Politique et pratiques de certification – AC LCP

V1.2 – Janvier 2022

IDEMIA

Sommaire

Introduction

Le présent document décrit les procédures opérationnelles d'enregistrement l'AC IDEMIA en vue d'émettre des certificats de signature de personne physique de niveau LCP.

Elle couvre en particulier toutes les opérations relatives à l'identification.

L'historique de ce document est le suivant :

Numéro de version	Auteur	Commentaire
V1.0	PRO	Version initiale du document.
V1.1	PRO	• Ajout en §7.2 > de la suppression des certificats de la CRL à leur expiration • Ajout en §1.4 > des opérateurs d'enregistrement et de révocation.
V1.2	JMD	• Transfert des opérations chez Docaposte Trust & Sign

1.1 > Présentation générale

Ce document constitue la Politique de Certification (PC) et la Déclaration des pratiques de certification (*certificate practice statements*, CPS) de l'autorité de certification AC IDEMIA produisant des certificats électroniques de signature destinés aux clients des partenaires d'IDEMIA.

Ce document décrit le niveau d'exigence que s'engage à respecter et maintenir l'autorité de certification lors de l'émission, de la gestion du cycle de vie et de la publication de ces certificats.

Il s'appuie, en tant que cadre de référence documentaire uniquement, sur les préconisations, émises par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'*European Telecommunications Standards Institute* (ETSI).

Cette politique de certification vise à permettre la délivrance de certificats de signature avancée au sens de l'article 38 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 »).

1.2 > Identification du document

Les politiques décrites dans le présent document sont identifiées par les OID suivante :

Famille	OID	Conformité
Personne Physique	*1.3.6.1.4.1.54916.1.4.1.1*	*ETSI EN 319 411-1 LCP* *0.4.0.2042.1.3*
OCSP		*N/A*

Le numéro d'OID d'une politique est porté dans les certificats soumis à celle-ci.

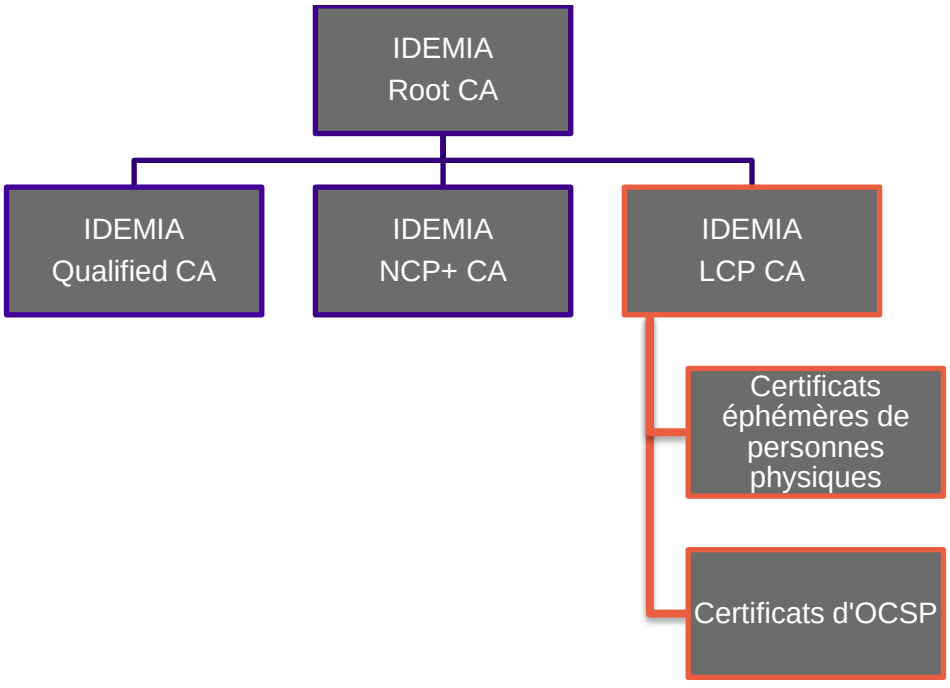
Les certificats OCSP sont des certificats techniques utilisés par la fonction d'information sur l'état des certificats de l'AC (§ 4.10 > Fonction d'information sur l'état des certificats). Ce sont des certificats émis par l'AC pour ses propres usages.

1.3 > Entrée en vigueur du document

La présente P.C. s'applique à partir du 1 janvier 2022.

1.4 > Entités intervenant dans l'IGC

La hiérarchie d'AC est la suivante.



Le périmètre de la présente PC est présenté en rouge.

1.4.1 > Autorité de Certification

L'autorité de certification IDEMIA LCP CA est en charge de 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).

L'autorité de certification est IDEMIA. . A la suite de la cession des activités de signature électronique de IDEMIA à la société Docaposte Trust & Sign, cession qui comprend le personnel en charge de ces activités, la gestion de la continuité des services est assurée par Docaposte Trust & Sign.

L'accord d'autorisation entre IDEMIA et Docaposte Trust & Sign engage Docaposte Trust & Sign à opérer les services selon le cadre déjà audité.

Fonction	Description	Entité responsable
Fonction de génération des certificats	Cette fonction génère (création du format, signature électronique avec la clé privée associée) les certificats en s'appuyant son infrastructure.	▪ IDEMIA
Fonction de remise au porteur	Cette fonction remet au porteur au minimum son certificat ou la chaîne de certification.	▪ *IDEMIA*
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.	▪ *IDEMIA*
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.	▪ *IDEMIA*
Fonction d'information sur l'état des certificats	Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats.	▪ IDEMIA
Fonction d'administration de l'IGC	Cette fonction est associée au rôle qui définit le comportement fonctionnel et le paramétrage technique de l'IGC.	▪ IDEMIA

Tableau 1 – Décomposition fonctionnelle de l'IGC

Chacune des fonctions sous la responsabilité de IDEMIA, mis à part la révocation, est opérée par Docaposte Trust & Sign, et peut être déléguée à des sous-traitants de Docaposte Trust & Sign.

1.4.2 > Autorité d'enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat ainsi que des contraintes liées à l'usage du certificat qui lui est délivré, conformément à la politique de certification.

L'AE est opérée par un client d'IDEMIA.

1.4.3 > Opérateur d'enregistrement (OE)

L’opérateur d’enregistrement, membre de l’AE, est la personne physique, rôle de confiance, ou le processus automatisé en charge de la vérification de l’identité du futur porteur de certificat.

1.4.4 > Opérateur de révocation (OR)

L’opérateur de révocation, est la personne physique, rôle de confiance d’IDEMIA, en charge de la vérification des demandes de révocation et de leur traitement. S’agissant, dans le cadre de cette PC, de certificats éphémères uniquement utilisés dans le cadre d’un processus de signature sous le contrôle d’IDEMIA, les révocations ont uniquement lieu en ligne de façon automatisée en cas de refus de signature. Les révocations manuelles par un opérateur de révocation sont donc inexistantes dans le cadre de cette PC.

1.4.5 > Porteurs de certificats

Un porteur de certificat est une personne physique, cliente d’un partenaire d’IDEMIA et signant des documents électroniques en son nom

1.4.6 > Utilisateurs de certificats

Les Utilisateurs sont les personnes physiques et morales destinataires des documents signés électroniquement.

1.5 > Usage des certificats

1.5.1 > Bi-clés et certificats des porteurs

Les restrictions d'utilisation des bi-clés et des certificats sont définies en § 4.5 > ci-dessous. L'AC respecte ces restrictions et impose leur respect.

À cette fin, elle communique à tous les signataires et utilisateurs potentiels les conditions générales relatives à l’utilisation du certificat.

1.5.2 > Bi-clés et certificats d’AC

Plusieurs clés sont utilisées par l’AC :

- La clé de signature de l’AC, utilisée pour signer les certificats générés par l'AC et, le cas échéant, la LCR de l’AC ;
- Les clés de signature du service OCSP de l’AC, utilisées pour signer les jetons OCSP produits par la fonction d’information sur le statut des certificats.

1.6 > Gestion de la politique de certification

1.6.1 > Entité gérant la politique de certification

L'entité en charge de l'administration et de la gestion de la présente politique de certification est le comité de pilotage DOCAPOSTE Trust & Sign (§ 1.4.1 > Autorité de Certification). Il est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.

1.6.2 > Point de contact

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

1.6.3 > Procédures d'approbation de la conformité de la PC et de la DPC

Cette PC sera revue périodiquement, a minima annuellement et à chaque changement majeur, par le comité de pilotage de l'AC pour assurer sa conformité aux normes de sécurité attendues par l'organisme de contrôle national (cf. Règlement européen eIDAS 910/2014).

1.7 > Abréviations

Les abréviations utilisées dans la présente P.C. sont les suivantes :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CPS	Certification practice statements (déclaration des pratiques de certification)

CSR	Certificate signing request
CRL	Liste des Certificats Révoqués (Certificate revocation list)
DN	Distinguished Name (nom distinctif)
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de gestion de clés
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol
OID	Object Identifier (identifiant d'objet)
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Électronique
PSCo	Prestataire de Service de Confiance
SSI	Sécurité des Systèmes d'Information
UH	Unité d'horodatage
URL	Uniform Resource Locator (adresse universelle)

2 / Responsabilités concernant la mise à disposition des informations devant être publiées

2.1 > Entités chargées de la mise à disposition des informations

Suite à l'approbation des politiques (et, éventuellement, autres informations publiées, cf. Tableau 2) par le comité de suivi de l'AC, le chef de projet fait une demande de publication à l'équipe chargée de la publication des opérations.

2.2 > Informations publiées

Le présent document[1]	http://pki.trust.idemia.io/policies/idemia-eidas-cp-lightweight-ca.pdf
Les conditions générales d'utilisation[1]	http://pki.trust.idemia.io/agreement/idemia-eidas-tac.pdf
Les certificats de l'AC en cours de validité[2]	http://pki.trust.idemia.io/cer/idemia-eidas-lightweight-ca.cer
Le certificat de l'AC racine et son empreinte cryptographique	http://pki.trust.idemia.io/cer/idemia-eidas-root-ca.cer SHA256(idemia-eidas-root.cer) : a22b214c91daf26bd8304f9f6f81d4d75aed28dd32cfb2d37163b24819d1cbf2
La PC de l'AC racine	http://pki.trust.idemia.io/policies/idemia-eidas-cp-root-ca.pdf
La CRL	http://pki.trust.idemia.io/crl/idemia-eidas-lightweight-ca.crl
L'ARL de l'AC racine	http://pki.trust.idemia.io/crl/idemia-eidas-root-ca.crl

[1] Version en vigueur et précédentes, le cas échéant

[2] Cela inclut les certificats *OCSP*.

Les mesures de sécurité techniques et non techniques	https://pki.trust.idemia.io/policies/idemia-eidas-security-measures.pdf

Tableau 2 – Informations publiées par l'AC

2.3 > Délais et fréquences de publication

Les informations liées à la l'autorité de certification d'entités, les systèmes ont une disponibilité de 7 jours sur 7, 24h sur 24. Le SLA assuré sur cette fonction est de 99.5% mensuel.

2.4 > Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est en 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).

3 / Identification et authentification

3.1 > Nommage

3.1.1 > 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 structuré comme suit, conformément à la norme ETSI EN 319 412-3.

Certificat personne physique
- **CN (Common Name) au format UTF-8 qui est la concaténation du Nom et du prénom. Optionnellement, le suffixe « - Test » peut être ajouté pour émettre un certificat temporaire de démonstration par exemple.** - **GN (givenName) au format UTF-8 contient le prénom de la personne physique** - **SN (surName) au format UTF-8 contient le nom de famille de la personne physique** - **SERIALNUMBER : numéro unique généré par l'application appelante** - **C (CountryName) au format PrintableString, contenant le code ISO 3166-2 de la nationalité du porteur (« FR » pour une personne de nationalité Française)**

3.1.2 > Nécessité d'utilisation de noms explicites

Les noms des porteurs sont explicites.

3.1.3 > Pseudonymisation des porteurs

Les certificats des porteurs ne sont pas pseudonymisés.

3.1.4 > Règles d'interprétation des différentes formes de nom

Aucune exigence n'est stipulée en plus des règles spécifiées ci-dessus.

3.1.5 > Unicité de Noms

Concernant le sujet d'un certificat, l'unicité du DN est assurée à l'aide du champ SN.

3.2 > Validation initiale de l'identité

3.2.1 > Méthode pour prouver la possession de la clé privée

Les clés sont générées par l'application de signature de DOCAPOSTE Trust & Sign qui la transmet de façon sécurisée à l'AC

3.2.2 > Validation de l'identité d'un organisme

Non applicable.

3.2.3 > Validation de l'identité d'un individu

Le dossier d'enregistrement, dématérialisé, comprend :

- Une demande de certificat dématérialisée et acceptée par le porteur
- Les CGUs validées par le demandeur
- Une copie d'une pièce d'identité valide.

La vérification de l'identité du porteur est réalisée à distance par l'AE partenaire en s'appuyant sur la pièce d'identité fournie.

Deux méthodes sont prévues :

- Identification initiale : « Remote Onboarding »
  - Identification automatisée de la pièce d'identité (recto / verso) avec optionnellement une reconnaissance faciale dynamique du porteur
- Identification a posteriori, faisant suite à l'identification initiale : « Remote Post-boarding »
  - Identification du porteur par l'application métier selon une méthode validée par IDEMIA

Le processus de signature est par la suite décrit dans la politique de signature « Service de signature avancée avec identification à distance », selon le schéma simplifié suivant :

La demande de certificat dématérialisée est transmise à IDEMIA.

La copie de la pièce d'identité sera, en fonction de la convention AC/AE mise en place :

- Soit conservée par l'AE pendant au moins 7 ans après la fin de validité du certificat
- Soit transmise à DOCAPOSTE Trust & Sign pour archivage.

3.2.4 > Informations non vérifiées du RC

Sans objet.

3.2.5 > Validation de l'autorité du demandeur

Sans objet, le demandeur et le signataire sont la même personne.

3.2.6 > Certification croisée d’AC

Pas d'exigences en l'état actuel de la PC.

3.3 > Identification et validation d'une demande de renouvellement des clés

Non applicable. Les certificats étant éphémères, ils ne font pas l’objet de renouvellement.

3.4 > Identification et validation d’une demande de révocation

Le certificat de personne physique est révoqué :

- Automatiquement en cas d’abandon du processus de signature ou en cas de refus explicite de signer
- En cas de demande explicite de révocation auprès de l’AC.

4 / Exigences opérationnelles sur le cycle de vie des certificats

4.1 > Demande de certificat

4.1.1 > Origine d'une demande de certificat

La demande est réalisée par le porteur au cours d'un processus de signature électronique opéré par DOCAPOSTE Trust & Sign à la demande d'un de ces clients.

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

Le processus est pris en charge par DOCAPOSTE Trust & Sign à travers le processus de signature électronique.

4.2 > Traitement d'une demande de certificat

4.2.1 > Exécution des processus d'identification et de validation de la demande

Le processus d'identification décrit en § 3.2.3 > Validation de l'identité d'un individu est réalisé par un opérateur de l'AE Partenaire DOCAPOSTE Trust & Sign.

4.2.2 > Acceptation ou rejet de la demande

La demande est acceptée ou rejetée par l'AE Partenaire lors de l'analyse du dossier.

En cas de rejet, le RC en est informé directement par l'AE.

4.2.3 > Durée d'établissement du certificat

Le certificat est établi immédiatement au cours du processus de signature électronique.

4.3 > Délivrance du certificat

4.3.1 > Actions de l'AC concernant la délivrance du certificat

Le certificat est inclus dans le document signé.

4.3.2 > Notification par l'AC de la délivrance du certificat au RC

Le porteur est notifié à travers la réussite du processus de signature.

4.4 > Acceptation du certificat

4.4.1 > Démarche d'acceptation du certificat

Le certificat est implicitement accepté à sa première utilisation.

4.4.2 > Publication du certificat

Les certificats des porteurs ne sont pas publiés par l’AC.

4.4.3 > Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.5 > Usages de la bi-clé et du certificat

4.5.1 > Utilisation de la clé privée et du certificat par le RC

Les RC doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

Certificat personne physique

L'utilisation de la clé privée est strictement limitée à la création de signatures électroniques avancées ou simples au sens du Règlement européen 910/2014 (dit « eIDAS ») dans le cadre d'un processus de signature opéré par un service Saas de DOCAPOSTE Trust & Sign.

Certificat d'OCSP
L'utilisation de la clé privée et du certificat est strictement limitée à la production de réponse OCSP.

4.5.2 > Utilisation de la clé publique et du certificat par l'utilisateur du certificat

La présente PC ne formule aucune exigence sur ce point.

4.6 > Renouvellement d'un certificat

Sans objet : le renouvellement est interdit dans le cadre de la présente PC. Un certificat ne peut être renouvelé sans renouvellement de la bi-clé correspondante.

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

Non applicable.

4.8 > Modification du certificat

Sans objet ; la modification de certificat n'est pas autorisée par la présente PC.

4.9 > Révocation et suspension des certificats

4.9.1 > Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat électronique :

- Les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat

- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement
- Le porteur n’a pas respecté les obligations découlant de la présente PC
- La clé privée du service applicatif est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d’activation associées)
- L’arrêt définitif du service applicatif ou la cessation d’activité de l’entité de rattachement du service
- Le porteur demande la révocation du certificat

Lorsqu’une des circonstances ci-dessus se réalise et que l’AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

4.9.2 > Origine d’une demande de révocation

Le signataire peut demander à révoquer son certificat.

4.9.3 > Procédure de traitement d'une demande de révocation

La révocation du certificat est prise en compte dans le processus de signature, en cas de refus de signature.

4.9.4 > Délai accordé au RC pour formuler la demande de révocation

Dès que le signataire a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.9.5 > Délai de traitement par l'AC d’une demande de révocation

La révocation est immédiate.

4.9.6 > Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

4.9.7 > Fréquence d'établissement des LCR

Les LCR sont publiées toutes les heures.

4.9.8 > Délai maximum de publication d'une LCR

Une LCR est publiée au plus 60 minutes après sa génération.

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

L'AC propose un service OCSP accessible à l'adresse indiquée dans les certificats. Voir § 4.10.1 > Disponibilité de la fonction. Ce service est disponible 7 jours sur 7, 24h sur 24 avec un niveau de disponibilité de 99,5% mensuel.

4.9.10 > Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.11 > Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats cachet et d'horodatage, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, la révocation suite à une compromission de la clé privée fera l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

Quant au porteur, l'AC impose par voie contractuelle qu'en cas de compromission de sa clé privée du porteur ou de connaissance de la compromission de la clé privée de l'AC, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.12 > Suspension de certificats

Sans objet ; la suspension des certificats n'est pas autorisée par la présente PC.

4.10 > Fonction d'information sur l'état des certificats

4.10.1 > Disponibilité de la fonction

Cette fonction à un niveau de disponibilité de 99.5% mensuel.

Le temps de réponse du serveur de vérification en ligne du statut d'un certificat (OCSP) à la requête reçue est inférieur à 10 secondes.

4.10.2 > Fin de la relation entre le RC et l'AC

En cas de fin de relation contractuelle ou hiérarchique entre l'AC et l’entité de rattachement avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

4.11 > Séquestre de clé et recouvrement

Sans objet, il n'est procédé à aucun séquestre ni recouvrement des clés privées des RC.

Il n’est procédé à aucun séquestre ni recouvrement des clés d’AC.

5 / Mesures de sécurité non techniques

5.1 > Mesures de sécurité physique

Se référer au document '*IGC_IDEMIA_ Mesures_sécurité*'.

5.2 > Mesures de sécurité procédurales

Se référer au document 'IGC_IDEMIA_ Mesures_sécurité'.

5.3 > Mesures de sécurité vis-à-vis du personnel

Se référer au document 'IGC_IDEMIA_ Mesures_sécurité'.

5.4 > Procédures de constitution des données d'audit

Se référer au document 'IGC_IDEMIA_ Mesures_sécurité'.

En plus des éléments communs décrits dans le document 'IGC_IDEMIA_ Mesures_sécurité' la présente PC précise les éléments suivants.

5.4.1 > Type d'événements à enregistrer

En particulier, IDEMIA distingue les catégories d'événements et de trace suivants :

- Les événements et traces techniques inscrits dans les dossiers d'enregistrement ;
- Les traces techniques relatives au cycle de vie des certificats, au cycle de vie des clés cryptographiques associées, au processus de vérification de l'identité ainsi qu'aux demandes de révocation.
- Les autres traces techniques assurant l'imputabilité des actions.

5.5 > Archivage des données

Se référer au document 'IGC_IDEMIA_ Mesures_sécurité'.

En plus des éléments communs décrits dans le document 'IGC_IDEMIA_ Mesures_sécurité' la présente PC/DPC précise les durées d'archivage suivant :

Elément	Durée d'archivage
Dossier d'enregistrement du porteur	7 ans après la fin de validité du certificat associé
Traces techniques relatives au cycle de vie des certificats des porteurs	Au maximum 7 ans après la fin de vie du certificat associé
Traces techniques relatives au cycle de vie des certificats des clés des porteurs	Au maximum 7 ans après la fin de vie du certificat associé
Traces techniques relatives à la vérification de l'identité du porteur	Au maximum 7 ans après la fin de vie du certificat associé
Traces techniques relatives aux demandes de révocation	Au maximum 7 ans après la fin de vie du certificat associé
Autres traces techniques (traces de pare-feu, activité des serveurs web…)	1 an après leur génération.

5.6 > Changement de clé d'AC

Se référer au document 'IGC_IDEMIA_ Mesures_sécurité'.

5.7 > Reprise suite à compromission et sinistre

Se référer au document 'IGC_IDEMIA_ Mesures_sécurité'.

5.8 > Fin de vie de l'IGC

Se référer au document 'IGC_IDEMIA_ Mesures_sécurité'.

6 / Section 6. Mesures de sécurité techniques

Se référer au document ‘‘*IGC_IDEMIA_ Mesures_sécurité*’. Ce chapitre ne décrit que les particularités de la présente PC quant à la gestion des bi-clés et certificats des porteurs.

6.1 > Génération des bi-clés et installation

6.1.1 > Transmission de la clé privée à son propriétaire

Les clés des certificats des signataires sont directement générées dans un environnement sécurisé opéré par DOCAPOSTE Trust & Sign.

6.1.2 > Transmission de la clé publique à l’AC

Les modes de transmission de la clé publique des porteurs sont définis dans la procédure de demande de certificat (§ 4.2 > Traitement d'une demande de certificat).

6.1.3 > Taille des clés

Les porteurs utilisent des clés RSA de 2048 bits minimum.

Les serveurs OCSP ont des clés de 4096 bits minimum.

L’AC suit les recommandations cryptographiques de l’autorité de contrôle des PSCO.

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

Les caractéristiques des bi-clés des porteurs sont validées par l’AE durant la validation de la demande.

6.1.5 > Objectifs d'usage de la clé

Pour les certificats des porteurs, voir §1.5.1 > Bi-clés et certificats des porteurs.

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

Certificat personne physique
La clé privée est protégée par un environnement sécurisé et est détruite après son utilisation. La clé privée ne peut être activée qu'après une authentification du signataire. La méthode d'authentification mise en œuvre doit être approuvée par IDEMIA.

Certificat d'OCSP
La clé privée est protégée dans un dispositif cryptographique certifié critères communs EAL4+.

6.3 > Autres aspects de la gestion des bi-clés

6.3.1 > Archivage des clés publiques

Pas d'exigence particulière concernant les clés des porteurs.

6.3.2 > Durées de vie des bi-clés et des certificats

Certificat personne physique
La clé privée et le certificat associé a une durée de vie de 50 min maximum (T0-5 ; T0+45). La clé privée est détruite après son utilisation.

Certificat d'OCSP
Le certificat et la clé ont une durée de vie limitée à 1 (un) an.

7 / Profils

7.1 > Profil des certificats

Les certificats émis respectent la norme X.509 v3. Les champs et extensions sont ceux définis dans la RFC 5280.

7.1.1 > Autorité de Certification ‘IDEMIA LCP CA’

Attribut	Valeur
Version	3 (0x2)
Serial Number	1120267BEB5D8504C9FE0292B7DCC7ACDD03
Signature Algorithm	sha512WithRSAEncryption
Issuer	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=IDEMIA eIDAS Root CA
Not Before	Jun 30 00:00:00 2020 GMT
Not After	Jun 30 00:00:00 2040 GMT
Subject	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=IDEMIA eIDAS Lightweight CA
Public Key Algorithm	rsaEncryption
Key length	4096 bit

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:TRUE Pathlen: 0
Subject Key Identifier	Méthode 1
Key Usage	Critical Certificate Sign, CRL Sign

Authority Information Access	CA Issuers : http://pki.trust.idemia.io/cer/idemia-eidas-root-ca.cer
CRL Distribution Points	http://pki.trust.idemia.io/crl/idemia-eidas-root-ca.crl
Certificate Policies	Policy : X509v3 Any Policy CPS : http://pki.trust.idemia.io/policies/
Authority Key Identifier	Méthode 1

7.1.2 > Certificat de personnes physiques

Attribut	**Valeur**
Version	3 (0x2)
Serial Number	20 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=IDEMIA eIDAS Lightweight CA
Not Before	MM DD HH:MM:SS YYYY GMT (T0 -5mn)
Not After	MM DD HH:MM:SS YYYY GMT (T0 +45mn)
Subject	C=<Nationalité> SERIALNUMBER=<Numéro unique de transaction fournit par l'application appelante> GN=<Prénom> SN=<Nom> CN=< Prénom Nom>
Public Key Algorithm	rsaEncryption
Key length	2048 bits

Extension X.509 v3	Valeur
Basic Constraints	CA:FALSE
Authority Key Identifier	Méthode 1
Authority Information Access	CA Issuers : http://pki.trust.idemia.io/cer/idemia-eidas-lightweight-ca.cer OCSP : http://pki.trust.idemia.io/ocsp/idemia-eidas-lightweight-ca
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.4.1.1 CPS : http://pki.trust.idemia.io/policies/ Policy : 0.4.0.2042.1.3
Subject Key Identifier	Méthode 1
Key Usage	Critical Non repudiation

7.1.3 > Certificat OCSP

Attribut	Valeur
Version	3 (0x2)
Serial Number	20 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=IDEMIA eIDAS Lightweight CA
Not Before	MM DD HH:MM:SS YYYY GMT
Not After	MM DD HH:MM:SS YYYY GMT (+ 1 an)
Subject	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=OCSP Responder <xx>
Public Key Algorithm	rsaEncryption
Key length	4096 bits

Extension X.509 v3	Valeur
Authority Key Identifier	Méthode 1
Extended Key Usage	ocspSigning
OCSP no check	✓
Subject Key Identifier	Méthode 1
Key Usage	Critical Digital Signature

7.2 > Profil des CRL

Champ/Extension	Valeur
Version	2 (0x01)
Algorithme de signature	RSA / SHA512
Issuer	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=IDEMIA eIDAS Lightweight CA
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 6 jours
Authority Key Identifier	inclus
Numéro de série	Généré automatiquement par l'AC

Les numéros de série des certificats révoqués sont maintenus dans la CRL jusqu'à la date d'expiration du certificat.

7.3 > Profil des réponses OCSP

L'OCSP de l'AC respecte le standard RFC 6960. Le profil de la réponse OCSP est la suivante

Champ/Extension	Valeur
Type de réponse	Basic OCSP response
Version	1 (0x00)
Date de production	Heure GMT
Certificate ID	Algorithme de hachage Haché du l'émetteur du certificat Haché de la clé publique de l'émetteur Numéro de série du certificat.
Statut du certificat	Statut de révocation du certificat.
Date de début de validité	Heure GMT
Date de fin de validité	Date de début de validité plus : • Statut « Good » : 24 minutes • Statut « Revoked » : 72 minutes • Statut « Unknown » : 15 secondes
Nonce (conditionnel)	Valeur de la requête si présent

OCSP Archive cutoff	Date de production depuis le début de validité de l'AC
Algorithme de signature	RSA / SHA256
Certificat de l'OCSP	Inclus

8 / Audit de conformité et autres évaluations

Se référer au document ‘IGC_IDEMIA_ Mesures_sécurité’.

9 / Autres problématiques métiers et légales

9.1 > Tarifs

Sans objet.

9.2 > Responsabilité financière

En cas d'inadéquation constatée entre l'utilisation des licences et les droits concédés dans le présent document, les Parties se rapprocheront pour discuter de la bonne foi des conditions financières de régularisation. À défaut d'accord, le CLIENT fera le nécessaire pour revenir aux droits d'utilisation concédés dans les plus brefs délais.

Ces stipulations sont arrêtées sans préjudice de l'indemnisation qui sera due à AC IDEMIA LCP CA en réparation de la violation des conditions d'utilisation des Services par le Client et de l'éventuelle résiliation du Contrat qui pourra intervenir dans les conditions prévues à l'article 20 des présentes.

9.3 > Confidentialité des données professionnelles

9.3.1 > 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 d'IDEMIA
- Les données d'activation associées aux clés privées des autorités de l'IGC d'IDEMIA
- Tous les secrets de l'IGC d'IDEMIA
- Les journaux d'événements des composantes des services de confiance d'IDEMIA
- Le dossier d'enregistrement des porteurs
- Les causes de révocations, sauf accord explicite de publication ;
- Le procès-verbal de cérémonie de clés.

9.3.2 > Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 > Responsabilités en termes de protection des informations confidentielles

IDEMIA, en tant que fournisseur de services de confiance, est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

9.3.4 > Protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'ensemble des services de confiance d'IDEMIA sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

9.3.5 > Responsabilité en termes de protection des données personnelles

Se référer à la législation et à la réglementation en vigueur sur le territoire français.

9.3.6 > Notification et consentement d'utilisation des données personnelles

Se référer à la législation et à la réglementation en vigueur sur le territoire français.

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

Se référer à la législation et à la réglementation en vigueur sur le territoire français.

9.4 > Droits sur la propriété intellectuelle et industrielle

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

9.5 > Limite de garantie

Sans objet.

9.6 > Limite de responsabilité

La responsabilité d'IDEMIA ne pourra être engagé en cas d'utilisation des clés privées et des certificats pour un usage autre que ceux prévus.

9.7 > Indemnités

Sans objet.

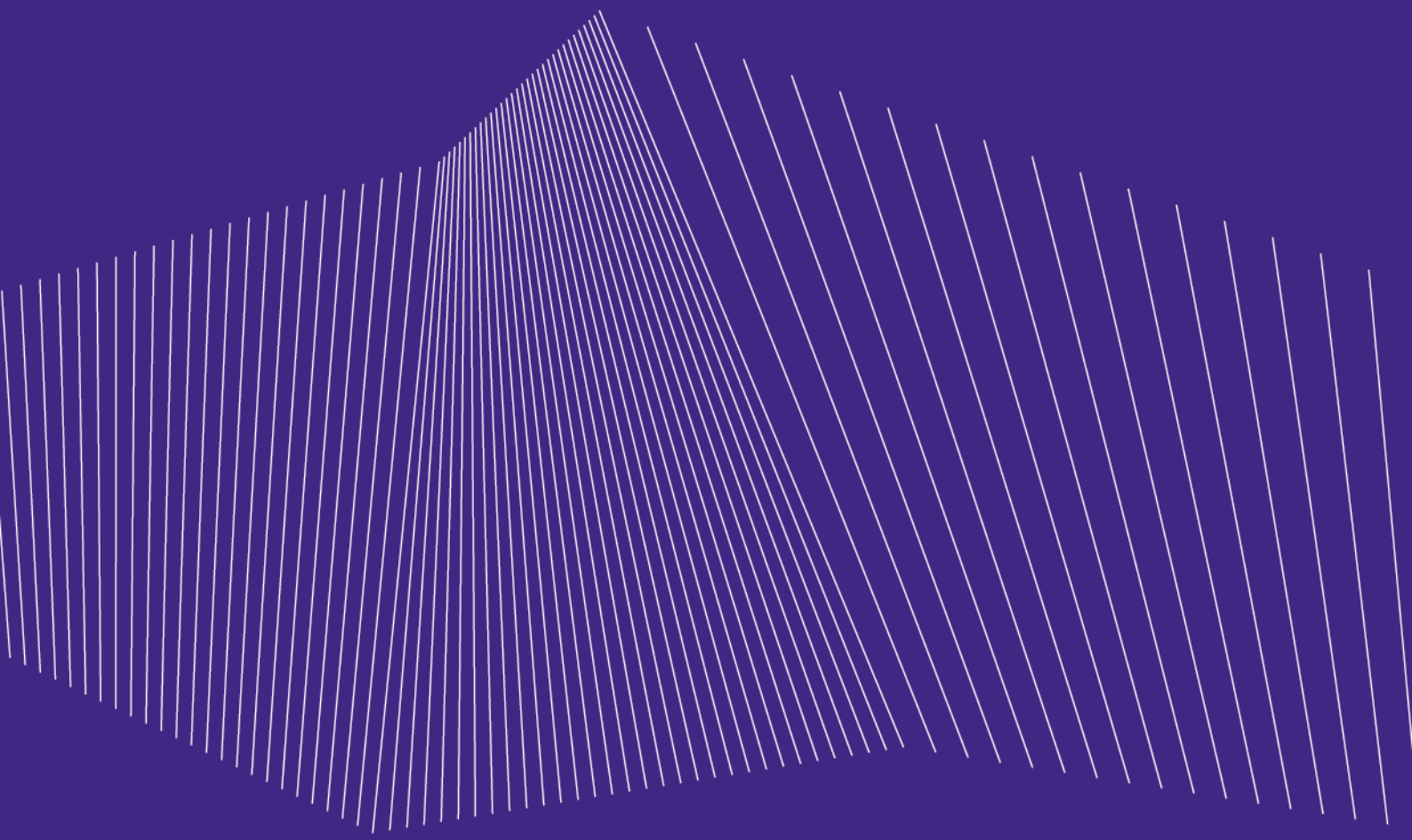
9.8 > Conformité aux législations et réglementations

Les pratiques d'IDEMIA sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures d'IDEMIA prennent en compte, dans la mesure du possible, l'accessibilité à tous les utilisateurs, « quel que soit leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales » (https://www.w3.org/Translations/WCAG20-fr/).

9.9 > Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.



IDEMIA

www.idemia.com