Politique et pratiques de certification – AC NCP+

V1.3 – Janvier 2022

IDEMIA

Sommaire

Introduction

Le présent document décrit les procédures opérationnelles d'enregistrement l'AC NCP+ IDEMIA en vue d'émettre :

- Des certificats de scellement de niveau NCP+
- Des certificats de signature de personne physique de niveau NCP+ à durée de vie courte
- Des certificats d'unité d'horodatage de niveau NCP+

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	• Modification du §1.4.6 pour autoriser le RC à faire partie d'une autre société du même groupe • Ajout en §3.2.3 des documents pour vérifier l'appartenance des sociétés au même groupe • Ajout en §3.1.1 du format d'OI pour la Polynésie et la Nouvelle Calédonie
V1.3	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 NCP+ IDEMIA produisant des certificats électroniques de cachet destinés aux clients d'IDEMIA et des certificats de personnes physiques destinés à être utilisés par leur propre clients dans le contexte d'un processus de signature dématérialisé. Par ailleurs, cette AC produit des certificats de cachet destinés à l'usage exclusif des unités d'horodatage du service d'horodatage d'IDEMIA (cf. PH).

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 cachets 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 »).

1.2 > Identification du document

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

Famille	OID	Conformité
Cachet	1.3.6.1.4.1.54916.1.3.1.1	*ETSI EN 319 411-1 NCP+ 0.4.0.2042.1.2*
Personne Physique (certificat à durée de vie courte)	1.3.6.1.4.1.54916.1.3.2.1	*ETSI EN 319 411-1 NCP+ 0.4.0.2042.1.2*
Horodatage	1.3.6.1.4.1.54916.1.3.3.1	*ETSI EN 319 411-1 NCP+ 0.4.0.2042.1.2*
OCSP		*N/A*

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

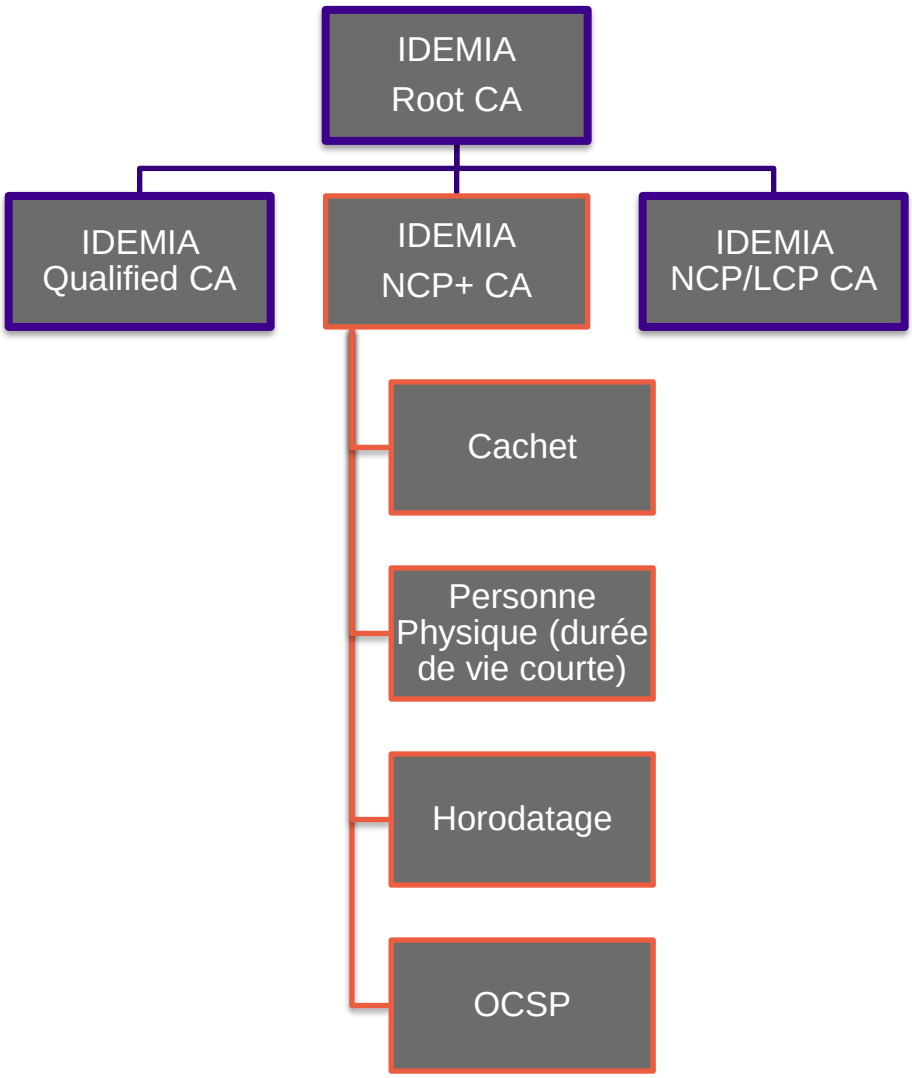
Les certificats OCSP sont des certificats techniques utilisés par la fonction d'information sur l'état des certificats de l'AC (§ 4.10 > Fonction d'information sur l'état des certificats). Ce sont des certificats émis par l'AC pour ses propres usages

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 orange.

1.4.1 > Autorité de Certification

L'autorité de certification IDEMIA NCP+ 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.

Certificat de cachet
L'AE est portée par IDEMIA. Elle est opérée par DOCAPOSTE Trust & Sign.

Certificat personne physique
L'AE est opérée par un client d'IDEMIA

Certificat d'horodatage
L'AE est portée par IDEMIA. Elle est opérée par DOCAPOSTE Trust & Sign.

1.4.3 > Opérateur d'enregistrement (OE)

L’opérateur d’enregistrement, est la personne physique, rôle de confiance, en charge de la vérification de l’identité du futur porteur de certificat.

Certificat de cachet
L’OE est un membre de DOCAPOSTE Trust & Sign.

Certificat personne physique
L’OE en tant que personne physique est employé par un client d’IDEMIA ou bien selon un processus automatisé accepté équivalent.

Certificat d’horodatage
L’OE est un membre de DOCAPOSTE Trust & Sign.

1.4.4 > Opérateur de révocation (OR)

L’opérateur de révocation, est la personne physique, rôle de confiancede l’AC, en charge de la vérification des demandes de révocation et de leur traitement.

Certificat de cachet
L’opérateur est en charge des demandes manuelles dans le cadre de la procédure définie au §4.9 > Révocation et suspension des certificats.

Certificat personne physique
S’agissant, dans le cadre de cette PC, de certificats éphémères uniquement utilisés dans le cadre d’un processus de signature sous le contrôle de DOCAPOSTE Trust & Sign, 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 pour les certificats éphémères.

Certificat d’horodatage
L’opérateur est en charge des demandes manuelles dans le cadre de la procédure définie au §4.9 > Révocation et suspension des certificats.

1.4.5 > Porteurs de certificats

Un porteur de certificat est une entité physique (resp. morale) signant (resp. scellant) des documents électroniques en son nom.

Certificat de cachet
Il s'agit d'une personne morale, client d'IDEMIA

Certificat personne physique
Il s'agit d'une personne physique.

Certificat d'horodatage
Il s'agit de l'AH IDEMIA (AH non qualifiée)1.

1.4.6 > Responsable de certificat de cachet (RC)

Le RC n'est défini que pour l'émission de certificat de cachet.

Certificat de cachet
Le RC est la personne physique responsable du certificat de cachet, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat. Cette personne utilise la clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle elle a un lien réglementaire. Dans le cadre de cette PC, le RC est forcément : ▪ Mandataire social de cette entité ou ▪ Salarié de cette entité ou salarié du groupe dont l'entité fait partie Un groupe est défini comme un ensemble de sociétés qui sont toutes contrôlées, directement ou indirectement, par une même société mère, en appliquant les critères de contrôles de l'article L233-3 du Code du Commerce. Le RC respecte les conditions qui lui incombent telles que définies dans la présente PC. Il est rappelé que le certificat étant attaché au serveur informatique et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc. L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions. L'AC révoque un certificat de cachet pour lequel il n'y a plus de RC explicitement identifié.

1.4.7 > Responsable de certificat d'UH (RCUH) ou responsable d'UH

Certificat d'horodatage

[1] Dans la présente version de la PC, il n'est pas prévu de fournir des certificats d'horodatage à une société autre qu'IDEMIA. Les versions ultérieures de la PC pourront envisager cette possibilité.

Le responsable d'UH est un RC désigné par l'AH non-qualifiée IDEMIA.

1.4.8 > Utilisateurs de certificats

Les Utilisateurs sont les personnes physiques et morales destinataires des documents signés, scellés électroniquement ou horodatés.

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 > Usages de la bi-clé et du certificat ci-dessous. L'AC respecte ces restrictions et impose leur respect par ses RC et ses utilisateurs de certificats.

À cette fin, elle communique à tous les signataires, les RC et utilisateurs potentiels les termes et conditions 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 DOCAPOSTE Trust & Sign (§ 1.4.1 > Autorité de Certification). Elle 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, Tableau 3) 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

Tableau 2 – Informations publiées par l'AC

Le présent document[2]	http://pki.trust.idemia.io/policies/idemia-eidas-cp-ext-normalized-ca.pdf
Les conditions générales d'utilisation[2]	http://pki.trust.idemia.io/agreement/idemia-eidas-tac.pdf
Les certificats de l'AC en cours de validité[3]	http://pki.trust.idemia.io/cer/idemia-eidas-extended-normalized-ca.cer
Le certificat de l'AC racine et son empreinte cryptographique	http://pki.trust.idemia.io/cer/idemia-eidas-root.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-extended-normalized-ca.crl
L'ARL de l'AC racine	http://pki.trust.idemia.io/crl/idemia-eidas-root-ca.crl
Les mesures de sécurité techniques et non techniques	https://pki.trust.idemia.io/policies/idemia_eidas_security_measures.pdf

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

[3] Cela inclut les certificats *OCSP* (OID : 1.3.6.4.1.49640.2.1.3.1).

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 de cachet[4]

- **CN (Common Name) au format UTF-8. Cette mention est obligatoire. C'est le nom commercial ou public de l'entité morale. Optionnellement, le suffixe « - Test » peut être ajouté pour émettre un certificat temporaire de démonstration par exemple.**
- **OI (OrganizationIdentifier) au format UTF-8. Il est constitué :**
  ○ **Pour les organisations immatriculées en France et enregistrées au SIRENE, du numéro de SIREN ou de SIRET de l'organisation représentée par le porteur, tel que figurant au Kbis, précédé des caractères « NTRFR- ».**
  ○ **Pour les autres organisations Européennes, il est composé de**
  ▪ **Des caractères « VAT<XX>- » où « <XX> est remplacé par les deux caractères ISO 3166 du pays d'enregistrement de la société, suivi**
  ▪ **Du numéro de TVA intra-communautaire de la société**
  ○ **Pour les organisations immatriculées en Polynésie Française, du numéro d'inscription au Répertoire Territorial des Entreprises, « T.A.H.I.T.I » à 6 chiffres, de l'organisation représentée par le porteur, tel que figurant au Kbis, précédé des caractères « NTRPF- ».**
  ○ **Pour les organisations immatriculées en Nouvelle Calédonie et qui ne sont pas enregistrées au SIRENE, du numéro d'immatriculation au RCS de Nouméa de l'organisation représentée par le porteur, tel que figurant au Kbis, précédé des caractères « NTRNC- ».**
- **O (Organization) au format UTF-8. Il est constitué de la raison sociale de l'organisation représentée par le porteur, tel que figurant par exemple au K-Bis.**
- **C (CountryName) au format PrintableString, contenant le code iso 3166-2 du Pays ou du Territoire (FR pour la France, PF pour la Polynésie Française, NC pour la Nouvelle Calédonie)**

-

Certificat personne physique

- **CN (Common Name) au format UTF-8 qui est la concaténation du prénom et du nom. 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)**

Certificat d'horodatage[5]

- **CN (Common Name) au format UTF-8. Identifiant de l'UH de la forme « IDEMIA - Time-Stamping Unit XX » où XX est le numéro d'indice de l'UH.**
- **OI (OrganizationIdentifier) au format UTF-8. Il est constitué du numéro de SIREN d'IDEMIA précédé des caractères « NTRFR- », soit « NTRFR-440305282 ».**
- **O (Organization) au format UTF-8 contient la chaîne « Idemia Identity & Security France ».**
- **C (CountryName) au format PrintableString, contenant la chaîne « FR ».**

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,

- Pour un certificat de cachet, l'unicité du DN est assurée à l'aide des champs CN et OI.
- Pour un certificat de personne physique, l'unicité du DN est assurée à l'aide du champ SERIAL NUMBER.

[5] La version actuelle de cette PC ne considère l'émission de certificat d'horodatage que pour l'AH IDEMIA. Les versions futures pourront le cas échéant permettre l'émission de certificats d'UH pour des AH tierces.

3.2 > Validation initiale de l'identité

3.2.1 > Méthode pour prouver la possession de la clé privée

Le RC ou le responsable de l'unité d'horodatage fournit une CSR signée avec la clé privée (format PKCS #10).

3.2.2 > Validation de l'identité d'un organisme

Elle est vérifiée lors de l'enregistrement du RC. Voir ci-dessous.

3.2.3 > Validation de l'identité d'un individu

→ Enregistrement d'un RC

L'enregistrement du futur porteur (personne morale) nécessite l'identification de cette entité et l'identification de la personne physique responsable du certificat (RC), et la preuve du rattachement de la personne physique à l'entité.

S'agissant d'un certificat de cachet, le responsable de certificat de cachet (RC) doit de plus être habilité à ce rôle en tant que RC pour le service de création de cachet considéré.

Certificat de cachet
Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre : - **Un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le RC auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le RC.** - **Une demande de certificat écrite, datée de moins de 3 mois, signée par le RC de l'entité et comportant le nom du service de création de cachet concerné par cette demande** - **Toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;** - **Tout document attestant de la qualité du signataire du mandat ;** - **Une copie d'un document officiel d'identité en cours de validité du RC ou une carte professionnelle délivrée par une autorité administrative, comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ;** - **Une adresse électronique permettant à l'AC de contacter le RC ;** - **Les conditions générales d'utilisation signées par le RC ou le demandeur.** - **Si le RC fait partie d'une autre société au sein du groupe auquel appartient l'entité, les éléments attestant l'appartenance des 2 sociétés au même groupe (au sens des critères d'appartenance à un groupe indiqué au paragraphe 1.4.6 >)**

Dans le cas où DOCAPOSTE Trust & Sign ne génère pas la bi-clé dans son environnement mais que celle-ci est générée par le porteur, deux éléments complémentaires doivent être fournis :

- **Une CSR contenant la demande technique de certificat.**
- **Un engagement formel que la clé privée a été générée sur un dispositif conforme aux dispositions de la présente PC.**

Certificat d'horodatage

Dans le cas du certificat d'horodatage, IDEMIA ne créant des certificats d'UH que pour son propre compte et le responsable d'UH étant un rôle de confiance, seule la demande de certificat écrite devra être transmise. La demande doit comporter le CN (Common Name) identifiant explicitement l'UH à porter dans le certificat.

Ces documents sont transmis à l'AE qui les conserve.

L'identité du RC est vérifiée lors d'un face-à-face physique avec l'AE.

→ Enregistrement d'une Personne physique

Certificat personne physique

Le dossier d'enregistrement, dématérialisé, comprend :

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

La vérification de l'identité du porteur est réalisée lors d'un face-à-face (ou une méthode équivalente) par l'AE partenaire.

La demande de certificat dématérialisée est transmise à **DOCAPOSTE Trust & Sign**

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 vie 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

Cette étape est effectuée en même temps que la validation de l'identité du RC.

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

Certificat de cachet

Les bi-clés et les certificats de cachet sont renouvelés tous les trois ans.

Le renouvellement de la bi-clé implique la génération d'un nouveau certificat.

Le RC réalise une demande de renouvellement de son certificat selon les modalités d'une demande initiale.

L'AC réalise les vérifications suivantes :

- Existence du certificat à renouveler et vérification de la validité des informations contenues dans la demande de renouvellement certificat (existence de l'entreprise…) à l'identique de la précédente.
- Vérification de l'origine de la demande (identification du RC)
- Vérification de la validité du document officiel d'identité du RC (en cas d'expiration de la pièce, une copie d'une pièce valide devra être fournie)
- Vérification des CGU signées. En cas de modification des CGU, les nouvelles CGU devront être signés par le RC.

Dans tous les cas, un nouveau certificat ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante.

Certificat d'horodatage

Idem que pour le certificat de cachet à l'exception que les bi-clés et les certificats d'UH sont renouvelés tous les ans.

Certificat personne physique

Non applicable. Les certificats de personne physique étant à durée de vie courte, ils ne font pas l'objet de renouvellement.

3.4 > Identification et validation d'une demande de révocation

Certificat de cachet

Le RC et l'AE conviennent, lors de la contractualisation, du moyen à utiliser pour effectuer les demandes de révocation. Ce moyen doit garantir l'authenticité et l'intégrité des demandes.

- **Lors d'une demande sur le portail de service, le RC doit d'une part s'authentifier et d'autre part, fournir une copie de sa pièce d'identité. L'opérateur de révocation vérifiera la complétude du dossier conformément aux procédures internes** de DOCAPOSTE Trust & Sign, conforme au processus précédemment mis en place par **IDEMIA.**
- **En cas de défaillance du portail, par téléphone en contactant DOCAPOSTE Trust & Sign. Dans ce cas de figure, DOCAPOSTE Trust & Signs'assurera de l'identité du demandeur**

en lui demandant d'apporter la preuve de son identité, par exemple, par la transmission d'une copie de sa pièce d'identité à l'aide de son adresse email professionnel

Le responsable légal de l'entité devra également être formellement identifié par DOCAPOSTE Trust & Sign. Le responsable devra prouver son identité et son autorité. Cela pourra être réalisé, pour une entreprise par la fourniture, à l'aide d'un email professionnel :

- **de sa pièce d'identité**
- **d'un extrait de KBIS récent**

L'opérateur de révocation DOCAPOSTE Trust & Signs'assurera alors de la correspondance entre l'identité de la pièce et l'identité du responsable légal présente sur le KBIS.

Certificat d'horodatage

IDEMIA étant à la fois AC et AH, le processus de révocation est interne.

Certificat personne physique

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

Certificat de cachet
La demande peut être effectuée par le RC, dûment mandaté (cf. § 3.2.3 > Validation de l'identité d'un individu).

Certificat d'horodatage
La demande peut être effectuée par le RCUH

Certificat personne physique
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

Certificat de cachet
Une fois la demande déposée, le RC et l'AE conviennent d'un rendez-vous (présence physique des parties) pour l'enregistrement du RC.

Certificat d'horodatage
Le processus est un processus interne de DOCAPOSTE Trust & Sign, conforme au processus précédemment mis en place par IDEMIA

Certificat personne physique
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

Certificat de cachet
La demande et l'identification du RC sont validées comme décrit en § 3.2.3 > Validation de l'identité d'un individu. **DOCAPOSTE Trust & Sign est en charge de la génération des bi-clés de cachet sur les HSM hébergés par DOCAPOSTE Trust & Sign et de la demande technique (CSR) associée si elle n'est pas présente dans la demande.** **Par ailleurs, l'AE au travers des opérateurs d'enregistrement identifiés fortement, vérifie les paramètres des bi-clés générés (taille et module, dans le cas d'une bi-clé RSA).**

Certificat d'horodatage
Le RCUH est identifié dans le cadre d'une procédure interne de DOCAPOSTE Trust & Sign, conforme au processus précédemment mis en place par IDEMIA

Certificat personne physique
Le processus d'identification décrit en § 3.2.3 > Validation de l'identité d'un individu est réalisé par un opérateur de l'AE.

4.2.2 > Acceptation ou rejet de la demande

Certificat de cachet
La demande est acceptée ou rejetée par l'AE IDEMIA lors du face-à-face avec le RC. En cas de rejet, le RC en est informé directement par l'AE.

Certificat d'horodatage
Voir certificat de cachet

Certificat personne physique
La demande est acceptée ou rejetée par l'AE Partenaire lors du face-à-face avec l'opérateur d'AE.

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

4.2.3 > Durée d'établissement du certificat

Certificat de cachet
Le certificat est produit par l'AC dans un délai maximal de dix jours ouvrés après la validation par l'AE.

Certificat d'horodatage
Voir certificat de cachet

Certificat personne physique
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

Certificat de cachet
L'AC génère le certificat et le met à disposition du RC en ligne, via l'interface du centre de service (ServiceDesk).

Certificat d'horodatage
Voir certificat de cachet

Certificat personne physique
Le certificat est inclus dans le document signé.

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

Certificat de cachet
Le RC est informé par courrier électronique de la mise à disposition du certificat, à l'adresse fournie dans la demande.

Certificat d'horodatage

Voir certificat de cachet

Certificat personne physique

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

Certificat de cachet

Le certificat est accepté explicitement par validation du ticket par le client. En cas de non acceptation par le client, le certificat est considéré comme implicitement accepté au bout d'un mois et le ticket est fermé par **DOCAPOSTE Trust & Sign**.

Certificat d'horodatage

Le certificat d'horodatage est implicitement accepté dès l'émission de la première contremarque de temps.

Certificat personne physique

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.

Remarque : les certificats des UH ont vocation à être publiés par l'autorité d'horodatage à laquelle ils sont destinés au travers de leurs inclusions systématiques dans le jeton d'horodatage.

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 de cachet
L'utilisation de la clé privée et du certificat est strictement limitée à la production de cachets électroniques avancés au sens du Règlement européen 910/2014 (dit « eIDAS »).
Certificat d'horodatage
L'utilisation de la clé privée par une unité d'horodatage est strictement limitée à la création des jetons d'horodatages au sens du Règlement européen 910/2014 (dit « eIDAS ») de l'autorité d'horodatage IDEMIA.

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 dans le cadre d'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

Certificat de cachet
La demande et la délivrance d'un nouveau certificat suite à changement de la bi-clé suit la procédure du paragraphe 3.3 >

Certificat d'horodatage
Voir certificat de cachet

Certificat personne physique
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 RC 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 RC ou son entité n'ont pas respecté leurs 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 RC ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service applicatif et/ou de son support)

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

Certificat de cachet
Le certificat peut être révoqué par : - Le RC ; - Le responsable légal de l’entité mentionnée dans le certificat ; - L’AE ou l’AC.

Certificat d’horodatage
Le certificat peut être révoqué par : - Le RCUH ; - l’AH ou l’AC.

Certificat personne physique
Le signataire peut demander à révoquer son certificat.

4.9.3 > Procédure de traitement d'une demande de révocation

Certificat de cachet
Le RC peut demander la révocation de son certificat via le centre de service de l’AC à l’aide de 2 points d’entrée : - **Le portail Web mis à disposition (Service Desk)** - **En cas de défaillance du portail, par téléphone en contactant DOCAPOSTE Trust & Sign**

Certificat d’horodatage
La demande de révocation s’appuie sur une procédure interne de DOCAPOSTE Trust & Sign, conforme au processus précédemment mis en place par IDEMIA

Certificat personne physique
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 RC (ou une personne autorisée), le RCUH, ou 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

Certificat de cachet
Toute demande de révocation est traitée en urgence, dans un délai maximum de 24h entre la réception de la demande et son traitement (acceptation ou refus de la demande). Le RC est notifié de la révocation effective du certificat. Les demandes de révocation sont archivées par l’AC après traitement

Certificat d’horodatage
Voir certificat de cachet

Certificat personne physique
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 entité sont directement générées sur les ressources cryptographiques (HSM) des porteurs opérés par IDEMIA.

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 tailles de clés sont les suivantes :

AC	Certificat cachet	Certificat UH	Certificat personne physique	Certificat OCSP
RSA 4096	RSA 4096	RSA 4096	RSA 2048	RSA 4096

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

Les clés privées sont protégées par les modules cryptographiques conforme à la norme FIPS 140-2 level 2.

Certificat de cachet
Les clés privées sont protégées par les modules cryptographiques conforme à la norme FIPS 140-2 level 2 ou critères communs EAL4+. L'activation de la clé privée pour déclencher un scellement ne peut être réalisée qu'après l'authentification de l'organisation à l'aide d'un certificat client TLS pour les clés privées opérées sur les HSM DOCAPOSTE Trust & Sign. Si le HSM est opéré par le client d'IDEMIA, il doit conserver la clé privée sous le contrôle de son organisation, conformément à l'exigence de la norme ETSI EN 319 411-1.

Certificat personne physique
Les clés privées sont protégées par les modules cryptographiques conforme à la norme FIPS 140-2 level 2 ou critères communs EAL4+. La clé privée ne peut être activée qu'après une authentification à l'aide de deux facteurs du signataire. La méthode d'authentification mise en œuvre doit être approuvée par DOCAPOSTE Trust & Sign.

Certificat d'horodatage
Les clés privées sont protégées par les modules cryptographiques conforme à la norme FIPS 140-2 level 2 ou critères communs EAL4+.

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

Le tableau suivant fournit les durées de vie

Type de certificat	Durée de vie de la bi-clé	Durée de vie du certificat
AC	20 ans	20 ans
Certificat cachet	3 ans	3 ans
Certificat d'UH	1 an	6 ans
Certificat de personne physique	45mn	50mn
Certificat d'OCSP	1 an	3 ans

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 NCP+ CA’

Attribut	Valeur
Version	3 (0x2)
Serial Number	11203D9DE0C54124C17C95E93B765B33D10E
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 Extended Normalized 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 Cachet

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 Extended Normalized CA
Not Before	MM DD HH:MM:SS YYYY GMT
Not After	MM DD HH:MM:SS YYYY GMT (+ 3 ans)
Subject	C=<Pays> O=<Raison sociale> OI=<Semantique ETSI> CN=<Nom entreprise / Service>
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 : https://pki.trust.idemia.io/cer/idemia-eidas-normalized-ca.cer OCSP :

	http://pki.trust.idemia.io/ocsp/idemia-eidas-extended-normalized-ca
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.3.1.1 CPS : http://pki.trust.idemia.io/policies/ Policy : 0.4.0.2042.1.2
CRL Distribution Points	http://pki.trust.idemia.io/crl/idemia-eidas-extended-normalized-ca.crl
Subject Key Identifier	Méthode 1
Key Usage	Critical Digital Signature

7.1.3 > Unité d'horodatage

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 Extended Normalized CA
Not Before	MM DD HH:MM:SS YYYY GMT
Not After	MM DD HH:MM:SS YYYY GMT (+ 6 ans)
Subject	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=IDEMIA - Time-Stamping Unit <XX>
Public Key Algorithm	rsaEncryption
Key length	4096 bits

Extension X.509 v3	Valeur
Basic Constraints	CA:FALSE
Authority Key Identifier	Méthode 1

Authority Information Access	CA Issuers : https://pki.trust.idemia.io/cer/idemia-eidas-normalized-ca.cer OCSP : http://pki.trust.idemia.io/ocsp/idemia-eidas-extended-normalized-ca
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.3.3.1 CPS : http://pki.trust.idemia.io/policies/ Policy : 0.4.0.2042.1.2
Extended Key Usage	Critical Time Stamping
CRL Distribution Points	http://pki.trust.idemia.io/crl/idemia-eidas-extended-normalized-ca.crl
Subject Key Identifier	Méthode 1
Private Key Usage Period	Not After: MM DD HH:MM:SS YYYY GMT (+ 1 an)
Key Usage	Critical Digital Signature

7.1.4 > Certificat personne physique

Attribut	Valeur
Version	3 (0x2)
Serial Number	16 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C=FR O=Idemia Identity & Security France OI=NTRFR-440305282 CN=IDEMIA NCP+ 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 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 : https://pki.trust.idemia.io/cer/idemia-eidas-normalized-ca.cer OCSP : http://pki.trust.idemia.io/ocsp/idemia-eidas-extended-normalized-ca
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.3.2.1 CPS : http://pki.trust.idemia.io/policies/ Policy : 0.4.0.2042.1.2
CRL Distribution Points	http://pki.trust.idemia.io/crl/idemia-eidas-extended-normalized-ca.crl
Subject Key Identifier	Méthode 1
Key Usage	Critical Non repudiation

7.1.5 > 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 Extended Normalized 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 de la 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 Extended Normalized 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 l'AC IDEMIA NCP+ 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.

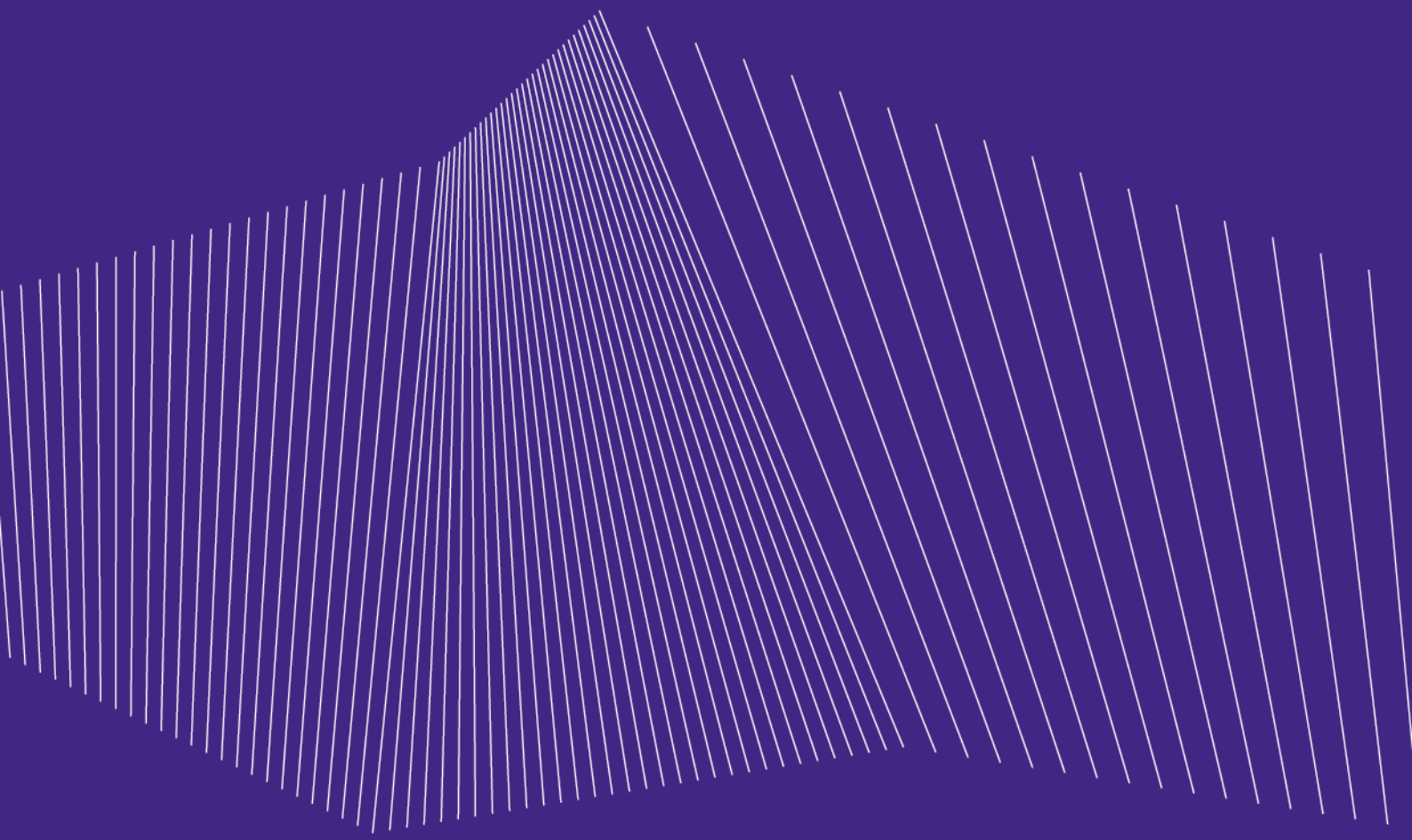
9.8 > Conformité aux législations et réglementations

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