Politique et pratiques de certification – AC Racine

V1.2 – Janvier 2022

IDEMIA

Sommaire

Introduction

Le présent document décrit les procédures opérationnelles de l'AC Racine IDEMIA en vue d'émettre des certificats aux AC filles IDEMIA.

L'historique de ce document est le suivant :

Numéro de version	Auteur	Commentaire
V1.0	PRO	Version initiale du document.
V1.1	PRO	Corrections typographiques
V1.2	JMD	Transfert DOCAPOSTE

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 Racine IDEMIA produisant des certificats électroniques d'AC destinés aux AC filles 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).

1.2 > Identification du document

La politique décrite dans le présent document est identifiée par l'OID suivant :

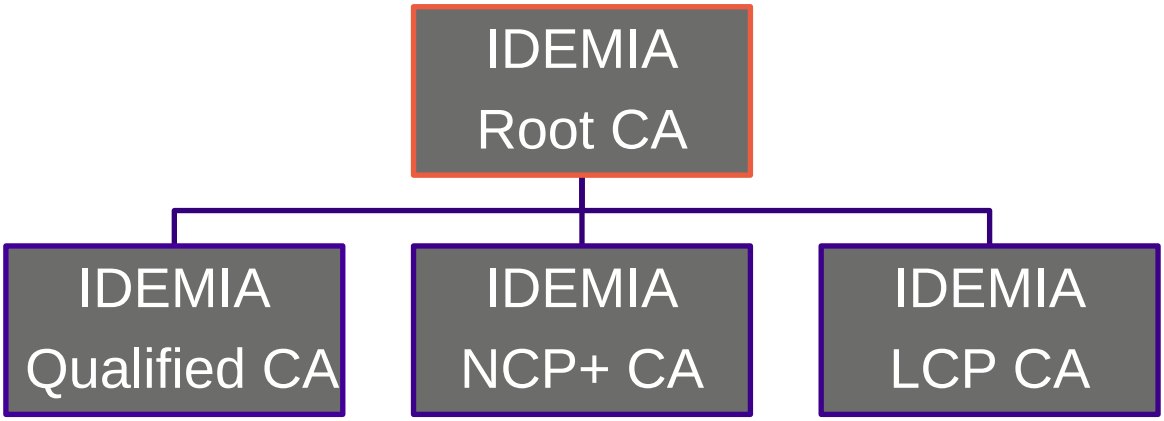
1.3.6.1.4.1.54916.1.1.1.1

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 Root 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 aux AC filles leur certificat	▪ *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 des AC filles 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

Les fonctions sous la responsabilité de IDEMIA sont opérées par DOCAPOSTE Trust & Sign, et peuvent être sous-traitées à des tiers sous la responsabilité 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'A.E. est portée par IDEMIA et n'enregistre que des demandes d'AC Fille d'IDEMIA.

1.4.3 > Porteurs de certificats

Le porteur de certificat dans le cadre de cette politique ne peut être qu'IDEMIA, en tant qu'organisme responsable des AC Filles de la hiérarchie[1].

[1] La présente version de cette PC n'envisage pas d'AC Fille appartenant à une autre entité d'IDEMIA. Une révision de la présente PC sera nécessaire pour permettre le rattachement d'AC Tierces à la racine IDEMIA.

1.4.4 > Utilisateurs de certificats

Les utilisateurs sont les personnes physiques et morales destinataires de certificats émis par les AC Filles d'IDEMIA.

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 à ses AC filles.

1.5.2 > Bi-clés et certificats d'AC

La clé de signature de l'AC Root IDEMIA est utilisée pour signer les certificats d'AC filles générés par l'AC Racine et l'ARL de l'AC Racine.

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 IDEMIA (§ 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
ARL	Authority Revocatin List (liste des autorités révoquées)
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 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

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.

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 des champs CN et OI. Lors du renouvellement d’une AC, un élément incrémental sera ajouté au CN par IDEMIA, tel que l’année d’émission.

3.2 > Validation initiale de l’identité

3.2.1 > Méthode pour prouver la possession de la clé privée

L’émission de la CSR est réalisée lors d’une cérémonie des clés.

3.2.2 > Validation de l'identité d'un organisme

Non applicable, les certificats sont uniquement émis au nom d’IDEMIA.

3.2.3 > Validation de l'identité d'un individu

L’identité des individus sont vérifiés lors de la cérémonie des clés en présence d’un huissier.

3.2.4 > Informations non vérifiées

Sans objet.

3.2.5 > Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l’identité lors de la KC.

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

Les bi-clés et les certificats d’AC fille sont renouvelés a minima trois ans avant l’expiration du certificat de l’AC Fille. Le renouvellement est réalisé dans le cadre d’une cérémonie des clés.

3.4 > Identification et validation d’une demande de révocation

Les AC filles et l’AC Racine étant la propriété d’IDEMIA, le processus de révocation est interne à IDEMIA.

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 décidée par le responsable des AC IDEMIA.

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

Le processus est un processus interne à IDEMIA. Il s’appuie sur l’élaboration d ‘une cérémonie des clés.

4.2 > Traitement d'une demande de certificat

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

Le processus est un processus interne à IDEMIA. Il s’appuie sur l’élaboration d ‘une cérémonie des clés.

4.2.2 > Acceptation ou rejet de la demande

Le processus est un processus interne à IDEMIA. Il s’appuie sur l’élaboration d ‘une cérémonie des clés.

4.2.3 > Durée d'établissement du certificat

Il n’y a pas de durée maximum d’établissement du Certificat.

4.3 > Délivrance du certificat

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

L’ensemble des actions concernant la délivrance du certificat sont décrites dans le script de cérémonie des clés.

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

Le demandeur étant présent à la cérémonie des clés au travers de représentant d'IDEMIA, il est notifié implicitement de la délivrance du certificat.

4.4 > Acceptation du certificat

4.4.1 > Démarche d'acceptation du certificat

Les Certificats sont considérés acceptés en l'absence d'objection dans un délai de 48h après sa mise à disposition ou à la première utilisation de la clé privée associée. LE certificat fait l'objet d'une relecture durant la cérémonie des clés.

4.4.2 > Publication du certificat

Les certificats émis sont publiés sur le site de publication d'IDEMIA avant tout mise en production de l'AC fille.

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 les AC filles

Les AC filles 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.

L'usage est strictement limité à :

- L'émission de certificats finaux ;
- La signature de CRL le cas échéant ;
- L'émission de certificat de répondeur OCSP, le cas échéant.

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

La demande et la délivrance d’un nouveau certificat suite à changement de la bi-clé suit la procédure du paragraphe 3.3 > Identification et validation d'une demande de renouvellement des clés.

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 :

- A la demande du responsable d’AC IDEMIA ;
- De compromission ou de soupçon de compromission de la clé privée d’une AC Fille ;

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 certificat peut être révoqué par :

- Le responsable légal d’IDEMIA
- Le responsable des AC IDEMIA

4.9.3 > Procédure de traitement d'une demande de révocation

La révocation d’une AC Fille étant une opération critique, l’opération ne pourra être réalisée sans vérification de l’origine de la demande et de sa recevabilité.

4.9.4 > Délai accordé pour formuler la demande de révocation

Dès que l’AC a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, elle doit formuler sa demande de révocation sans délai.

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

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).

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 LAR

Les LAR sont établies tous les 6 mois.

4.9.8 > Délai maximum de publication d'une LCR

Les LAR sont publiées sans délais après leur émission.

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

Sans objet.

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 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.).

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 a un niveau de disponibilité de 99.5% mensuel.

4.10.2 > Fin de la relation entre l’AC Racine et l'AC Fille

Sans objet.

4.11 > Séquestre de clé et recouvrement

Sans objet.

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

5 / Mesures de sécurité non techniques

Se référer au document ‘*IGC_IDEMIA_ Mesures_sécurité*’

L’AC Racine est opérée hors-ligne.

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

Non applicable. Les clés des certificats sont directement générées sur les ressources cryptographiques (HSM) des porteurs opérés par IDEMIA.

6.1.2 > Transmission de la clé publique à l’AC Racine

Les modes de transmission de la clé publique des porteurs sont définis dans la cérémonie des clés.

6.1.3 > Taille des clés

Les tailles de clés sont de 4096 bits.

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 lors de la préparation de la cérémonie des clés.

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

La clé privée est protégée dans un dispositif HSM opéré par IDEMIA

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 Qualifiée	10 ans	10 ans
AC non qualifiée	30 ans	30 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 Root CA’

Attribut	Valeur
Version	3 (0x2)
Serial Number	11206C5C520623FFC50EDB6E69126BA57AE2
Signature Algorithm	sha512WithRSAEncryption
Issuer	CN=IDEMIA eIDAS Root CA, OI=NTRFR-440305282, O=Idemia Identity & Security France, C=FR
Not Before	Jun 30 00:00:00 2020 GMT
Not After	Jun 30 00:00:00 2050 GMT
Subject	CN=IDEMIA eIDAS Root CA, OI=NTRFR-440305282, O=Idemia Identity & Security France, C=FR
Public Key Algorithm	rsaEncryption
Key length	4096 bit

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

7.1.2 > Certificat d’AC Fille

Attribut	Valeur
Version	3 (0x2)
Serial Number	Défini lors de la cérémonie des clés
Signature Algorithm	sha512WithRSAEncryption
Issuer	CN=IDEMIA eIDAS Root CA, OI=NTRFR-440305282, O=Idemia Identity & Security France, C=FR
Not Before	MM DD HH:MM:SS YYYY GMT
Not After	MM DD HH:MM:SS YYYY GMT (+ X ans)
Subject	CN=IDEMIA eIDAS <Level> CA, OI=NTRFR-440305282, O=Idemia Identity & Security France, C=FR
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

7.2 > 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 Root CA
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 1 an
Authority Key Identifier	inclus
Numéro de série	Généré automatiquement par l'AC

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

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 Root 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
- 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.

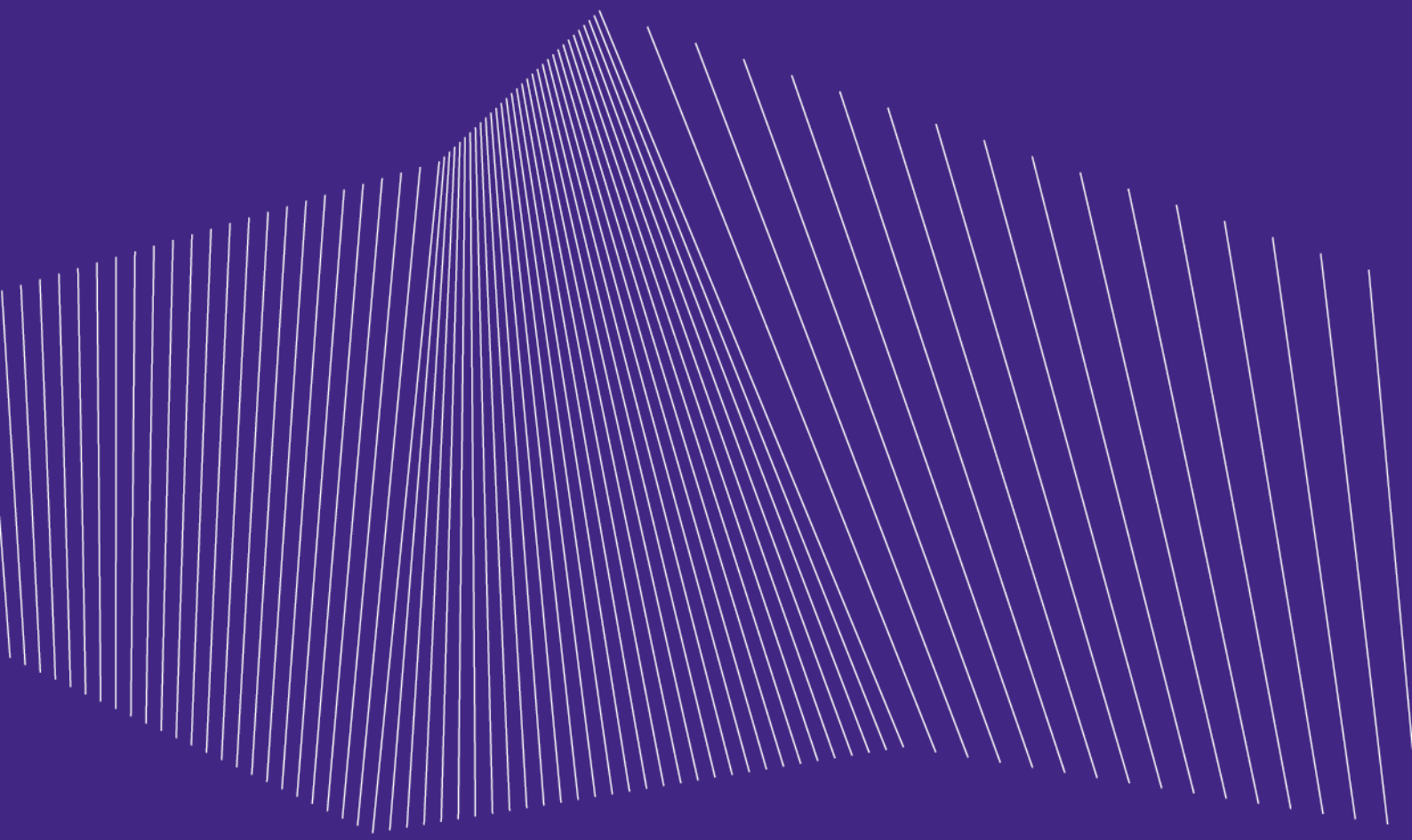
9.8 > Conformité aux législations et réglementations

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