whose role is to regularly check the compliance of the implementing of the functions supplied by the CA with the certification policies, the certification practices statements of the PKI and the security policies.

A description of the roles and responsibilities of each person is given in the "Certification Practices Statement" of the CA CDC - LEGALIA and "Roles and Responsibilities".

5.2.2 Number of persons required per task

Depending on the task to be performed, one or more people may be present during the execution of the task. For the critical tasks of the CA, three people must be involved to ensure the quality and the security of these interventions.

5.2.3 Identification and authentication for each role

Identification and authentication measures are set up to support the implementing of the access control policy and operation tracking; the access control policy limits access solely

to authorised people in accordance with their need to know. The roles assigned are notified in writing to the persons concerned in their job description.

5.2.4 Roles requiring separation of attributions

Several roles may be assigned to the same person, provided that this combining of roles does not compromise the security of the functions implemented. For trusted roles, however, it is recommended that a given person does not hold several roles, and the following minimum requirements concerning non-combining of roles must be met.

Concerning trusted roles, the following combinations are prohibited:

- security manager and system engineer / operator
- auditor/controller and any other role
- system engineer and operator.

5.3 Security measures with regard to personnel

5.3.1 Qualifications, expertise and required accreditations

Any person called upon to occupy a role identified as being sensitive is subject to a confidentiality clause. The attributions of members of personnel operating on sensitive workstations correspond to their professional skills. The supervisory personnel have the appropriate expertise, and are familiar with the security procedures. Any person intervening in trusted roles is informed of his responsibilities (job description), and of the procedures associated with system security and monitoring of personnel.

5.3.2 Procedures for checking past history

Procedures for checking past history are set up for persons who are going to occupy a sensitive role. The CA requests in particular the production of a copy of their police record. These checks are carried out prior to the assignment of a trusted role and reviewed at least every three years.

5.3.3 Requirements in terms of initial training

Personnel are trained in the software, hardware and operating procedures of the Certification Authority

5.3.4 Requirements and frequency in terms of continuous training

Each change in systems, procedures or organisations leads to information or training of the personnel involved if this change affects their mode of work. The personnel involved are trained in incident management and are aware of the incident feedback organisation.

5.3.5 Frequency and sequence of rotations between different attributions

Rotation between attributions is carried at the time of a change of position or function of one of the persons with an operational role or a trusted role for the CA. The validity of the attributions, according to the positions actually occupied by the target persons, is reviewed in each internal audit.

5.3.6 Disciplinary measures in the event of unauthorised actions

The disciplinary measures in the event of unauthorised actions are indicated in the job definition or the personnel security charter (charter for use of computer, digital and technological resources) for sensitive roles held by CA personnel.

5.3.7 Requirements with respect to external service provider personnel

The requirements with respect to external service provider personnel are contractualised.

5.3.8 Documentation supplied to personnel

Personnel are informed of the security rules when they take up their position, in accordance with the role assigned to the person involved. Persons who are going to occupy an operational role in the Public Key Infrastructure have the corresponding procedures available to them.

5.4 Audit data constitution procedures

5.4.1 Type of events to be recorded

The following events are recorded:

- system events of the various components of the PKI (starting of servers, network access, etc.);
- technical events of the applications composing the PKI;
- functional events of the applications composing the PKI (certificate application, validation, revocation, rejection, etc.);
- creation / modification / deletion of user accounts (access rights) and the corresponding authentication data (passwords, certificates, etc.);
- physical access to premises;
- publication and updating of information associated with the CA;
- generation and then publication of CRLs
- actions to destroy and reset media containing confidential data (keys, activation data, personal information on Holders, etc.);
- Changes made to personnel.

These logs guarantee the traceability and attributability of the actions performed.

5.4.2 Frequency of processing of event logs

Event logs are analysed daily, and systematically in the event of reporting of an abnormal event.

5.4.3 Period of storage of event logs

The logs are stored on site for a maximum of one month before being sent to the archiving solution.

In accordance with French law, physical access recordings and video surveillance recordings are not kept for more than one month.

5.4.4 Protection of event logs

Event logs are accessible only to authorised CA personnel. They cannot be edited. Alarms are sent back in the event of modification of the logs or the parameters defining the content of the logs.

5.4.5 Event log backup procedure

Event logs are backed up every 30 days.

5.4.6 Event log collection system

An event log collection system is set up.

5.4.7 Notification of the recording of an event to the person responsible for the event

Not applicable.

5.4.8 Appraisal of vulnerabilities

Checking of the system and technical event logs is continuous and daily to enable anticipation of vulnerabilities and alert feedback in the event of vulnerabilities.

Operationally, the event log checking frequency is:

- Frequency of complete analysis of event logs: once a week and whenever an anomaly is detected.
- Frequency of checking of event logs for identification of failed access or operation attempts: once every 24 hours.
- Frequency of comparison of event logs: once a month.

Checking of functional event logs is carried out on demand in the event of a dispute, or for Certification Authority behaviour analysis.

5.5 Data archiving

The CA archives the following data itself, and reserves the right to delegate all or some of these obligations to a third party with which it will contract on the basis of these obligations.

5.5.1 Types of data to be archived

The CA data to be archived are as follows:

- CP and CPS;
- Certificates and CRLs published;
- Holder registration files and signed General Terms of Use, presented by the Certification Agents;
- Certification Agents' mandates;
- Attestations of unique identification of the Customers' company;
- Attestations of the Customers' Legal Representatives;
- Holder revocation forms;
- CA – RA agreements drawn up for the various lines of business covered by the CA;
- Event logs;
- Executable software and configuration files of:
    - The middleware installed on the customer's workstation;
    - The tools programmed at the Certification Service Provider Keynectis.

5.5.2 Archive storage period

The certificates of the CA are archived for 10 years. Registration files are archived over a period of one month in the archive office local to the RA before being transferred to the CA's archiving site for a period of 10 years. Certificates and CRLs are archived for 10 years. Event logs are archived for 10 years.

5.5.3 Archive protection

Whatever their medium, the integrity of archives is protected and they are accessible only to authorised persons. These archives are readable and usable throughout their life cycle.

5.5.4 Archive backup procedure

Archives are backed up securely, and accessible only to authorised persons (i.e. to the CA steering committee or to any person who has received authorisation from this steering committee).

5.5.5 Data time stamping requirements

Time stamping of logged event data is automatic. For this purpose, the components of the PKI are synchronised on the same server synchronised with universal time. Synchronisation is also set up between the internal infrastructures of the CA and the external infrastructures of the CSP.

5.5.6 Archive collection system

Not applicable.

5.5.7 Archive retrieval and checking procedure

Any archive retrieval request must be addressed to the Application Manager of the CA CDC - LEGALIA. Retrieval and checking of archives can be carried out for a period of 10 years. The archives are retrieved and checked within 2 working days at most.

5.6 CA key change

The service life of the keys of the CA CDC - LEGALIA is 10 years. Its renewal will be requested within a period at least equal to the service life of the certificates signed by the corresponding private key. This new CA will also be subject to a new audit.

The CA cannot generate a certificate whose end date is later than the expiry date of the corresponding certificate of the CA. The period of validity of the CA certificate must therefore be greater than that of the certificates the CA signs.

When a new CA key pair is generated, only the new private key is used to sign certificates. In the renewal process, Holders' requests will automatically be directed for signing to the new CA key pair.

The previous CA certificate remains usable to validate the certificates issued under this key until all the certificates signed with the corresponding private key have expired.

5.7 Restart following compromise and incident

5.7.1 Procedures for reporting and processing of incidents and compromises

Procedures (particularly personnel information and training) and means of reporting and processing of incidents (particularly analysis of the various event logs) are implemented.

A major incident – loss, suspected compromise, compromise or theft of a private key for certificate management, for example – must be immediately reported to the CA. Publication of the revocation of the certificate, if it proves to be necessary, is carried out urgently by any means necessary. The CA will then directly and without delay inform the contact identified on the website: http://www.references.modernisation.gouv.fr.

5.7.2 Restart procedures in the event of corruption of computer resources (hardware, software and/or data)

A continuity plan is set up to meet the availability requirements for the various components of the PKI. This continuity plan is specific to each business line branch of the CDC Group. This continuity plan is tested at least once a year.

5.7.3 Restart procedures in the event of compromise of the private key of a component

Compromise of a CA key leads immediately to the revocation of the corresponding certificate. Cases of compromise of the secret elements of the other components are dealt with in the business continuity plan.

5.7.4 Capacities for business continuity following an incident

The capacity for business continuity following an incident is also dealt with in the business continuity plan.

5.8 End of life of PKI

5.8.1 Transfer of activity or discontinuation of activity affecting a component of the PKI

One or more Components of the PKI may have to discontinue their activity or transfer it to another entity. Transfer of activity has no effect on the validity of the Certificates issued prior to the transfer in question, and the resumption of this activity is organised by the CA in collaboration with the new entity.

To ensure a constant level of trust during and after such events, the CA has taken the following measures:

- It has set up procedures enabling a constant service to be provided for RAs, Holders and their representatives (agents and legal representatives), in particular in terms of archiving (especially archiving of Holders' certificates and of information relating to certificates)
- It ensures the continuity of the archiving service;
- It ensures the continuity of the Revocation service;
- It informs the Certification Agents if the envisaged changes may have repercussions on the commitments made.

If the envisaged changes may have repercussions on commitments to Holders or certificate users, the CA undertakes to inform them of this transfer as soon as possible and at least one month beforehand.

The CA will communicate as soon as possible, to the representative of the DGME, the principles of the action plan implementing the technical and organisational resources to organise the transfer of activity. It will present in particular the systems set up for archiving (keys and information relating to certificates) in order to perform or ensure the performing of this function over the whole period initially stipulated in its CP. The CA will also communicate to the DGME, according to the various components of the PKI concerned, the procedures for the changes which have occurred.

The CA will measure the impact and draw up an inventory of the consequences (legal, economic, functional, technical, communicational, etc.) of this event. It will present an action plan to eliminate or reduce risks for the applications and inconvenience for Holders and certificate users. The CA will keep the DGME informed of any obstacle or additional delay encountered in the implementing of the process.

Discontinuation of activity affects the activity of the CA, as defined below.

5.8.2 Discontinuation of activity affecting the CA

Discontinuation of activity affects the validity of the Certificates issued prior to the discontinuation concerned, and a specific procedure is implemented in such cases.

If the envisaged changes may have repercussions on commitments to Holders or certificate users, the CA undertakes to inform them of this discontinuation as soon as possible and at least one month beforehand.

In the event of discontinuation of activity, the CA undertakes to comply with the following principles:

- Inform the Holders, Certification Agents, and representatives of the RA at least one month in advance;
- The private key for issuing of certificates will in no case be passed on;
- All necessary steps will be taken to destroy it or render it inoperative;
- The CA certificate will be revoked;
- All issued certificats which are still valid will be revoked;
- All certification agents responsible for the certificates which have been revoked or are to be revoked will be kept informed.

The CA will communicate as soon as possible, to the representative of the DGME, the principles of the action plan implementing the technical and organisational resources to deal with the discontinuation of activity. It will present in particular the systems set up for archiving (keys and information relating to certificates) in order to perform or ensure the performing of this function over the whole period initially stipulated in its CP. The CA will also communicate to the DGME, according to the various components of the PKI concerned, the procedures for the changes which have occurred.

The CA will measure the impact and draw up an inventory of the consequences (legal, economic, functional, technical, communicational, etc.) of this event. It will present an action plan to eliminate or reduce risks for the applications and inconvenience for Holders and certificate users. The CA will keep the DGME informed of any obstacle or additional delay encountered in the implementing of the process. The representatives of the CA steering committee must meet to perform the sensitive operations of deactivation of CA keys and revocation of previously issued certificates.

6 TECHNICAL SECURITY MEASURES

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

6.1.1.1 CA keys

The keys of the CA CDC - LEGALIA are generated in the key ceremony, in the presence of the CA steering committee, and in accordance with the procedure indicated by the master of ceremonies. This key ceremony session takes place under the control of a ministerial public officer checking correct application of the procedures and compliance with the security requirements defined in this document and in the Certification Practices Statement.

6.1.1.2 Holder keys generated by the CA

Not applicable.

6.1.1.3 Holder keys generated by the Holder

The private key is generated on the Holder's SSCD physical medium at the time of collection of his certificate. A personal PIN code chosen by the Holder protects access to the content of the physical medium: the Holder's private key remains under his exclusive control.

6.1.2 Sending of the private key to its owner

The private key is generated locally at the time of the collection triggered by the (future) Holder of the certificate, either on the SSCD physical medium protected by a personal PIN code, or in software form in the Holder's certificate store.

The physical medium used by the Certification Authority CDC - LEGALIA is of the "SSCD qualified" type. It guarantees the security of exchanges between the physical medium and the various components of the Certification Authority.

6.1.3 Sending of the public key to the CA

Not applicable for the CA's public key. In the case of the Holder's public key, it is sent to the CA via a channel guaranteeing the integrity and authentication of the transmission, in the certificate collection phase.

6.1.4 Sending of the CA's public key to certificate users

The CA's signature check public keys are made available to certificate users, and are publicly consultable as defined in section 2.2.2.

6.1.5 Size of keys

The key sizes are as follows:

- 2048 bits for the keys of the CA CDC - LEGALIA.
- 2048 bits for Holders' keys for an authentication certificate (OID 1.2.250.1.5.1.1.1.3.2) or a signature certificate (OID 1.2.250.1.5.1.1.1.3.2).

6.1.6 Checking of generation of key pair parameters and their quality

See chapter 7.

6.1.7 Purposes of uses of the key

Use of the private key for the CA CDC - LEGALIA, and of the associated certificate, is limited to the signing of Holder certificates and CRLs. The CA private key is used only in a secure environment, in a hardware security module (HSM).

The Holder makes a commitment to the CDC, by signing the certificate application form and the corresponding General Terms of Use, to use his certificate only for purposes of authentication (OID 1.2.250.1.5.1.1.1.2.2) or signature (OID 1.2.250.1.5.1.1.1.3.2) on the target applications defined in 1.4.1. Any other use is made under the Certificate Holder's responsibility.

6.2 Security measures for protection of private keys and for cryptographic modules

6.2.1 Standards and security measures for cryptographic modules

6.2.1.1 CA cryptographic module

The CA cryptographic module for generation and use of signature keys meets the requirements stipulated by the regulations. It is a hardware security module, meeting the level EAL4+ common criteria, dedicated to the management of the Caisse des Dépôts' certificates. The cryptographic module for signature of certificates and revocation information undergoes no unauthorised handling during its transport or storage.

6.2.1.2 Holder authentication devices

The CA supplies the Holder with a hardware device for private key storage. Holders are responsible for the confidentiality of their activation data (PIN code). Holders' private keys are used only in a secure environment, in the physical medium evaluated at level EAL4+ and SSCD-qualified by ANSSI ("MultiApp ID IAS ECC on NXP component" range).

6.2.2 Control of private key by several people

Control of the private key of the CA CDC - LEGALIA is carried out by at least three members of the steering committee, who are present simultaneously to make the use of these keys possible. Holders' private keys are under their exclusive control.

6.2.3 Sequestration of private key

The private key of the CA CDC - LEGALIA, and Holders' private keys, do not undergo sequestration.

6.2.4 Backup copy of private key

A backup copy is made of the private key of the CA CDC - LEGALIA. Such backup copies benefit from the same level of security as the original private key. No backup copy is made of Holders' private keys.

6.2.5 Archiving of private key

The private keys of the CA CDC - LEGALIA, and Holders' private keys, do not undergo archiving.

6.2.6 Transfer of private key to / from the cryptographic module

No transfer of the private key of the CA CDC - LEGALIA is possible because it is generated and stored by the same HSM. The only transfer possible is the transfer of

private keys to the Backup HSM, from the backup copy (see above). No transfer of Holders' private keys is possible.

6.2.7 Storage of private key in a cryptographic module

The private key of the CA and Holders' private keys are stored by the cryptographic hardware (respectively the HSM, USB key or smart card) under the security conditions defined by their respective protection profiles supporting the EAL 4+ evaluation.

6.2.8 Method of activation of private key

6.2.8.1 CA private keys

Activation of the private key of the CA CDC - LEGALIA requires the presence of at least three members of the steering committee.

6.2.8.2 Holders' private keys

Activation of the private key of a Holder requires entry of the PIN code of the physical medium, and is under the Holder's exclusive control.

6.2.9 Method of deactivation of private key

6.2.9.1 CA private keys

The private key of the CA CDC - LEGALIA can be deactivated from the cryptographic module. This deactivation requires the presence of at least three members of the steering committee.

6.2.9.2 Holders' private keys

Not applicable.

6.2.10 Method of destruction of private keys

6.2.10.1 CA private keys

Destruction of the private key of the CA can be carried out only from the cryptographic module (HSM).

6.2.10.2 Holders' private keys

Destruction of the private key of a Holder can be carried out only from the physical medium.

6.2.11 Level of qualification of cryptographic module and authentication devices

The cryptographic modules of the CA and of Holders' private keys have undergone an EAL 4+ evaluation.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

The public keys of the CA CDC - LEGALIA, and the Holders' public keys are archived within the framework of the certificate archiving policy (see 5.5).

6.3.2 Service life of key pairs and certificates

The signature keys and certificates of the CA CDC - LEGALIA have a service life of 10 years. Holders' signature keys and certificates have a service life of 3 years.

6.4 Activation data

6.4.1 Generation and installation of activation data

6.4.1.1 Generation and installation of activation data corresponding to the private key of the CA

The elements necessary for activation of the private key of the CA are generated securely and only accessible to the members of the steering committee, the only people authorised to carry out this activation.

6.4.1.2 Generation and installation of activation data corresponding to the Holder's private key

The elements necessary for activation of Holders' private keys (PIN code of the physical medium) are to be defined by the Holder at the time of installation of the physical medium. This system requires prior installation of the tools enabling the operating system used by the Holder to communicate with the physical medium.

The CA checks that the activation code used by the Holder is secure, applying a password policy aimed at rejecting over-simple passwords. This password management policy is directly integrated in the configuration of the tools necessary for use of the physical medium. The password management policy is therefore explicitly presented to the Holder in PIN code change operations. In this case the Holder is asked to give the old PIN code.

Policy for PIN code
The policy is as follows:

- The password must comprise 6 characters, and it must include numerals from "0" to "9".
- Use of the previous PIN is prohibited.
- Sequences of 6 identical characters are prohibited.
- In addition, the following PIN codes are prohibited: "123456", "012345", "654321" and "543210".

6.4.2 Protection of activation data

6.4.2.1 Protection of activation data corresponding to the private key of the CA

CA key activation data are supplied only to the members of the steering committee. Their identity is kept in a documentary database maintained by the CA CDC - LEGALIA.

6.4.2.2 Protection of activation data corresponding to Holders' private keys

A Holder's activation data are known only to the Holder, and under his exclusive control.

6.4.3 Other aspects associated with activation data

Not applicable.

6.5 Computer system security measures

6.5.1 Technical security requirements specific to computer systems

6.5.1.1 Identification and authentication

The systems, applications and databases identify and authenticate users uniquely. Any interaction between the system and a user is possible only after successful identification

and authentication. For each interaction, the system establishes the identity of the entity. Authentication information is stored in such a way that it is only accessible to authorised users.

6.5.1.2 Access control

Profiles and access rights to the CA's equipment are defined and documented, together with Holders' registration procedures. The systems, applications and databases can distinguish and administrate the access rights of each user on objects subject to administration of rights, at user level, at user group level or at both levels. It is possible to:

- Completely refuse access to an object to users or user groups,
- Limit a user's access to an object solely to operations which do not modify this object,
- Grant access rights to an object individually down to individual user level.

Someone who is not an authorised user cannot grant or withdraw access rights to an object. Similarly, only authorised users can introduce new users or delete or suspend existing users.

6.5.1.3 Administration and operation

Use of utility programs is restricted and controlled.
The operational administration and operating procedures of the Certification Authority are documented, monitored and regularly updated.
The start-up conditions (initial security parameters of the servers) are documented.

The end-of-life conditions (destruction and discarding) of the equipment are documented to guarantee non-disclosure of the sensitive information which they may contain.

All sensitive hardware of the PKI undergoes maintenance procedures to guarantee the availability of the functions and information.
Maintenance action checking measures are applied.

6.5.1.4 Integrity of components

Control, detection and prevention measures are implemented on all the components of the PKI to provide protection against malicious software. The components of the local area network are kept in a physically secure environment; periodic checks of the conformity of their configuration are carried out.

6.5.1.5 Flow security

Security measures are implemented to guarantee the origin authentication, integrity and confidentiality (if necessary) of the data exchanged between entities intervening in the process.

6.5.1.6 Logging and audit

Activity can be monitored via the event logs.

6.5.1.7 Supervision and control

Permanent surveillance is set up and alarm systems installed to detect, record and react quickly to any unauthorised and/or illicit access to (physical and/or logical) resources.

6.5.1.8 Awareness

Appropriate procedures to enhance the awareness of PKI users are implemented.

6.5.2 Level of qualification of computer systems

- The hardware security module (HSM) and Holders' physical media are evaluated at level EAL4+.
- The physical media of the "MultiApp ID IAS ECC on NXP component" range are qualified at reinforced level (see the ANSSI website: http://www.ssi.gouv.fr/site_rubrique52_p_35_carte_MultiApp_IAS_ECC.html).
- The technical service supplied by the CSP is qualified (see the ANSSI website: http://www.ssi.gouv.fr/site_rubrique52.html).

6.6 Security measures for systems during their life cycle

6.6.1 Security measures associated with system development

The development and test infrastructures are separate from the operational infrastructures of the PKI. The criteria for acceptance and validation of new information systems, upgrades and new versions are documented and appropriate tests of the system are performed before its acceptance and placing in production.

6.6.2 Measures associated with security management

The PKI is monitored as part of the setting up of the CA's security management system. The steering committee manages feedback to the CA which is informed of any significant change. Changes to the components lead to updating of the operational procedures.

6.6.3 Level of security appraisal of system life cycle

Not applicable.

6.7 Network security measures

The measures introduced are in line with the CDC's risk management strategy for information systems. The CA is implanted in a network protected by at least two levels of "firewall" type gateways. These gateways are configured to only accept flows which are strictly necessary. Network communications carrying confidential data are subject to protective measures against data tapping. Periodic vulnerability detection scans on the PKI equipment are conducted. Security gateways are set up to protect the local component of the information system against unauthorised access.

6.8 Time stamping / dating system

See 5.5.5.

7 CERTIFICATE, OSCP AND CRL PROFILES

7.1 Certificate profiles

The certificates of the CDC PKI are in X509v3 format.

7.1.1 Certificate of the CA CDC - LEGALIA

```
    Data:
        Version: 3 (0x2)
        Serial Number: 11:21:0a:35:c8:2b:57:cf:e7:69:fd:c8:55:5f:f1:a6:a9:5f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=CDC - RACINE
        Validity
            Not Before: Nov 17 00:00:00 2009 GMT
            Not After : Nov 15 00:00:00 2019 GMT
        Subject: C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=CDC - LEGALIA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:d5:60:28:38:18:22:79:57:55:92:95:88:fa:de:
                    a5:9d:1f:a4:b9:61:c8:a5:00:f8:4f:d8:02:4d:95:
                    01:18:52:b3:7f:31:88:03:9e:ee:af:d8:f4:65:60:
                    67:af:63:5a:83:2f:9f:c1:ce:fb:8b:3c:02:f5:c4:
                    e2:ca:25:95:0c:a1:ef:e3:eb:d8:53:16:be:cf:51:
                    f0:14:97:f3:00:e8:79:4a:b9:da:54:c3:21:b3:90:
                    db:34:4d:9e:11:ee:0c:37:3d:ad:53:e2:4a:a1:7c:
                    93:a6:55:17:01:7a:e1:55:ac:ef:c6:d9:ae:14:fc:
                    0d:12:0d:42:90:b3:09:2a:e9:40:bc:08:70:68:52:
                    8e:a8:63:51:c7:e0:b1:12:84:d9:c0:70:91:f5:fb:
                    a5:3b:ec:08:13:2d:ec:b1:7f:3d:d4:8d:f2:ea:5d:
                    e2:b5:17:a3:31:af:26:2f:da:f7:ac:7e:1e:f9:97:
                    36:82:f2:e5:a8:a4:ee:fc:21:5b:f2:d9:b1:a0:9d:
                    81:58:67:b2:d5:cd:a2:28:6d:d7:4d:87:ba:7d:14:
                    7f:52:8f:37:a1:bf:52:01:08:61:44:09:35:79:3b:
                    96:e5:38:4e:fc:af:8d:8e:cb:2b:36:ba:c0:39:f0:
                    fd:4f:8e:85:f2:7d:24:28:12:6b:97:51:25:16:bc:
                    93:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                OCSP - URI:http://igc-ocsp.caissedesdepots.fr/ocsp-racine/
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: http://igc-pc.caissedesdepots.fr/pc-racine.pdf
            X509v3 CRL Distribution Points:
                URI:http://igc-crl.caissedesdepots.fr/cdc/racine.crl
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                04:16:3A:3F:01:62:EC:FA:D6:DB:5D:64:2B:7E:03:E0:94:85:A2:E5
            X509v3 Authority Key Identifier:
                keyid:78:D3:33:04:E2:2A:ED:94:09:2A:15:E1:0C:4E:33:F9:F2:F7:07:7D
    Signature Algorithm: sha256WithRSAEncryption
        10:1a:ea:d4:9b:b2:d5:7c:bf:6a:2d:a8:4e:dc:d1:b3:e0:4b:
        67:0e:c1:e1:d5:25:11:e8:0f:a1:4d:14:10:f7:3d:c2:ac:d7:
        fa:d8:f8:79:bc:09:1e:ab:5c:ba:67:bc:23:85:c1:46:0a:78:
        2e:b6:c2:8d:ed:a5:4b:a5:cc:3e:63:91:43:ab:32:a3:a5:00:
        87:04:7b:2b:d6:5d:f4:37:6e:02:3d:b3:4b:c2:cb:24:9e:5f:
        0d:7d:fd:96:c4:e8:e6:52:75:6a:12:18:d3:40:07:bb:39:e0:
        fe:00:95:62:6b:14:cb:46:d6:04:cd:e1:e0:db:e6:cc:9a:41:
        3d:39:7c:06:d0:92:8b:2b:15:f0:dd:60:fc:a7:c0:b4:29:2c:
        3f:3b:4b:97:6e:b0:8c:00:9a:4e:be:0f:ef:a5:35:6e:2d:50:
        16:33:b3:32:55:ce:87:95:7f:ec:be:38:81:68:ee:19:54:96:
        10:ab:22:2c:e1:89:3c:d7:ac:b5:66:5b:e6:df:3b:71:7f:0d:
        59:6d:66:7c:cd:1b:e3:41:4b:c9:fe:1b:9a:fb:3a:ff:01:1f:
        e8:35:8f:b5:88:fb:a7:13:89:5e:4d:57:46:83:28:c3:62:b3:
        5e:73:eb:26:df:61:45:86:60:4a:57:27:e9:f8:51:64:26:56:
        57:ab:94:dd
```

7.1.2 Holders' certificate

7.1.2.1 Basic fields

```
Data:
    Version: 3 (0x2)
    Serial Number: 21:21:71:8a:cc:1f:73:7f:85:37:22:c4:ee:4b:d9:06:92:6b
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=CDC - LEGALIA
    Validity
        Not Before: Jul 22 13:12:21 2010 GMT
        Not After : Jul 22 13:12:21 2013 GMT
    Subject: C=FR, O=Entite, OU=0002 SIREN ou SIRET, CN=Prenom NOM
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit): [...]
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Key Usage: critical
            Digital Signature (OID : 1.2.250.1.5.1.1.1.2.2)
            Non Repudiation   (OID : 1.2.250.1.5.1.1.1.3.2)
        Authority Information Access:
            OCSP - URI:http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/
        X509v3 Certificate Policies:
            Policy: 1.2.250.1.5.1.1.1.3.1
              CPS: http://igc-pc.caissedesdepots.fr/pc-legalia-sign.pdf
        X509v3 CRL Distribution Points:
            URI:http://igc-crl.caissedesdepots.fr/cdc/legalia.crl
        X509v3 Subject Alternative Name:
            email:augustin.deromanet@caissedesdepots.fr
        X509v3 Subject Key Identifier:
            F7:AD:51:43:D1:2A:B7:DA:4B:57:B0:43:65:1A:11:9B:5D:24:BF:5C
        X509v3 Authority Key Identifier:
            keyid:04:16:3A:3F:01:62:EC:FA:D6:DB:5D:64:2B:7E:03:E0:94:85:A2:E5
Signature Algorithm: sha256WithRSAEncryption [...]
```

7.2 Certificate revocation list profile

The DN of the issuer of the revocation list is the name of the Certification Authority signing this CRL. Revoked certificates are listed and named by their serial number. The revocation date is specified. For each certificate revoked, the reason for revocation will not be published.

The CRLs issued present the following characteristics:

- The version of the CRL is v2.
- The signature algorithm is sha256WithRSAEncryption.
- The CRL Number & Authority Key Identifier extensions will be presented.
- Period of validity: 7 days
- Update interval: 24 hours
- Publication http URL (CRLdp): http://igc-crl.caissedesdepots.fr/cdc/legalia.crl

7.3 OCSP profile

The OCSP service is operated by the CA's Certification Service Provider. For Holder certificates, it is accessible via the URL:
http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/

8 CONFORMITY AUDIT AND OTHER APPRAISALS

8.1 Frequencies and/or circumstances of appraisals

Checking of conformity with the CP may be carried out at the request of the steering committee of the Certification Authority and under the Controller's responsibility. The CA undertakes to carry out this check at least once a year.

In addition, before the first placing in service of a component of its PKI or following any significant change in a component, the CA will also check the conformity of this component.

At the time of RGS referencing of the Certification Authority CDC - LEGALIA, an initial audit was carried out by LSTI, in accordance with the regulatory procedures in force.

8.2 Identities / qualification of appraisers

The controller must carry out his work rigorously to make sure that the policies, declarations and services are correctly implemented and detect cases of non-conformities which could compromise the security of the service provided. The CA undertakes to appoint internal controllers with expertise in information system security, particularly in the field of activity of the component checked. The persons who may perform these checks for the CA CDC - LEGALIA are defined in the Certification Practices Statement.

For the first referencing audit, LSTI was mandated. LSTI is a private certification body specialising in the field of information security. LSTI is independent from all manufacturers, suppliers or service providers.

8.3 Relationship between appraisers and appraised entities

The controller is designated by the CA, which authorises him to check the practices of the component concerned by the audit. He will be independent from the CA and the RA.

8.4 Subjects covered by appraisals

The controller carries out conformity checks on the audited component, concerning all or part of the implementation of the:

- certification policies;
- certification practices statements;
- certification services implemented.

For each specific audit, the controller will draw up an audit programme precisely defining the component of the PKI concerned by the audit. This check will be carried on each placing in service of a new component or major modification of an existing component. Every year, the auditors will propose to the person responsible for the application a list of components and procedures which they will wish to check, and thus draw up the detailed programme of the audit.

8.5 Actions taken as a result of appraisals

Following a conformity check, the audit team gives the CA its verdict, which may be "success", "failure" or "to be confirmed".

In the event of failure, the audit team submits recommendations to the CA and describes the level of criticality and the identified flaws to be corrected. Depending on the importance of the non-conformities, the audit team makes recommendations to the CA

which may be (temporary or permanent) discontinuation of activity, revocation of the component's certificate, revocation of all certificates issued since the last positive check, etc. It is then up to the CA to choose the steps to be taken.

In the event of a "to be confirmed" result, the audit team identifies the non-conformities, and prioritises them. It is up to the CA to propose a timetable for correcting the non-conformities; a verification check will allow the non-conformities identified to be lifted. In the event of success, the CA confirms to the audited component its compliance with the requirements of the CP.

8.6 Communication of results

The results of the audit will be kept at the disposal of the steering committee of the Certification Authority and of the qualification body responsible for the qualification of the CA.

9 OTHER PROFESSIONAL AND LEGAL ISSUES

9.1 Price rates

9.1.1 Price rates for supply or renewal of certificates

The certificates are issued by the Caisse des Dépôts (CDC), which reserves the right to invoice their issuing, or to invoice related services such as providing the revocation list.

9.1.2 Price rates for accessing certificates

The certificates are issued by the Caisse des Dépôts (CDC), which reserves the right to invoice their issuing, or to invoice related services such as providing the revocation list.

9.1.3 Price rates for accessing certificate status and revocation information

The certificates are issued by the Caisse des Dépôts (CDC), which reserves the right to invoice their issuing, or to invoice related services such as providing the revocation list.

9.1.4 Price rates for other services

The certificates are issued by the Caisse des Dépôts (CDC), which reserves the right to invoice their issuing, or to invoice related services such as providing the revocation list.

9.1.5 Refund policy

No specific requirements.

9.2 Financial liability

9.2.1 Coverage by insurance

Risks liable to entail the CDC's liability are covered internally by the CDC, which is its own insurer.

9.2.2 Other resources

The CDC confirms that it has a sufficient financial guarantee specially allocated to coverage of the financial risks relating to its PSCE activity.

9.2.3 Coverage and guarantee concerning user entities

Coverage and guarantee concerning user entities.

9.3 Confidentiality of professional data

9.3.1 Perimeter of confidential information

The CA sets up an inventory of all information assets and classifies them to define protection requirements according to needs.

In particular, the following information is treated as being confidential:

- The private keys of the CA CDC – LEGALIA and of the Holders' certificates;
- Personal information (surname, first name and e-mail address) collected concerning Holders and Certification Agents in the certificate application process;
- Activation data (PIN code for access to the physical medium or secret data for activation of the HSM);
- Event logs;

- Audit reports;
- Reasons for revocation of certificates.

9.3.2 Information outside the confidential information perimeter

Not applicable.

9.3.3 Responsibilities in terms of protection of confidential information

Confidential information is accessible only to persons concerned by such information or who are obliged to store and/or process such information.
The CDC undertakes to handle all confidential information collected in compliance with the laws and regulations in force.

The confidential information listed above will be communicated externally only for the strict requirements of management of the operations performed in execution of the CPS, to meet legal requirements or for the execution of services entrusted to third parties, it being specified that said third parties are contractually bound by an obligation of confidentiality.

9.4 Protection of personal data

9.4.1 Personal data protection policy

Technical, procedural and organisational measures are set up to guarantee protection of the personal data collected at the time of registration. The CDC complies with the legal and regulatory provisions in force concerning collection and processing of personal data. In application of the French Data Protection Act of the 6th of January 1978, individuals have a right to access, correct or object to personal data concerning them. This right may be exercised by sending an e-mail to the Registration Authority.

9.4.2 Personal information

The personal information is the personal information concerning the Holder and the Certification Agent recorded in the registration file. It consists of the surname / first name / e-mail address information and reasons for revocation.

9.4.3 Non-personal information

No specific requirement.

9.4.4 Responsibility in terms of protection of personal data

Naturally, all collection of personal data by the CA is carried out in strict compliance with the laws and regulations in force, in particular the French Data Protection Act of the 6th of January 1978. The CA confirms that it has carried out the declaration formalities incumbent on it with respect to this CP and the handling of personal data consequently performed.

9.4.5 Notification and consent to use of personal data

The Holder is informed of the use made by the CA of these personal data at the time of signing of the General Terms of Use of Certificates during registration. He personally signs these terms of use, thereby indicating his acceptance and consent.

9.4.6 Conditions for disclosure of personal information to judicial or administrative authorities

Recorded information may be made available if need be to serve as proof in a judicial or administrative procedure.

9.4.7 Other circumstances of disclosure of personal information

No specific requirement.

9.5 Intellectual and industrial property rights

During the performing of the services defined in this document, elements protected by legislation on copyright or databases may be exchanged or used. Such elements, together with the associated intellectual property rights, will remain the property of the holder of the corresponding rights. The beneficiary of the services will have the right to reproduce these elements for his own internal use. He may not, without the prior permission of the holder of the rights, make available to third parties, extract or reuse these elements or derived works or copies, particularly software and databases, either in whole or in part.

Through his registration, the Holder acquires, for the encryption creation data submitted to him by the RA, only a right of use limited to operations performed in accordance with this Certification Policy and the contractual terms of use of the service. The Holder does not acquire any property right of any nature over the certificates and key pairs, which he undertakes to return to the RA and to cease to use in the cases stipulated in this document or in the general terms of use of the service.

9.6 Contractual interpretations and guarantees

9.6.1 Certification Authorities

The CDC is responsible, as a PSCE, for:

- validation and publication of the CP,
- validation of the CPS and its compliance with the CP,
- compliance of issued certificates with this CP,
- compliance with all the security principles by the various components of the PKI, and the related checks.

The CDC deals with any damaging consequences resulting directly from failure to comply with this document by itself or by one of the entities of the PKI, in accordance with the principles of civil liability. The CDC undertakes to use the means described in this CP to ensure the security of the services, take the necessary actions to correct non-conformities following a conformity audit and enable the issuing and delivery of the certificate, the implementing of the certificate renewal and revocation procedures and the publication of this CP and the Certificate Revocation List.

Unless it can demonstrate that it has committed no intentional fault or negligence, the CDC is responsible for any damages caused to any individual or legal entity placing reasonable trust in the certificates issued in each of the following cases:

- The information contained in the certificate does not correspond to the information supplied at the time of registration
- The issuing of the certificate has not led to checking that the Holder possesses the corresponding private key
- The CA has not registered the revocation of a certificate and published this information in accordance with its commitments.

The CDC is not responsible for any damages caused by use of the certificate outside the limits defined for its use.

9.6.2 Registration service

The RA undertakes to use the means described in this CP complemented by the "CA - RA Agreement" for the business line in question, and complemented by the CPS for:

- checking of the compatibility of the information collected with that required by this CP for the issuing of Holder certificates;
- the conformity of the information contained in the certificate with the information collected for certificate issuing purposes;
- checking of the supporting documents which have been supplied to it to support the identification of the Certification Agent (if any) and the Holders;
- checking of the authenticity of a revocation request which is submitted to it,
- protection of its private keys and its activation data used within the framework of its relations with the CA.

9.6.3 Certificate Holders

The Holder has a duty to:

- supply correct and up-to-date information at the time of the certificate application, and when making renewal requests;
- use the certificates of the CA CDC - LEGALIA only for purposes of authentication (OID 1.2.250.1.5.1.1.1.2.2) or signature (OID 1.2.250.1.5.1.1.1.3.2) in accordance with the Certification Policy of the CA;
- use the physical medium (supplied by the CDC) to collect the certificate;
- protect his private key by means appropriate to his environment;
- protect the activation data of the corresponding key pair (PIN code);
- comply with the terms of use of his private key and the corresponding certificate;
- inform the CA of any change concerning the information contained in his certificate;
- make a request for revocation of his certificate to the RA, the Certification Agent or the CA without delay in the event of:
    - loss or theft of the USB key or the smart card
    - compromise or suspected compromise of his private key
- cease all use of the certificate and the associated private key in the event of discontinuation of the activity of the CA or revocation of the Certification Authority's certificate by the CDC.

The relationship between the Holder and the CA is formalised by a Holder commitment defined in the General Terms of Use of the certificate.

9.6.4 Certificate users

The users of the certificates must:

- Check the use for which the certificate has been issued;
- Check that the certificate used has been issued by the CA CDC - LEGALIA;
- Check that the Holder's certificate is not included in the revocation lists of the CA CDC - LEGALIA;
- Check the signature of the Holder's certificate and of the certification chain up to the CA "CA CDC RACINE" and check the validity of the certificates.

9.6.5 Other participants

9.6.5.1 Certification Agents

The Certification Agent has a duty to:

- Identify the Holder in accordance with the requirements defined in the "CA - RA Agreement" for the business line concerned;

- Guarantee the authenticity, completeness and up-to-date nature of the information communicated in the certificate application and of the documents accompanying this information;
- Inform the RA and the CA without delay of any change relating to this information and/or these documents;
- Provide information to Certificate Holders on the General Terms of Use of certificates, management of keys or the equipment and software enabling them to be used;
- Have the private key of each Certificate Holder protected by means appropriate to his environment;
- Have the activation data (PIN code) of each Holder protected by means appropriate to his environment;
- Ensure that each Holder complies with the General Terms of Use of the private key and the corresponding certificate;
- Ensure that the revocation of a certificate is requested whenever necessary,
- Ensure that the RA or the CA are informed without delay in the event of suspected compromise or compromise of the private key of one of its Certificate Holders.

9.7 Limits of guarantee

No specific requirement.

9.8 Limits of liability

Subject to any applicable public provisions, the CDC may not be held responsible for any unauthorised or incorrect use of the certificates, the associated private keys and activation data, the CRLs or any other equipment or software made available.

The CDC declines in particular any responsibility for any damages resulting from:

- use of the key pairs for a use other than those stipulated;
- use of revoked or expired certificates;
- absence of revocation of a certificate leading to the use of the certificate and the key pair by an unauthorised third party;
- a case of force majeure as defined by French courts.

The CDC also declines any responsibility for any damages resulting from errors or inaccuracies in the information contained in the certificates, when these errors or inaccuracies result directly from the erroneous nature of the information communicated by the Holder or the Certification Agent.

9.9 Compensation

No specific requirement.

9.10 Period of validity and early expiry of CP

9.10.1 Period of validity

This document is applicable until the end of the service life of the last certificate issued under this CP.

9.10.2 Early expiry

Except in exceptional circumstances relating to security, changes in this document do not necessitate the revocation of certificates already issued.

9.10.3 Effects of expiry and clauses remaining applicable

No specific requirement.

9.11 Individual notifications and communication between participants

In the event of a change of any nature in the composition of the PKI, the CDC will have this change validated by way of a technical appraisal and will analyse the impact in terms of security and quality of service provided.

If necessary, a special information procedure will be conducted to notify the components of the CA of the changes to be taken into account, with reasonable prior notice before the changes come into effect.

9.12 Amendments to the CP

9.12.1 Amendment procedures

The CA makes any changes to the specifications stipulated in the CP and the CPS and/or to the Components of the CA which it considers necessary for improvement of the quality of the Certification services and the security of the processes. The CA also makes any changes to the specifications stipulated in the CP and the CPS and/or to the Components of the CA which are made necessary by legislation, applicable regulations or audit results. The Application Manager of the CA CDC – LEGALIA is responsible for the Certification Policy amendment procedure. The CDC undertakes to check that any change made to this document remains in line with the objectives of compliance with the regulatory requirements associated with the service provided.

9.12.2 Mechanism and period of information on amendments

All components and players in the PKI are kept informed of the amendments made on the CP and the resulting effects for them.

9.12.3 Circumstances in which the OID must be changed

Any major change to the CP which has a major impact on the certificates already issued will be marked by a change in the OID (see 1.2).

9.13 Provisions concerning settlement of disputes

In accordance with existing legislation and the regulations in force, certificates issued under this Certification Policy are certificates whose terms of use are defined by this Certification Policy and by the general terms of use which define relations between the PKI of the CDC and its users. Relations between the CDC and the Holder of the certificate are governed by the General Terms of Use of the certificate.

9.14 Jurisdiction

This Certification Policy is subject to French law.
For contractual matters, any dispute relating to the validity, interpretation or execution of this Certification Policy shall be referred to the qualified courts of the Paris Court of Appeal.

9.15 Compliance with legislation and regulations

This CP complies with the requirements indicated in French legislation and regulations.

9.16 Miscellaneous provisions

9.16.1 Global agreement

No specific requirement.

9.16.2 Transfer of activities

See chapter 5.7.

9.16.3 Consequences of an invalid clause

No specific requirement.

9.16.4 Application and waiver

No specific requirement.

9.16.5 Force Majeure

In addition to the cases generally upheld as such by French courts, the following are considered to be cases of force majeure which may suspend the CDC's obligations under the terms this Certification Policy: social conflicts, interventions by civil or military authorities, natural disasters, fires, water damage and incorrect functioning or interruption of the external telecommunications network.

9.17 Other provisions

No specific requirement.