IDEMIA Identity & Security France
2, Place Samuel de Champlain
92400 Courbevoie
France

Politique de certification Dictao

Autorités Trust CA et Business CA

Réf. : dictao_IGC_PC_hors ligne
Version 1.6 du 09/04/2019

Référence :	dictao_IGC_PC_hors ligne
Version :	1.6
Date de dernière mise à jour :	09/04/2019
Date de publication :	26/04/2019
Niveau de confidentialité :	PUBLIC

Table des mises à jour du document

N° de version	Etat[1]	Date	Auteur	Objet de la mise à jour
1.0	V	19/02/2013	Dictao	Publication initiale
1.1	V	02/04/2013	Dictao	Version mise à jour
1.2	V	16/04/2013	Dictao	Séparation des OID des 2 AC hors ligne
1.3	V	27/02/2015	Morpho	Transfert de patrimoine Dictao vers morpho
1.4	V	24/04/2017	Safran I&S	Mise à jour vers ETSI EN 319 411-1
1.5	V	08/08/2017	Safran I&S	Mise à jour du §10.2
1.6	V	09/04/2019	Idemia I&S France	Mise à jour vers IDEMIA

[1] **T** : En cours de modification ; **V** : Validé

SOMMAIRE

1. PREAMBULE

Nous vous informons que la dissolution et de la transmission universelle de patrimoine de la société Dictao à la société Idemia Identity & Security France, société par actions simplifiées, dont le siège social est domicilié au 2 Place Samuel de Champlain, 92400 Courbevoie, immatriculé au RCS de Nanterre, sous le numéro 440 305 282, est effective depuis le 2 Janvier 2015.

Suite à cette dissolution avec transmission universelle de patrimoine, l'ensemble des contrats conclus par Dictao avec ses clients et prestataires ont été transmis à Idemia Identity & Security France (société appartenant au groupe IDEMIA et dénommé comme tel par la suite), qui lui a succédé tant aux titres de ses droits que ses obligations, dans le strict respect des conditions contractuelles.

Par ailleurs, IDEMIA s'engage à étendre la certification ETSI EN 319 411-1 «Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements ».

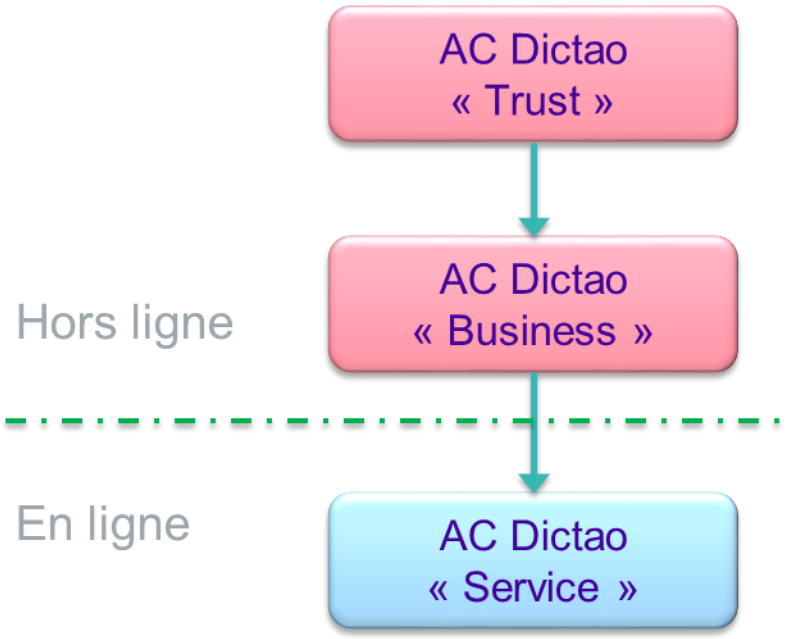
2. INTRODUCTION

2.1 Présentation générale

Ce document constitue la Politique de Certification (PC) de l'autorité racine dénommée « DICTAO Trust Certification Authority » (« **Trust CA** » dans la suite du document) et de l'autorité de certification dénommée « DICTAO Business Certification Authority » («**Business CA** » dans la suite de ce document) dans le cadre de l'émission de certificats électroniques destinés aux autorités de certification de plus bas niveau de l'infrastructure de gestion des clés.

Ce document expose le niveau d'exigence que s'engage à respecter et maintenir des autorités Trust CA et Business CA, lors de l'émission, de la gestion du cycle de vie et de la publication de ces certificats.

Cette politique de certification vise à permettre la délivrance de certificats de signature électronique au sens de l'article 36 du Règlement (UE) No 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit « Règlement eIDAS »).



2.2 Identification du document

Le présent document est dénommé « Politique de Certification – Autorité Racine et Intermédiaire de l'IGC de IDEMIA ».

Les numéros d'OID correspondant à la présente politique de certification sont :

- AC racine « Trust CA » : 1.2.250.1.195.1.1.1.2 (ETSI EN 319 411-1 NCP)
- AC intermédiaire « Business CA » : 1.2.250.1.195.6.1.1.2 (ETSI EN 319 411-1 NCP)

La branche OID de IDEMIA est déposée : {iso(1) member-body(2) fr(250) type-org(1) dictao(195)} Autorités 'Trust CA' et 'Business CA' **(1** ou **6**) Politique de Certification(**1**) Profil 'AC'(**1**) Version(**2**)

2.3 Entrée en vigueur du document

La présente politique de certification s'applique aux certificats émis à partir du 19 février 2013.

2.4 Entités intervenant dans la PKI

2.4.1 Porteurs de certificats

➢ **S'agissant de l'autorité de certification « Trust CA »**

Dans le cadre de la présente politique, un porteur de certificat est l'autorité de certification « Business CA ».

➢ **S'agissant de l'autorité de certification « Business CA »**

Dans le cadre de la présente politique, un porteur de certificat est l'autorité de certification de plus bas niveau de l'IGC, également appelée « **autorités en ligne** ».

2.4.2 Utilisateurs de certificats

La présente politique traitant de certificats d'autorités de certification, un utilisateur de certificats peut être :

- Un service applicatif qui reconnaît les certificats des autorités « Trust CA » et « Business CA » et vérifie, en s'appuyant sur un dispositif de vérification, le certificat fourni et la chaîne de certification d'un certificat de porteur émis par l'autorité racine.
- Tout collaborateur d'un client de IDEMIA qui souhaite vérifier la chaîne de certification de l'autorité (des autorités) émettrice de son certificat

2.4.3 Autorités de certifications

La notion d'Autorité de Certification (AC) telle qu'utilisée dans la présente politique est définie au 2.4.1 ci-dessus.

Les autorités « Trust CA » et « Business CA » sont en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation …) et s'appuie pour cela sur une infrastructure à clés publiques (IGC).

Les prestations des autorités « Trust CA » et « Business CA » sont le résultat de fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats (cf. ci-dessous).

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI (European Telecommunications Standards Institute) dans le domaine, la décomposition fonctionnelle de cette PKI est la suivante :

- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée associée) les certificats :
  - Soit en s'appuyant sur les outils propres aux composants techniques ou aux futurs porteurs de certificat
  - Soit en s'appuyant sur les outils de sa PKI
- **Fonction de remise au porteur** - Cette fonction remet au porteur au minimum son certificat ou la chaîne de certification par l'autorité racine.

- **Fonction de publication -** Cette fonction met à disposition des différentes parties concernées : les politiques publiées, les certificats d'autorité et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **Fonction de gestion des révocations -** Cette fonction traite les demandes de révocation et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats -** Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (statut révoqué en particulier). Cette fonction est mise en œuvre selon un mode de publication d'informations qui se matérialise par une Liste de Certificats Révoqués (CRL).

L'ensemble des fonctions assurées par l'autorité racine (en tant que service technique) est opérée par le service informatique de IDEMIA.

La Déclaration des Pratiques de Certification (DPC) associées aux autorités identifiées dans le présent document décrit l'organisation opérationnelle de la PKI et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans la présente politique. (cf. chapitre 6.2.2).

2.4.3.1 Autorités « Trust CA » et « Business CA » de IDEMIA

Les autorités « Trust CA » et « Business CA » sont une composante de la PKI qui dispose d'une plate-forme lui permettant d'émettre et de gérer les certificats d'autorité de plus bas niveau.

2.4.3.2 Autorités de certification en ligne

Il s'agit des autorités de certification de plus bas niveau des métiers, rattachées à l'IGC de IDEMIA.

2.4.4 Opérateur de certification

L'Opérateur de Certification assure des prestations techniques, en particulier, cryptographiques et d'hébergement permettant d'atteindre les exigences de la présente politique.

Le rôle d'opérateur de certification est assuré par IDEMIA qui s'appuie sur son partenaire Getronics, en position d'hébergeur. Toutes les fonctions qui ne sont pas directement assurées par IDEMIA, sont prises en charge par Getronics dont les responsabilités vis-à-vis de IDEMIA sont décrites contractuellement. Toutes les fonctions sous la responsabilité de Getronics sont documentées par cette entreprise. Certaines informations sont confidentielles et leur diffusion nécessite une validation préalable des parties prenantes.

2.5 Usage des certificats

2.5.1 Domaines d'utilisation applicables

2.5.1.1 Bi-clés et certificats des porteurs

La présente politique traite des bi-clés et des certificats à destination des catégories de porteurs identifiés au chapitre 2.4.1, afin que ces porteurs puissent :

- Signer les certificats avec leur certificat d'Autorité de Certification pour le compte de leurs propres porteurs
- Signer les listes de révocation

2.5.1.2 Bi-clés et certificats de l'autorité Trust CA et Business CA

Les autorités « Trust CA » et « Business CA » génèrent et signent différents types d'objets : certificats et listes de révocation.

Pour signer ces objets, elles disposent d'une bi-clé unique. Cette bi-clé et le certificat associé ne sont utilisés ni à des fins de chiffrement, ni à des fins d'authentification.

2.6 Gestion de la politique de certification

2.6.1 Entité gérant la politique de certification

L'entité en charge de l'administration et de la gestion de la présente politique de certification est l'entité Digital Lab au sein de IDEMIA, appelée 'direction' par la suite dans le document. Elle est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.

2.6.2 Point de contact

La direction de IDEMIA peut être contactée pour toutes questions concernant la présente Politique de Certification. Toute demande doit être adressée à :

Idemia Identity & Security France,

2 Place Samuel de Champlain 92400 Courbevoie,

Coordonnées: info@idemia.com. - Tél. : +33 1 73 60 20 20

2.6.3 Entité déterminant la conformité d'une DPC avec cette politique de certification

La direction de IDEMIA nomme les personnes (ou services) déterminant la conformité de la DPC avec cette politique de certification.

2.6.4 Procédures d'approbation de la conformité de la DPC

L'approbation de la conformité de la DPC passe par :

- Une présentation des analyses par les personnes (ou services) désignées pour déterminer la conformité de la DPC et / ou
- Une validation des analyses par un tiers accrédité

2.7 Définitions et acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- **AC / CA** : Autorité de Certification
- **AE / RA** : Autorité d'Enregistrement
- **AED** : Autorité d'Enregistrement Déléguée
- **ANSSI** : Agence nationale de la sécurité des systèmes d'information
- **CGU** : Conditions Générales d'Utilisation
- **CRL / LCR** : Certificate Revocation List
- **DN** : Distinguished Name
- **DPC / CPS** : Déclaration des Pratiques de Certification
- **IGC / PKI** : Infrastructure de Gestion de Clés
- **OCSP** : Online Certificate Status Protocol
- **OID** : Object Identifier
- **PC / CP** : Politique de Certification
- **PDS** : PKI Disclosure Statement
- **PSCE :** Prestataire de Services de Certification Électronique
- **RSA** : Rivest Shamir Adelman
- **SSI** : Sécurité des Systèmes d'Information
- **URL** : Uniform Resource Locator

Public Key Infrastructure (PKI ou IGC)	**Ensemble de composants physiques, procédures et logiciels permettant de gérer le cycle de vie des certificats et d'offrir des services d'authentification, de chiffrement et de signature.**
Certificat	Fichier électronique délivré par une Autorité de Certification attestant l'identité d'un porteur (personne physique, machine…). Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Autorité de Certification (AC ou CA)	Service chargé de signer, émettre et maintenir les certificats d'une infrastructure à clés publiques, conformément à une politique de certification. Services applicatifs exploitant les certificats émis par l'Autorité de Certification du porteur du certificat.
Politique de certification (PC)	Ensemble de règles et d'exigences auxquelles est soumise une autorité de certification dans la mise en place et la fourniture de ses prestations.
Déclaration des pratiques de certification (PC)	Description des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité de certification applique dans le cadre de la fourniture de ses services de certification électronique, en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.
Liste de révocation des Certificats (CRL ou LCR)	Liste publiée par l'autorité de certification présentant les certificats n'étant plus dignes de confiance (révoqués, invalides…). Par simplicité on y associe également les listes de révocation d'autorités (appelées ARL)
Bi-clé	Couple de clés composé d'une clé privée et d'une clé publique.
X 509	Norme de l'Union internationale des

	télécommunications (UIT) relative aux infrastructures à clés publiques (PKI), entre autres les formats standards de ses composants : certificats électroniques, listes de révocation, algorithme de validation…
UTF-8	Codage des caractères définis par Unicode où chaque caractère est codé sur une suite de un à six mots de 8 bits (il n'existe pas actuellement de caractères codés avec plus de 4 mots).
Distinguished Name (DN)	Elément permettant d'identifier un porteur ou une autorité de certification de façon unique.
Object Identifier (OID)	identifiant universel, représenté sous la forme d'une suite d'entiers associé dans le cadre d'une PKI à un élément de référence tel que la politique de certification ou la déclaration de pratiques de certification.

3. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

3.1 Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des porteurs et des utilisateurs de certificats, les autorités « Trust CA » et « Business CA » mettent en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (cf. chapitre 2.4.3).

La présente politique précise les méthodes de mise à disposition et les URL correspondantes (serveurs Web de publication).

3.2 Informations devant être publiées

Les autorités « Trust CA » et « Business CA » publient les informations suivantes à destination des porteurs et des utilisateurs de certificat :

- La présente politique de certification
- Les listes des certificats révoqués
- Les certificats des autorités en cours de validité

Le responsable de la sécurité des systèmes d'information tient à disposition des entités les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.).

3.3 Délais et fréquences de publication

Les délais et les fréquences de publication dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information doit être publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'autorité racine.
- Pour les informations d'état des certificats, cf. chapitre 5.10.2

Les exigences de disponibilité des systèmes publiant ces informations dépendent des informations concernées : les informations liées à l'IGC et les certificats des autorité Trust CA et Business CA d'a, les systèmes doivent avoir une disponibilité pendant **7 jours sur 7 ouvrés** avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de **8h** et une durée totale maximale d'indisponibilité par mois de **32h** ceci hors cas de force majeure.

A noter que la perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information ; les exigences ci-dessus s'appliquent donc de la même façon.

3.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture. L'accès en modification aux systèmes de publication (ajout, suppression,

modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

4. IDENTIFICATION ET AUTHENTIFICATION

4.1 Nommage

4.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X509 v3 l'autorité émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un « *Distinguished Name* » DN de type X.501 dont le format exact est précisé dans le chapitre 8 décrivant le profil des certificats.

4.1.2 Nécessité d'utilisation de noms explicites

Le DN comprend dans sa structure le nom d'usage du certificat au sein de l'IGC et notamment la raison sociale de la société dans l'attribut « *organizationName* » 'O'. Le contrôle des informations est assuré lors de la cérémonie de clés par les opérateurs techniques de l'IGC.

4.1.3 Pseudonymisation des AC

Les certificats d'AC ne sont pas anonymisés.

4.1.4 Règles d'interprétation des différentes formes de nom

Aucune exigence n'est stipulée en plus des règles spécifiées au §4.1.1.

4.1.5 Unicité de Noms

Afin d'assurer la continuité d'une identification unique du porteur au sein de l'IGC dans ses certificats successifs (renouvellement) et pour éviter toute ambigüité, le DN du champ « *subject* » de chaque certificat de porteur doit permettre d'identifier de façon unique son usage.

L'unicité d'un certificat est basée sur l'unicité de son numéro de série définie par l'AC. Cependant, il convient d'éviter les ambiguïtés sur la propriété d'un certificat en respectant l'unicité d'un même nom au sein de la même AC. Cette unicité est garantie par l'exigence décrite au paragraphe 3.1.2.

4.1.6 Identification, authentification et rôle de marques déposées

IDEMIA est une marque est déposée dans 17 pays dont notamment en Union européenne, Japon, et aux États-Unis d'Amérique.

4.2 Validation initiale de l'identité

L'identification des autorités de certification en ligne est décrite dans la DPC associée.

4.2.1 Méthode pour prouver la possession de la clé privée

➢ **Pour l'autorité de certification Trust CA**

Lorsqu'elle génère sa bi-clé, elle génère également un certificat auto-signé.

➢ **Pour l'autorité de certification Business CA**

Lorsqu'elle génère sa bi-clé, elle doit fournir à l'autorité racine une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

Cette preuve est fournie techniquement par la transmission à l'autorité racine d'une requête de certificat, ou CSR (Certificate Signing Request), au format PKCS#10.

➢ **Pour les autorités de certification en ligne**

Lorsqu'elles génèrent leur bi-clé, elles doivent fournir à l'autorité « Business CA » une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

Cette preuve est fournie techniquement par la transmission à l'autorité « Business CA » d'une requête de certificat, ou CSR (Certificate Signing Request), au format PKCS#10.

4.2.2 Validation de l'identité d'un organisme

Cf. §4.2.3.

4.2.3 Validation de l'identité d'un individu

La validation est interne à la direction de la division DSA de IDEMIA.

4.2.3.1 Enregistrement d'un porteur sans MC

Sans objet.

4.2.3.2 Enregistrement d'un Mandataire de Certification

Sans objet.

4.2.3.3 Enregistrement d'un porteur via un MC

Sans objet.

4.2.4 Informations non vérifiées de l'AC

Sans objet.

4.2.5 Validation de l'autorité du demandeur

Cette étape est effectuée lors d'une cérémonie de clés constatée optionnellement par un huissier de justice.

4.2.6 Critères d'interopérabilité

Sans objet.

4.3 Identification et validation d'une demande de renouvellement des clés

4.3.1 Identification et validation pour un renouvellement courant

Conformément au document [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du porteur).

Le renouvellement ne s'applique pas dans le cadre de cette PC.

4.3.2 Identification et validation pour un renouvellement après révocation

Si une autorité de certification a sa clé privée compromise, il faut avoir l'accord de la direction pour générer une nouvelle bi-clé.

Si le certificat d'une des AC est révoqué alors il ne peut y avoir de renouvellement de certificat. Il faut que l'AC génère de nouvelles clés.

4.4 Identification et validation d'une demande de révocation

La validation d'une demande de révocation d'une autorité de certification est un phénomène exceptionnel.

Les conditions de cette demande sont précisées au chapitre 4.9.

La méthode de validation d'une demande de révocation issue d'une autorité de certification est identique à la validation initiale du porteur.

5. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

5.1 Demande de certificat

5.1.1 Origine d'une demande de certificat

Un certificat peut être demandé uniquement par **l'opérateur de l'IGC** dans le cadre de l'activité commerciale de la société.

5.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre 4.2) :

- Les données à certifier, y compris le DN ;
- La clé publique ;
- La preuve de possession de la clé privée ;
- Les éléments d'identification de l'autorité de certification concernée

5.2 Traitement d'une demande de certificat

5.2.1 Exécution des processus d'identification et de validation de la demande

L'identité du demandeur est vérifiée conformément aux exigences du chapitre 4.2.

Un huissier, ou toute personne habilitée, atteste de la conformité de la demande de création de tout certificat d'autorité de l'IGC de IDEMIA.

5.2.2 Acceptation ou rejet de la demande

Celle-ci se matérialise par la signature d'un procès-verbal de Cérémonie des clés.

5.2.3 Durée d'établissement du certificat

Le délai de traitement est variable car il dépend essentiellement du travail à réaliser pour vérifier la recevabilité de la demande.

La durée d'établissement du certificat est conditionnée par le déroulement de la cérémonie de clé.

5.3 Délivrance du certificat

5.3.1 Actions de l'AC concernant la délivrance du certificat au porteur

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande, l'autorité Trust CA ou Business CA, en qualité de service technique, déclenche les processus de génération du certificat.

5.3.2 Notification de la délivrance du certificat au porteur

A l'issue de la cérémonie, si aucune anomalie n'a été signalée sur le certificat, celui-ci est officiellement remis à la direction de IDEMIA, sous la forme d'un fichier au format DER, sur un support amovible (CD-ROM).

5.4 Acceptation du certificat

5.4.1 Démarche d'acceptation du certificat

La direction de IDEMIA accepte formellement le certificat délivré lors de la cérémonie de clés en émargeant le registre de cérémonie. Aucune objection postérieure à la cérémonie ne pourra être reçue pour annuler l'acceptation du certificat.

5.4.2 Publication du certificat

Cette information doit être accessible à partir d'internet.

5.4.3 Notification de la délivrance du certificat

Non applicable dans le cadre de la présente PC.

L'utilisation des clés privées des autorités « Trust CA » et « Business CA » et de leurs certificats associés est strictement limitée à la signature de certificats d'autorités de certification et à la signature de listes de certificats d'autorités révoqués.

L'usage autorisé de la bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

5.5 Usages de la bi-clé et du certificat

5.5.1 Utilisation de la clé privée et du certificat par le porteur

La hiérarchie d'AC est représentée au §2.1.

L'utilisation de la clé privée est limitée à :

- La signature d'autorité de certification
- La signature de listes de certificats révoqués

5.5.2 Utilisation de la clé privée et du certificat par l'utilisateur du certificat

Les certificats délivrés par les autorités « Trust CA » et « Business CA » ne peuvent être utilisés par un utilisateur qu'à des fins de validation d'une chaîne de confiance comprenant le certificat de celle-ci.

5.6 Renouvellement d'un certificat

Non applicable dans le cadre de la présente PC.

5.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

5.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être changées :

- Pour suivre l'évolution de l'état de l'art en cryptographie, et en particulier les recommandations émises par l'ANSSI afin de minimiser les possibilités d'attaques cryptographiques ;
- En cas de compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'autorité racine.

Dans tous ces cas la délivrance d'un nouveau certificat d'autorité est possible pour toute l'IGC de IDEMIA.

5.7.2 Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat suit les mêmes conditions que celles portées au paragraphe 5.1.

5.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Le traitement d'une demande de certificat suite au changement d'une bi-clé est identique à celui décrit au paragraphe 5.2.

5.7.4 Notification au porteur de l'établissement du nouveau certificat

Cf. chapitre 5.3.2.

5.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 5.4.1.

5.7.6 Publication du nouveau certificat

Cf. chapitre 5.4.2.

5.7.7 Notification par les autorités hors ligne aux métiers de la délivrance d'un nouveau certificat

Cf. chapitre 5.4.3.

5.8 Modification du certificat

La modification d'un certificat correspond à la délivrance d'un nouveau certificat pour la même clé publique, consécutif à des modifications d'informations autres que les dates de validité et le numéro de série (dans le cas contraire il s'agit d'un renouvellement de certificat).

La modification de certificat n'est pas autorisée dans la présente politique.

5.9 Révocation et suspension des certificats

5.9.1 Causes possibles d'une révocation

Pour une autorité de certification en ligne et hors ligne, les causes de révocation sont les suivantes :

- Cessation d'activité commerciale associée à l'autorité de certification
- Compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'autorité métier
- Non-conformité révélée lors d'un contrôle de conformité.

5.9.2 Origine d'une demande de révocation

Seule la direction de IDEMIA est habilitée à effectuer une demande de révocation.

5.9.3 Procédure de traitement d'une demande de révocation

La révocation d'un certificat nécessite une cérémonie de clés.

5.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dans le cas d'une compromission ou d'une suspicion de compromission de clé privée d'une autorité hors ligne ou en ligne la direction de IDEMIA demande immédiatement à révoquer le certificat de celle-ci. La révocation est traitée dans les 24 heures.

5.9.5 Délai de traitement par les autorités hors ligne d'une demande de révocation

Les demandes de révocation devront être traitées à réception par l'autorité correspondante.

5.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

Sans objet.

5.9.7 Fréquence d'établissement des CRL des autorités hors ligne

La fréquence de publication des CRL des autorités hors ligne est de 1 an.

5.9.8 Délai maximum de publication d'une CRL d'autorité hors ligne

Une CRL doit être publiée dans un délai maximum de 24 heures ouvrées suivant sa génération.

5.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Les autorités « Trust CA » et « Business CA » ne mettent en œuvre aucun système de vérification en ligne de la révocation et de l'état des certificats, indépendamment de la publication sur Internet d'ARL et de certificats.

5.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Sans objet.

5.9.11 Autres moyens disponibles d'information sur les révocations

Si d'autres moyens sont mises en œuvre, la DPC les précisera.

5.9.12 Exigences spécifiques en cas de compromission de la clé privée

La révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de IDEMIA.

5.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

5.10 Fonction d'information sur l'état des certificats

5.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de CRL.

Les CRL de l'autorité racine sont au format V2, accessibles en http aux adresses suivantes :

- **S'agissant de l'autorité Trust CA ; http://trust.dictao.com/crl/dictao-trust-ca.crl**

- **S'agissant de l'autorité business CA : http://trust.dictao.com/crl/dictao-business-ca.crl**

Ces informations sont accessibles depuis internet.

5.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est rendue disponible par les autorités Trust CA et Business CA avec une durée maximale d'indisponibilité par mois de 32 heures (jours ouvrés) par mois.

5.11 Fin de la relation avec le porteur

Cf. chapitre 5.9.1, les causes possibles d'une révocation.

5.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des porteurs est interdit.

6. MESURES DE SECURITE NON TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que les autorités de certification hors ligne doivent respecter. La DPC décrit les moyens mis en œuvre pour respecter ces exigences.

6.1 Mesures de sécurité physique

6.1.1 Situation géographique et construction des sites

Les certificats et les bi-clés des autorités de certification sont conservés dans des coffres sous la responsabilité de la direction de IDEMIA.

Les sites contenant les informations devant être publiées sont ceux de l'hébergeur de IDEMIA.

6.1.2 Accès physique

Sans objet puisque les AC sont hors-ligne

6.1.3 Alimentation électrique et climatisation

. Sans objet puisque les AC sont hors-ligne

6.1.4 Vulnérabilité aux dégâts des eaux

. Sans objet puisque les AC sont hors-ligne

6.1.5 Prévention et protection incendie

.Sans objet puisque les AC sont hors-ligne

6.1.6 Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) correspondant aux informations relatives à l'activité de l'IGC (fonctions d'exploitation, de sauvegarde, etc.) sont traités et conservés dans une enceinte sécurisée accessibles aux seules personnes autorisées.

Parmi les supports, on distinguera :

- Les cartes contenant une partie du secret d'accès aux clés des autorités « Trust CA » et « Business CA » qui doivent être conservées dans un coffre personnel à chaque détenteur de carte.
- Les archives stockées dans le coffre de la PKI.

Les archives sont conservées durant toute la vie des autorités « Trust CA » et « Business CA ».

6.1.7 Mise hors service des supports

Les supports papier et magnétiques en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité.

Les supports de stockage (disque dur de serveurs) de la PKI ne sont pas réutilisés à d'autres fins avant destruction complète des informations liées à la PKI qu'ils sont susceptibles de contenir.

6.1.8 Sauvegardes hors site

Les sauvegardes hors site sur CD ROM sont stockées dans des coffres-forts. La DPC précise les modalités de stockage.

6.2 Mesures de sécurité procédurales

6.2.1 Rôles de confiance

On distingue les rôles suivants :

- **Le Responsable de la sécurité des systèmes d'information rattaché à la direction de IDEMIA**: il est en charge de l'application de la politique de certification de l'autorité racine.
  - Il ne peut être un opérateur porteur de secret
  - Il peut être un administrateur porteur de secret.
- **Opérateurs techniques de l'IGC** : ils sont chargés de l'utilisation, de la configuration et de la maintenance technique des équipements, boîtier cryptographique et serveur. En particulier, ils développent techniquement le déroulement de la cérémonie de clé.
- **Contrôleurs / auditeurs** : Personne désignée par une autorité compétente (conforme par exemple à « Instruction relative à la procédure d'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance »)et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante. Le contrôleur est nommé par l'organisation du client de IDEMIA et validée par le management de IDEMIA. ils sont désignés par la Direction pour vérifier la conformité de la PC et de la DPC associée.
- **Porteurs de secrets** :
  - L'administrateur porteur de secret permet de créer le contexte de sécurité d'accès au boîtier et de le restaurer ;
  - L'opérateur porteur de secret participe à créer et activer la bi-clé de l'autorité « Trust CA » et « Business CA » dans le contexte de sécurité détenu par les administrateurs porteurs de secret.

6.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles seront réparties sur plusieurs personnes. La présente politique définit les exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de la PKI.

La DPC de l'autorité racine précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

Il est admis qu'une même personne puisse assurer plusieurs rôles. La répartition est définie dans le cadre de la DPC.

6.2.3 Identification et authentification pour chaque rôle

La direction de IDEMIA fait vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants.

6.2.4 Rôles exigeant une séparation des attributions

Les porteurs de secret ne détiennent jamais deux parties différentes d'un même secret.

6.3 Mesures de sécurité vis-à-vis du personnel

6.3.1 Qualifications, compétences et habilitations requises

Tout le personnel amené à travailler au sein des composantes de l'IGC est soumis à une clause de sécurité vis-à-vis de IDEMIA.

Chaque Service opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

L'AC informe toute personne intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC,
- Des procédures liées à la sécurité du système et au contrôle du personnel.

Chaque personne dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille.

La documentation adéquate concerne :

- La politique de certification ;
- La déclaration des pratiques de certification ;
- Les procédures internes ;
- Les documents techniques relatifs aux matériels et logiciels utilisés.

6.3.2 Procédures de vérification des antécédents

Les personnels de l'IGC sont identifiés et ne doivent pas avoir de condamnation en contradiction avec leurs attributions.

6.3.3 Exigences en matière de formation initiale

Le personnel exécutant doit être formé aux logiciels, matériels et procédures internes de fonctionnement de la composante pour laquelle il opère.

6.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

6.3.5 Fréquence et séquence de rotation entre différentes attributions

En termes de gestion de carrière pour un exploitant donné, les règles à appliquer sont celles pratiquées par l'organisme employeur.

6.3.6 Sanctions en cas d'actions non autorisées

La direction de IDEMIA, en conformité avec les directives de la société, décide des sanctions à appliquer lorsqu'un agent abuse de ses droits ou effectue une opération non conforme à ses attributions.

6.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les personnels contractants doivent respecter les mêmes conditions que celles énoncées dans les § 6.3.1 à 6.3.4.

6.3.8 Documentation fournie au personnel

Les documents dont doit disposer le personnel sont les suivants :

- Déclaration des Pratiques de Certification propre au domaine de certification ;
- Documents constructeurs des matériels et logiciels utilisés ;
- Politiques de Certification supportées par la composante à laquelle il appartient ;
- Procédures internes de fonctionnement.

L'ACR et l'AE doivent veiller à ce que leur personnel respectif (comme défini dans la DPC) possède bien les documents identifiés ci-dessus en fonction de leur besoin comme le précise la DPC.

6.4 Procédures de constitution des données d'audit

La journalisation consiste à enregistrer des événements sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

6.4.1 Type d'évènements à enregistrer

L'IGC permet de journaliser les évènements suivants pour les autorités de certification hors ligne :

- Journaux applicatifs de la PKI

- Réception d'une demande de certificat (initiale et renouvellement)
- Validation / rejet d'une demande de certificat
- Evènements liés aux clés de signature et aux certificats d'autorités (génération, sauvegarde / récupération, révocation, renouvellement, destruction, etc.)
- Génération des certificats des porteurs
- Réception d'une demande de révocation
- Validation / rejet d'une demande de révocation
- Génération puis publication des CRL

- Autre journaux :
  - Les accès physiques
  - Les actions de maintenance et de changements de la configuration des systèmes
  - Les changements apportés au personnel
  - Publication et mise à jour des informations liées à l'autorité (PC, certificats d'autorité, conditions générales d'utilisation, etc.)

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants lorsqu'applicable :

- Destinataire de l'opération
- Nom du demandeur de l'opération ou référence du système effectuant la demande
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes)
- Cause de l'évènement
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat)

6.4.2 Fréquence de traitement des journaux d'évènements

L'analyse du contenu des journaux d'événements doit être effectuée de manière régulière par les autorités « Trust CA » et « Business CA » lors de chaque signature de certificat ou de CRL.

6.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés jusqu'à la fin de vie des autorités « Trust CA » et « Business CA ».

6.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

6.4.5 Procédure de sauvegarde des journaux d'évènements

L'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente politique.

Une copie de sauvegarde des journaux d'événements est réalisée après chaque cérémonie sur les plates-formes de l'IGC.

6.4.6 Système de collecte des journaux d'évènements

L'IGC s'appuie sur les systèmes de collecte internes à chacune de ses composantes.

6.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

6.4.8 Evaluation des vulnérabilités

Le processus d'évaluation des vulnérabilités est décrit dans l'analyse de risque de l'IGC.

Des tests d'intrusion complémentaires sont réalisés périodiquement.

6.5 Archivage des données

6.5.1 Types de données à archiver

Les procédures et les outils permettent d'archiver les données suivantes :

- Certificats des autorités hors ligne
- Certificat des autorités en lignes, valides comme révoqués
- Journaux d'événements, cf. §6.4
- Logiciels et fichiers de configuration des différentes composantes
- Ensembles des éléments utiles à l'enregistrement ou à la révocation :
  - Récépissés
  - Demandes de révocation et leurs résultats
- Registres de cérémonie de clés
- Scripts des cérémonies
- Listes de révocations

6.5.2 Période de conservation des archives

Les archives sont conservées jusqu'à la fin de vie de l'IGC.

Cette durée est :

- Les dossiers d'enregistrement sont conservés 7 ans après expiration du certificat associé.
- Les certificats et les informations sur le statut des certificats (CRL) sont conservés au moins 8 ans après leur date d'expiration.
- Les traces techniques assurant l'imputabilité des actions sont conservées 7 ans après leur génération.

6.5.3 Durée de restitution des archives

Les archives (papier ou électroniques) peuvent être récupérées dans un délai inférieur à 3 jours ouvrés.

6.5.4 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- Protégées en intégrité
- Accessibles aux personnes autorisées
- Accessibles pour relecture et exploitation

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

6.5.5 Exigences d'horodatage des données

Sans objet.

6.5.6 Système de collecte des archives

Le système de collecte des archives est celui du système d'informations de Getronics.

6.5.7 Procédures de récupération et de vérification des archives

Les archives sont sous la responsabilité de l'IGC. Le processus de récupération doit faire l'objet d'une procédure interne de fonctionnement mentionnée dans la DPC des AC hors lignes. La récupération doit être effectuée sous un délai maximal égal à 2 jours ouvrés.

6.6 Changement de clé de l'autorité

L'AC change sa bi-clé lorsqu'elle n'est plus conforme au référentiel cryptographique de niveau standard émis par l'ANSSI. La durée de vie maximale d'un certificat d'AC doit être en cohérence avec le référentiel cryptographique de l'ANSSI.

Les autorités « Trust CA » et « Business CA » ne peuvent pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant à la sienne. Pour cela, la période de validité de son certificat est supérieure à celle des certificats qu'elle signe.

Aussi lorsqu'elle accède à une demande de certification, l'autorité « Trust CA » et « Business CA » fixe la durée de vie du certificat demandé de telle sorte qu'il ne soit jamais valable au-delà de la date de fin de validité du certificat de sa bi-clé utilisée pour la signature.

Dans le cadre de la présente IGC tous les certificats sont générés en même temps et ont une durée de vie équivalente.

6.7 Reprise suite à compromission et sinistre

6.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Les équipes d'exploitation de IDEMIA mettent en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels

L'analyse des différents journaux d'évènements est contrôlée par des auditeurs habilités.

6.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

La sauvegarde des composants l'IGC permet d'assurer une reprise d'activité en cas de sinistre sous 48 heures. Ceci ne s'applique que lorsque des CRL doivent être générées en urgence.

6.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Dans le cas de compromission d'une clé d'autorité, le certificat correspondant est immédiatement révoqué (en fonction des délais de réalisation de la cérémonie de clés).

6.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de la l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente politique.

S'agissant des autorités Trust CA et Business CA, hors ligne, la continuité d'activité consiste à restaurer l'IGC à partir des sauvegarde et secrets.

6.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

6.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Cessation d'activité d'une composante autre que l'ACR.

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'ACR doit entre autres obligations :

- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC Type. A défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat du porteur est encore valide.
- communiquer avant une date donnée son intention de transfert d'activité ;
- mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires (utilisateurs finaux, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité ;
- remettre ses archives à l'AA ;
- l'ACR doit préciser dans sa DPC qui elle doit prévenir, comment se déroule le transfert des obligations (archives et logs à une autre entité), et comment seront traités les certificats encore valides qui seraient amenés à être révoqués.

6.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux trois premiers items ci-dessous soient à exécuter par l'ACR, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'ACR ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LAR conformément aux engagements pris dans sa PC.

Lors de l'arrêt du service, l'ACR doit :

- s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- révoquer son certificat ;
- révoquer les certificats valides qu'elle a signé (uniquement pour une fin de vie due à une compromission ou suspicion de compromission de clé, une perte ou un vol) ;
- révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre 4.2.3)
- l'ACR doit s'assurer qu'aucun contractant ne peut agir pour son compte dans le processus de génération de certificat ;
- les clés privées de l'ACR doivent être détruites ou ne doivent plus être utilisées ;
- communiquer avant une date donnée son intention de cessation d'activité.

En fin de vie l'IGC, les autorités « Trust CA » et « Business CA » :

- Révoque(nt) tous les certificats encore valides qu'elle(s) a(ont) signés, y compris les siens ;
- Prend(prennent) toutes les mesures nécessaires pour la détruire ou la rendre inopérante.

7. MESURES DE SECURITE TECHNIQUES

7.1 Génération et installation de bi clés

7.1.1 Génération des bi-clés

La confidentialité des clés est notamment assurée par des mesures techniques détaillées dans la DPC.

Les clés de signature de l'autorité « Trust CA » et « Business CA » sont générées et mises en œuvre dans un boîtier cryptographique dont les caractéristiques sont décrites dans la DPC.

La génération des clés de signature des autorités « Trust CA » et « Business CA » est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre 6.2.1), dans le cadre de « cérémonies de clés ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation de la PKI et/ou la génération des clés de signature de l'autorité Trust CA et Business CA s'accompagne de la génération de parties de secrets (principe de protection n sur m). Ces parties de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature des autorités Trust CA et Business CA, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures de l'autorité racine.

Le boîtier cryptographique, utilisé par toutes les autorités de l'IGC de IDEMIA pour générer et mettre en œuvre les clés de signature (pour la génération des certificats électroniques, des listes de révocation) a pour objectif :

- D'assurer la confidentialité et l'intégrité des clés privées de signature durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- D'être capable d'identifier et d'authentifier ses utilisateurs, porteurs de secrets d'activation du boîtier ;
- De permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'autorité, qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- De créer des enregistrements d'audit pour chaque action réalisée à partir d'une clé d'autorité.

7.1.2 Transmission de la clé privée à son propriétaire

Les clés privées des autorités « Trust CA » et « Business CA » lui sont transmises sous la forme de secrets partagés entre plusieurs porteurs.

7.1.3 Transmission de la clé publique à l'AC

➢ **S'agissant de l'autorité racine « Trust CA »**

Les modes de transmission de la clé publique de l'autorité (**certificat auto-signé**, PKCS#10, …), sont définis dans la procédure de demande de certificat indiquée au paragraphe 5.2.

➢ **S'agissant de l'autorité « Business CA »**

Les modes de transmission de la clé publique de l'autorité (**certificat signé par l'AC Trust CA**, PKCS#10, …), sont définis dans la procédure de demande de certificat indiquée au paragraphe 5.2.

➢ **S'agissant des autorités en ligne**

Les modes de transmission de la clé publique de l'autorité (**certificat signé par l'AC Business CA**, PKCS#10, …), sont définis dans la procédure de demande de certificat indiquée au paragraphe 5.2.

7.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

L'IGC met à disposition tous les certificats d'autorité via son service de publication.

Elle peut remettre également son certificat sur un support amovible directement aux participants d'une cérémonie de clés.

7.1.5 Taille des clés

Les autorités utilisent des clés de 4096 bits.

L'AC suit les recommandations cryptographiques de l'ANSSI sur la base de la TS 119 312 de l'ETSI.

7.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. chapitre 8).

7.1.7 Objectifs d'usage de la clé

L'utilisation d'une clé privée et du certificat associé est strictement limitée à la signature de certificats et de CRL.

7.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

7.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Les clés privées des autorités de certification de l'IGC (hors ligne ou en ligne) sont protégées par un boitier cryptographique dont le niveau de résistance est évalué certifié EAL4+.

Le boîtier utiliser par les AC « Trust CA » et « Business CA » est qualifié par l'ANSSI.

7.2.2 Contrôle de la clé privée par plusieurs personnes

Cf.7.1.2.

7.2.3 Séquestre de la clé privée

Sans objet.

7.2.4 Copie de secours de la clé privée

La copie de secours des clés des autorités « Trust CA » et « Business CA » est réalisée en utilisant les spécifications du boîtier cryptographique qui est décrit dans la DPC.

7.2.5 Archivage de la clé privée

Les clés privées de toutes les autorités de l'IGC ne sont en aucun cas archivées.

7.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Cf. 7.2.4.

7.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées d'une autorité de l'IGC (racine ou subordonnée) sont stockées dans un module cryptographique répondant au minimum aux exigences du chapitre 12 ci-dessous.

7.2.8 Méthode d'activation de la clé privée

L'activation de la clé privée de chaque AC de l'IGC dans un module cryptographique doit être contrôlée via des données d'activation et doit faire intervenir au moins m parmi n personnes identifiées dans les rôles de confiance correspondants.

7.2.9 Méthode de désactivation de la clé privée

La désactivation des clés privées des AC de l'IGC dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur technique de la PKI, etc.

La désactivation de la clé privée d'une AC de l'IGC utilisée lors d'une cérémonie de clés ou de génération de bi-clé et de certificat, est réalisée immédiatement après l'utilisation de la clé.

7.2.10 Méthode de destruction des clés privées

La méthode de destruction de la clé privée d'une AC de l'IGC doit permettre de répondre aux exigences définies dans le chapitre 12

En fin de vie d'une AC de l'IGC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

7.2.11 Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques d'une AC de l'IGC sont évalués au niveau correspondant à l'usage visé, tel que précisé au chapitre 10 ci-dessous.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques

Les clés publiques des AC de l'IGC sont archivées dans le cadre de l'archivage des certificats correspondants.

7.3.2 Durées de vie des bi-clés et des certificats

La fin de validité du certificat des AC de l'IGC doit être postérieure à la fin de vie des certificats porteurs qu'elle émet. Elle a été définie pour les autorités « Trust CA » et « Business CA » à 20 ans.

7.4 Données d'activation

7.4.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation d'un module cryptographique de la PKI sont effectuées lors de la phase d'initialisation et de personnalisation de ce module.

Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre 6.2.1).

7.4.2 Protection des données d'activation

Les données d'activation générées pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire.

Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

7.4.2.1 Protection des données d'activation correspondant aux clés privées des porteurs

Les données d'activation sont stockées dans des enveloppes scellées qui sont mises au coffre. La répartition des secrets dans différents coffres permet de se prémunir contre toute usurpation d'identité de l'IGC.

7.4.2.2 Autres aspects liés aux données d'activation

Sans objet.

7.5 Mesures de sécurité des systèmes informatiques

7.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

Les mesures de sécurité de l'IGC sont conformes à la politique de sécurité de IDEMIA et couvrent les points suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs),
- Gestion des droits des utilisateurs,
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- Protection du réseau contre toute intrusion d'une personne non autorisée,
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- Fonctions d'audits (non-répudiation et nature des actions effectuées),
- Eventuellement, gestion des reprises sur erreur.

7.5.2 Niveau de qualification des systèmes informatiques

Le module cryptographique utilisé par l'IGC fait l'objet d'une qualification par l'ANSSI et d'une certification critère commun EAL4+.

7.6 Mesures de sécurité liées au développement des systèmes

Les environnements de développement sont distincts de l'environnement de production.

7.6.1 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

7.6.2 Niveau d'évaluation sécurité du cycle de vie des systèmes

La présente politique ne formule pas d'exigence spécifique sur le sujet.

7.7 Mesures de sécurité réseau

Sans objet. Les autorités « Trust CA » et « Business CA » sont hors ligne. Les mesures de sécurité réseau pour les AC en ligne sont décrites dans le politique de certification associées

7.8 Horodatage / Système de datation

Il n'y a pas d'horodatage au sein de l'IGC, mais un système de datation dont la description est donnée dans la DPC.

8. PROFILS DES CERTIFICATS, OCSP ET DES CRL

8.1 Profil des certificats

8.1.1 Numéro de version

Les certificats émis dans le cadre de l'IGC respectent la norme X.509 v3.

8.1.2 Champs de base

Les certificats respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

Nom du champ	Description	Contenu
Version	Version du certificat X.509	Contient la valeur 2 pour indiquer que le certificat est un certificat x.509v3
SerialNumber	Numéro de série du certificat	Contient une valeur entière pour indiquer le numéro de série du certificat, cette valeur doit être unique pour chaque certificat émis par l'autorité racine.
Signature	Signature de l'autorité pour l'authentifier	Sha2WithRSAEncryption
Issuer	Nom de l'autorité	Contient le DN (X.500) de l'autorité
Validity	Période de validité du certificat	Contient les dates d'activation et d'expiration du certificat. Cette période est de **20 ans**
Subject	Nom du porteur	Contient le DN de l'autorité
Subject Public Key Info	Informations sur la clé publique de l'abonné	Contient l'OID de l'algorithme et la clé publique de l'abonné (**longueur de clés = 4096 bits**)
Extensions	Liste des extensions	Voir chapitre suivant

8.1.3 Extensions du certificat

Les certificats émis par les autorités hors ligne de l'IGC comportent les extensions X.509v3 suivantes. La DPC précise les valeurs utilisées.

Extension	Extension critique	Description
Authority Key Identifier	N	Elément d'identification de la clé publique de l'autorité signant le certificat
KeyUsage	O	Description des utilisations autorisées de la clé privée
Certificate Policies	N	OID de la PC régissant le certificat et Intitulé de la PC
Authority Information Access	N	Informations d'accès au certificat de l'autorité.
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur
Certificate Policy	N	Indique l'adresse ou sont publiées toutes les politiques de certification de IDEMIA
CRL Distribution Points	O	indique les adresses auxquelles est publiée la CRL de l'autorité ayant émis le certificat

8.1.4 OID des algorithmes

Les identificateurs d'algorithmes doivent être inscrits auprès d'un registre (par exemple, un registre international tel que celui de l'ISO).

L'algorithme de condensat utilisé dans le cadre de l'IGC est SHA-2 (OID 2.16.840.1.101.3.4.2.1). L'algorithme de chiffrement utilisé dans le cadre de l'IGC est RSA.

8.1.5 Forme des noms

Les noms attribués aux porteurs dans le cadre de l'IGC respectent la norme X.500, comme détaillé au chapitre 4.1 de ce document.

8.1.6 OID des politiques de certification

Les acteurs présents lors de la cérémonie de clés s'assurent que les certificats émis contiennent l'OID de la politique de certification qui régit le cadre de la présente politique de certification.

8.1.7 Utilisation de l'extension « contraintes de politique »

La présente politique n'émet pas d'exigence particulière sur ce sujet.

8.1.8 Sémantique et syntaxe des qualifiants de politique

La présente politique n'émet pas d'exigence particulière sur ce sujet.

8.1.9 Sémantiques de traitement des extensions critiques de la politique de certification

La présente politique n'émet pas d'exigence particulière sur ce sujet.

8.2 Profil des CRL

8.2.1 Numéro de version

Les CRL émises utilisent la version 2 du format défini dans la norme ISO [9594-8].

8.2.2 Champs de base

Les champs de base des CRL émise par l'autorité racine sont les suivants :

Champ	Description
Version	Version de la CRLX.509
Signature	Identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste Sha2WithRSAEncryption retenu pour la présente PC.
Issuer	Nom de l'autorité de l'IGC
This Update	Date d'émission de la CRL
Next Update	Date limite d'émission de cette CRL
Revoked Certificates	Liste d'enregistrement de révocation. On spécifiera pour chaque révocation les valeurs associées aux champs suivants : - User Certificate (numéro de série du certificat révoqué) - Revocation Date (date de révocation du certificat).
CRL Extensions	Extensions générales de la CRL

La CRL dans sa forme finale est l'ensemble des éléments suivants :

Champ	Description
tbsCertlist	L'ensemble des champs décrits ci-dessus
signatureAlgorithm	L'identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste Sha2WithRSAEncryption retenu pour la présente PC.
signatureValue	Le résultat de cet algorithme sur l'ensemble des champs de tbsCertList

8.2.3 Extensions de CRL et d'entrées de CRL

Les CRL incluent les champs de base présentés au paragraphe précédent, ainsi que les extensions d'entrée suivantes :

Extension d'entrée	Description
Authority Key Identifier	Identifie la clé publique de l'autorité ayant signé la CRL
CRL Number	Donne un nombre croissant séquentiel pour chaque CRL émise
Reason Code	Identifie la cause de révocation du certificat. Sauf spécification particulière, la valeur pour chaque révocation sera « unspecified ».

9. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

9.1 Fréquences et / ou circonstances des évaluations

Un contrôle de conformité de l'ensemble de l'IGC est réalisé tous les deux ans.

9.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné par la direction de IDEMIA à une équipe d'acteurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

9.3 Relations entre évaluateurs et entités évaluées

L'organisation des audits internes est écrite dans la DPC associée.

9.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur l'ensemble de l'IGC et visent à vérifier le respect des engagements et pratiques définies dans la présente politique de certification et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

9.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'évaluateur émet auprès de la direction de IDEMIA un rapport de conformité assorti de recommandations.

La Direction de IDEMIA, par délégation aux acteurs identifiés dans la présente politique a en charge la résolution des points de non-conformité ainsi que le choix de la mesure à appliquer.

9.6 Communication des résultats

Les résultats des audits de conformité sont confidentiels et ne peuvent être communiqué qu'à des tiers en cas de demande explicite.

10. ANNEXE 1 - AUTRES PROBLEMATIQUES METIERS ET LEGALES

10.1 Tarifs

Sans objet.

10.2 Responsabilité financière

Le TSP s'engage à conserver, pendant toute la durée du présent Contrat, les capacités financières et/ou assurantielles nécessaires au respect de l'ensemble de ses engagements au titre du présent Contrat, y incluse la couverture des conséquences financières de tout engagement de sa responsabilité au titre des présentes.

10.3 Confidentialité des données professionnelles

10.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La partie non-publique de la DPC correspondant à la présente PC,
- Les clés privées des composantes et des porteurs de certificats de l'IGC
- Les données d'activation associées aux clés privées des autorités de l'IGC
- Tous les secrets de l'IGC
- Les journaux d'évènements des composantes de l'IGC
- Le dossier d'enregistrement des porteurs
- Les causes de révocations, sauf accord explicite de publication ;
- Le procès-verbal de cérémonie de clés.

10.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

10.3.3 Responsabilités en termes de protection des informations confidentielles

IDEMIA, en tant qu'autorité, est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

10.3.4 Protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'ensemble de ses composantes de l'IGC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

10.3.5 Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français.

10.3.6 Notification et consentement d'utilisation des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français.

10.3.7 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire français.

10.3.8 Droits sur la propriété intellectuelle et industrielle

Application de la législation et de la réglementation en vigueur sur le territoire français.

10.4 Limite de garantie

Sans objet.

10.5 Limite de responsabilité

Sans objet.

10.5.1 Indemnités

Sans objet.

11. ANNEXE 1 – DOCUMENTS CITES EN REFERENCE

11.1 Réglementation

Non applicable.

11.2 Documents techniques

Référence	Objet du document	Lien vers le document
RGS_A4	Référentiel Général de Sécurité - Profils de certificats et des CRL	https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_A4.pdf

12. ANNEXE 2 - EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DES AC

12.1 Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'IGC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR), ainsi que générer les bi-clés des porteurs, doit répondre aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- Etre capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

12.2 Exigence sur la qualification

Le module cryptographique utilisé par l'IGC est qualifié au minimum au niveau élémentaire, selon le processus décrit dans le la Référentiel Général de Sécurité de l'administration française et être conforme aux exigences du chapitre ci-dessus.