Mesures de sécurité techniques et non techniques

V1.2 – Janvier 2022

IDEMIA

Sommaire

Introduction

IDEMIA, en tant que prestataire de services de confiance qualifié et non qualifié au sens du Règlement no 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive no 1999/93/CE (dit « Règlement eIDAS »), doit, entre autres obligations :

- Assurer la protection et la licéité des traitements de données à caractère personnel
- Gérer les risques liés à son activité
- Notifier l'organe de contrôle des incidents de sécurité et des changements dans sa fourniture de services
- Assurer le niveau d'expertise, de fiabilité, d'expérience et de qualification des personnels et sous-traitants
- Maintenir des ressources financières suffisantes
- Utiliser des produits et systèmes fiables pour le traitement et le stockage des données
- Assurer la sécurité et la fiabilité de ses processus
- Mettre en place des mesures contre la falsification et le vol des données

Le présent document décrit les mesures de sécurité communes à tous les services de confiance d'IDEMIA permettant de respecter ces exigences. Le cas échéant, des précisions spécifiques à chaque service sont fournies dans les politiques associées.

Remarque : de manière à respecter la numérotation usuelle des chapitres des politiques de certification (PC) auxquels ils font référence, les chapitres suivants sont respectivement numérotés 5 (cinq) et 6 (six).

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 à partir du 1 janvier 2022.
L'accord d'autorisation entre IDEMIA et Docaposte Trust & Sign engage Docaposte Trust & Sign à opérer les services selon le cadre déjà audité

L'historique de ce document est le suivant :

Numéro de version	Auteur	Commentaire
V1.0	PRO	Version initiale du document.
V1.1	PRO	Synchronisation avec les PC
V1.2	JMD	Transfert vers DOCAPOSTE

5 / Mesures de sécurité non techniques

Des analyses de risques sont réalisées pour déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble des services, ainsi que les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.

5.1 > Mesures de sécurité physique

5.1.1 > Accès physique

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

L'accès aux machines (serveurs, boîtiers cryptographiques, poste d'administration de l'AC, éléments actifs du réseau) est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines (contrôle d'accès par biométrie, droits associés)

5.1.2 > Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles permettent également de respecter les exigences des PC et les engagements de l'AC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.3 > Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement de l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 > Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement de l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 > Conservation des supports

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

5.1.6 > Mise hors service des supports

Les supports papiers et magnétiques en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité. Les dossiers d'enregistrement devront être conservés au moins pendant la durée de validité du certificat d'entité (en cas de renouvellement, la durée sera prolongée)

5.1.7 > Sauvegardes hors site

Les sauvegardes sont stockées sur les différents sites de production de l'hébergeur de l'IGC : en local sur le site primaire et à distance via des mécanismes de synchronisation automatique.

5.2 > Mesures de sécurité procédurales

5.2.1 > Rôles de confiance

Les rôles fonctionnels de confiance sont :

- **Le Responsable de la sécurité des systèmes d'information** d'IDEMIA : il est en charge de l'application de la politique de certification de l'autorité racine.
    - Il ne peut être un opérateur porteur de secret
    - Il peut être un administrateur porteur de secret.
- **Autorités d'enregistrement** : En charge de la validation des demandes de certificat et de révocation. Ces personnes sont nommées par le responsable de l'IGC d'IDEMIA.
- **Responsable de sécurité physique** : Il est chargé les contrôles d'accès physiques aux équipements des systèmes de la composante. Ce responsable est nommé par le partenaire hébergeur d'IDEMIA.
- **Opérateurs techniques de l'IGC** : ils sont chargés de l'utilisation, de la configuration et de la maintenance technique des équipements, boîtier cryptographique et serveur. En particulier, ils développent techniquement le déroulement de la cérémonie de clé.
- **Contrôleur** : Personne désignée par une autorité compétente (conforme par exemple à l'Instruction relative à la procédure d'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance) et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante. Le contrôleur est nommé par l'organisation du client d'IDEMIA et validée par le management d'IDEMIA.
- **Porteur de parts de secrets :** Les opérations concernant l'Autorité Racine (signature d'Autorité de Certification opérationnelle, signature de la LAR…) sont protégées par des secrets découpés en parts remis à des porteurs lors d'une cérémonie des clés en présence d'un huissier. Chaque porteur de parts de secrets de l'IGC se sont engagés à assurer la confidentialité, l'intégrité et la disponibilité des parts qui leurs ont été confiés. Il est de sa responsabilité que de transmettre ces secrets dans les mêmes conditions de sécurité en cas de départ de ce rôle (changement de fonction, départ de la société…).

5.2.2 > Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

5.2.3 > Identification et authentification pour chaque rôle

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

5.2.4 > Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les attributions associées à chaque rôle sont décrites dans les documents internes des services de confiance et sont conformes à la politique de sécurité de la composante concernée.
Concernant les rôles de confiance, les cumuls suivants sont interdits :

- Responsable de sécurité et ingénieur système / opérateur ;
- Contrôleur et tout autre rôle ;
- Ingénieur système et opérateur.

Pour des raisons de sécurité, les fonctions sensibles seront réparties sur plusieurs personnes, notamment pour les opérations liées aux modules cryptographiques rattachés aux services de confiance.

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

5.3.1 > Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes des services de confiance sont soumis à une clause de confidentialité vis-à-vis de leur employeur.
Chaque entité opérant une composante des services de confiance s'assure que les attributions de ses personnels, amenées à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

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

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

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

La documentation adéquate concerne :

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

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de la société.

5.3.2 > Procédures de vérification des antécédents

Les personnels employés dans les services de confiance sont identifiés et ne doivent pas avoir de condamnation en contradiction avec leurs attributions. Des vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement pour vérifier les antécédents et éviter tout conflit d'intérêts préjudiciable à l'impartialité des tâches.

5.3.3 > Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

5.3.4 > Exigences et fréquence en matière de formation continue

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

5.3.5 > Fréquence et séquence de rotation entre différentes attributions

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

5.3.6 > Sanctions en cas d'actions non autorisées

La direction d'IDEMIA décide des sanctions à appliquer lorsqu'un agent abuse de ses droits ou effectue une opération non conforme à ses attributions.

5.3.7 > Exigences vis-à-vis du personnel des prestataires externes

Les personnels contractants doivent respecter les mêmes conditions que celles énoncées dans la présente section.

5.3.8 > Documentation fournie au personnel

Les documents dont doit disposer le personnel sont les suivants :

- Déclaration des pratiques propre au service de confiance ;
- Documents constructeurs des matériels et logiciels utilisés ;
- Politiques du ou des services de confiance auxquels contribue la composante à laquelle il appartient ;
- Procédures internes de fonctionnement.

5.4 > Procédures de constitution des données d'audit

La journalisation d'événements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.
La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés.

Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité ainsi que de s'assurer que la séparation des fonctions est effective. Ce système permet également de collecter des preuves et de détecter des anomalies. La journalisation des événements est protégée, sauvegardée et fait l'objet de règles strictes d'exploitation.

5.4.1 > Type d'événements à enregistrer

Les systèmes journalisent les événements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre des services de confiance :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.)
- Démarrage et arrêt des systèmes informatiques et des applications
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes
- D'autres événements doivent pouvoir aussi être recueillis par le Responsable de sécurité, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :
  - Les accès physiques
  - Les actions de maintenance et de changements de la configuration des systèmes
  - Les changements apportés au personnel
  - Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs, ...)
  - En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions des services de confiance, des événements spécifiques aux différentes fonctions des services de confiance doivent également être journalisés, notamment :
  - Réception d'une demande de certificat (initiale et renouvellement)
  - Validation / rejet d'une demande de certificat
  - Événements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...)
  - Génération des certificats des porteurs
  - Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.)
  - Réception d'une demande de révocation
  - Validation / rejet d'une demande de révocation
  - Génération puis publication des CRL
  - Requêtes et réponses OCSP

Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants :

- Type de l'événement
- Nom de l'exécutant ou référence du système déclenchant l'événement

- Date et heure de l’événement
- Résultat de l’événement (échec ou réussite)

L’imputabilité d’une action revient à la personne, à l’organisme ou au système l’ayant exécutée. Le nom ou l’identifiant de l’exécutant doit figurer explicitement dans l’un des champs du journal d’événements.

5.4.2 > Fréquence de traitement des journaux d'événements

Voir 5.4.6 > ci-dessous.

5.4.3 > Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins un mois.
Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous un mois.

5.4.4 > Protection des journaux d'événements

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

5.4.5 > Procédure de sauvegarde des journaux d'événements

Chaque entité opérant une composante met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences réglementaires, aux engagements du service, et en fonction des résultats de l'analyse de risques du service de confiance.

5.4.6 > Évaluation des vulnérabilités

Chaque entité opérant une composante est en mesure de détecter toute tentative de violation de l’intégrité de la composante considérée.
Les journaux d’événements sont contrôlés quotidiennement afin d'identifier des anomalies liées à des tentatives en échec.
Les journaux sont analysés dans leur totalité au moins une fois par jour et dès la détection d’une anomalie et un rapprochement des journaux est effectué au moins une fois par semaine.

5.5 > Archivage des données

L'archivage est réalisé par l'AC dans le but d'assurer la continuité de service, l'auditabilité et la non-répudiation des opérations.

Les mesures nécessaires sont mises en place par l'AC afin que ces archives soient disponibles, ré-exploitables, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

L'AC décrit précisément dans ses procédures internes les points suivants :

- Types de données à archiver,
- Période de rétention des archives, dont notamment :
  - Les PC et DPC successives sont conservées pendant toute la durée du service de l'AC.
  - Toutes les traces des événements liés au cycle de vie des clés gérées par l'AC sont conservées au minimum 7 ans après l'expiration des clés (notamment, les P.-V. des cérémonies de clés).
  - Les certificats, récépissés, notifications, dossiers d'enregistrement et justificatifs d'identité sont conservés au minimum 7 ans après l'expiration des clés.
  - Les LCR et les réponses OCSP sont conservées 7 ans.
- Protection des archives,
- Duplication des archives,
- Horodatage des enregistrements,
- Collecte des archives (interne ou externe),
- Récupération et vérification des archives.

5.6 > Changement de clé d'AC

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

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant à la sienne. Pour cela, la période de validité de son certificat est supérieure à celle des certificats qu'elle signe.

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

5.7 > Reprise suite à compromission et sinistre

5.7.1 > Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents. Les équipes d'exploitation mettent en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. L'AC prévient également directement et sans délai l'organe de contrôle (ANSSI), et la CNIL, en cas d'événement concernant des données personnelles.

5.7.2 > Procédures de reprise en cas de sinistre

Chaque composante dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions.

La sauvegarde des composants l'IGC permet d'assurer une reprise d'activité en cas de sinistre sous 24 heures.
Ces plans sont testés au minimum une fois par an.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante (cf. § 5.7.2 > Procédures de reprise en cas de sinistre).
Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué.

5.7.4 > Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences du présent document (cf. § 5.7.2 > Procédures de reprise en cas de sinistre).

5.8 > Fin de vie de l'IGC

5.8.1 > Cessation ou transfert d'activité

La société IDEMIA peut être amenée à changer d'activité, à l'arrêter ou à la transférer à une autre entité. Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

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

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

- Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats) ;
- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour les fonctions définies dans ses politiques de service.
- Communiquer avant une date donnée son intention de transfert d'activité ;
- Mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires (utilisateurs finaux, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité ;
- Doit précises dans sa DPC qui elle doit prévenir, comment se déroule le transfert des obligations (archives et logs à une autre entité), et comment seront traités les certificats encore valides qui seraient amenés à être révoqués.

5.8.2 > Cessation d'activité affectant les services de confiance

→ Cessation d'activité concernant l'AC

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

- S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ; En particulier :
  - Destruction de la clé sur l'ensemble des HSM
  - Destruction de l'ensemble des sauvegardes de la clé
  - Chaque fois que cela est possible, destruction des moyens de restauration des sauvegardes.
- Révoquer les certificats valides qu'elle a signé (uniquement pour une fin de vie due à une compromission ou suspicion de compromission de clé, une perte ou un vol) ;
- Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Révoquer son certificat ;
- Informer (par exemple par récépissé) tous ses clients et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant ;
- Doit s'assurer qu'aucun contractant ne peut agir pour son compte dans le processus de génération de certificat ;
- S'assure que les clés privées de l'AC doivent être détruites ou ne doivent plus être utilisées ;
- Communiquer publiquement au plus tôt son intention de cessation d'activité ;
- Informer l'organisme de contrôle (ANSSI) de cette décision.

Le serveur OCSP générera une dernière réponse OCSP pour chaque certificat émis, la fin de validité sera positionnée au 31 décembre 9999 conformément aux recommandations de l'ANSSI. La clé du répondeur OCSP sera alors détruite. Les réponses OCSP pré-générées seront mises à disposition des tiers par IDEMIA.

→ Cessation d'activité concernant l'AH

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

- S'interdire de transmettre les clés privées lui ayant permis d'émettre des contremarques de temps ;
- Prendre toutes les mesures nécessaires pour les détruire ou la rendre inopérante, en détruisant l'instance de la clé sur le HSM.
- Informer (par exemple par récépissé) tous ses clients et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant ;
- Doit s'assurer qu'aucun contractant ne peut agir pour son compte dans le processus de génération de certificat ;
- S'assure que les clés privées de l'AC doivent être détruites ou ne doivent plus être utilisées ;
- Communiquer publiquement au plus tôt son intention de cessation d'activité ;
- Informer l'organisme de contrôle (ANSSI) de cette décision.

5.8.3 > Transfert des Archives

Dans le cas d'une fin de vie d'une AE, le contrat liant l'AE à l'AC précise, le cas échéant, les modalités de transfert des archives. Celles-ci pourront :

- Soit être conservées pour la durée légale par l'organisme opérant l'AE.
- Soit être transférée à l'AC par une méthode sécurisée permettant de garantir l'intégrité et la confidentialité des archives transférées.

En cas d'arrêt d'activité d'une composante de l'AC ou de l'AH ne transférant pas ses archives en central à IDEMIA, les archives de la composante seront transférées à IDEMIA.

En cas d'arrêt d'activité du service, IDEMIA se réserve au moment voulu le choix d'effectuer le transfert des archives

- Soit en interne au sein d'un autre service opérant un service d'archivage
- Soit via un tiers archiveur

5.8.4 > Cas du transfert d'Activité

Dans le cas du transfert d'activité, la société reprenant l'activité de l'AC devra reprendre les archives, soit en gestion directe, soit par l'intermédiaire d'un prestataire.

5.8.5 > Cas de la cessation d'activité

Si l'AC arrête son activité, elle devra transférer ses archives à un prestataire agréé dans ce domaine et informer l'AC ainsi que l'organe de contrôle national (au sens du Règlement eIDAS) des coordonnées de cette société.

6 / Mesures de sécurité techniques

La présente section ne traite que des bi-clés d'AC, d'UH et d'OCSP. Pour les clés et les certificats des porteurs, se référer à la PC correspondante.

6.1 > Génération des bi-clés du porteur et installation

6.1.1 > Génération des bi-clés

Pour la procédure de génération des bi-clés des porteurs présentes sur les HSM d'IDEMIA, se référer au document 'IDEMIA_eIDAS_KeyPair_Generation'.

6.1.2 > Clé d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé.
Les clés de signature de l'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences de l'ANSSI (cf. § 6.2.1 > Standards et mesures de sécurité pour les modules cryptographiques).

La génération des clés de signature d'AC doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. § 5.2.1 > Rôles de confiance), dans le cadre de « cérémonies de clés ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins deux sont externes à l'AC et attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.3 > Clé OCSP

La génération des clés de signature des jetons OCSP est effectuée dans un environnement sécurisé, dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. § 5.2.1 > Rôles de confiance).

Ces clés sont générées et mises en œuvre dans un module cryptographique conforme aux exigences de l'ANSSI (cf. § 6.2.1 > Standards et mesures de sécurité pour les modules cryptographiques) pour le niveau qualifié. Pour le niveau non qualifié, le module cryptographique est a minima évalué conforme au niveau EAL4+ des critères communs ou fait l'objet d'une évaluation FIPS 140-2.

6.1.4 > Clé d'UH

La génération des clés de signature des UH est effectuée dans un environnement sécurisé, dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. § 5.2.1 > Rôles de confiance).

Ces clés sont générées et mises en œuvre dans un module cryptographique conforme aux exigences de l'ANSSI (cf. § 6.2.1 > Standards et mesures de sécurité pour les modules cryptographiques) pour le

niveau qualifié. Pour le niveau non qualifié, le module cryptographique est a minima évalué conforme au niveau EAL4+ des critères communs ou fait l'objet d'une évaluation FIPS 140-2.

6.1.5 > Transmission de la clé privée à son propriétaire

Sans objet pour des clés d'AC, d'UH ou d'OCSP.

6.1.6 > Transmission de la clé publique à l'AC

La transmission des clés est réalisée de façon sécurisée par des personnels en rôle de confiance.

6.1.7 > Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de l'AC sont disponibles sur le site Internet de l'AC.
Les clés publiques d'UH sont intégrées dans le jeton d'horodatage.

6.1.8 > Taille des clés

La taille de la clé de l'AC est de 4096 bits.

6.1.9 > Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR.

L'utilisation de la clé privée d'OCSP et du certificat associé est strictement limitée à la signature des jetons OCSP produits par le service de l'AC.

L'utilisation de la clé privée d'UH et du certificat associé est strictement limitée à la signature des jetons d'horodatage produits par le service de l'AH.

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

6.2.1 > Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques utilisés par l'AC pour la protection de ses clés (AC et OCSP de l'AC qualifiée) doivent respecter les exigences du § II.3.5 des Critères d'évaluation de la conformité au règlement eIDAS (version 1.1 du 3 janvier 2017 ou ultérieure, publié sur le site https://www.ssi.gouv.fr).

6.2.2 > Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par plusieurs personnes du personnel de confiance et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s’authentifier, avec n au moins égal à 2).

6.2.3 > Séquestre de la clé privée

Les clés privées d'AC et d’AH ne sont en aucun cas séquestrées.

6.2.4 > Copie de secours de la clé privée

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du § 6.2.1 >, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d’intégrité.

Les clés privées d’UH ne sont pas sauvegardées. Une seule exception est prévue pour la mise en production de l’UH suite à la cérémonie des clés. La copie est détruite dans un bref délai après la mise en production de l’UH.

6.2.5 > Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.

6.2.6 > Transfert de la clé privée vers / depuis le module cryptographique

Pour les clés privées d'AC, tout transfert est réalisé sous forme chiffrée, conformément aux exigences du § 6.2.4 > Copie de secours de la clé privée.

6.2.7 > Méthode d'activation de la clé privée

L'activation des clés privées d'AC et d’OCSP dans un module cryptographique est contrôlée via des données d'activation (cf. § 6.4 > Données d’activation) et fait intervenir au moins deux personnes dans des rôles de confiance.

6.2.8 > Méthode de désactivation de la clé privée

La désactivation des clés privées d'AC, d’UH et d’OCSP dans le module cryptographique est automatique dès que l'environnement du module évolue.

6.2.9 > Méthode de destruction des clés privées

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

6.3 > Autres aspects de la gestion des bi-clés

6.3.1 > Archivage des clés publiques

Les clés publiques de l'AC, des UH et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

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

Les bi-clés et les certificats d'AC ou d'OCSP ont la même durée de vie.
La durée de vie d'une clé d'UH est de un (1) an.

6.4 > Données d'activation

6.4.1 > Génération et installation des données d'activation

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se font lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles leur sont transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. § 5.2.1 > Rôles de confiance).

6.4.2 > Protection des données d'activation

Les données d'activation qui sont générées par l'AC ou l'AH pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.5 > Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risques que l'AC a menée.

6.5.1 > Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC/DPH de l'AC et de l'AH. Il répond aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC et l'AH, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),

- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non autorisés et mises à jour des logiciels,
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- Protection du réseau contre toute intrusion d'une personne non autorisée,
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- Fonctions d'audits (non-répudiation et nature des actions effectuées),
- Protections IDS (Intrusion Detection System) et IPS (Intrusion Prevention System) en amont des serveurs.

6.6 > Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risque menée sur les services de confiance.

6.6.1 > Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes des services de confiance est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation.

La configuration du système des composantes, ainsi que toute modification et mise à niveau, est documentée et contrôlée.

6.6.2 > Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante est signalée à IDEMIA pour validation.

6.7 > Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante.
Les composants du réseau local des services de confiance sont maintenus dans un environnement physiquement sécurisé et leurs configurations sont périodiquement auditées.

6.8 > Horodatage / Système de datation

Plusieurs fonctions de sécurité nécessitent la datation par les différentes composantes des services de confiance d'événements liés à l'activité de ces services (cf. § 5.4 > Procédures de constitution des données d'audit).
Pour dater ces événements, les différentes composantes sont synchronisées quotidiennement, au minimum, à la minute près, et par rapport à une source fiable de temps UTC.

8 / Audit de conformité et autres évaluations

8.1 > Fréquences et / ou circonstances des évaluations

Un contrôle de conformité de l'ensemble des services de confiance est réalisé tous les ans. Les audits externes de conformité aux normes ETSI ou de qualification (au sens du Règlement eIDAS) sont réalisés tous les deux ans.

8.2 > Identités / qualifications des évaluateurs

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

8.3 > Relations entre évaluateurs et entités évaluées

Les auditeurs internes ne doivent pas participer, contribuer ou être subordonnés aux composantes auditées.

8.4 > Sujets couverts par les évaluations

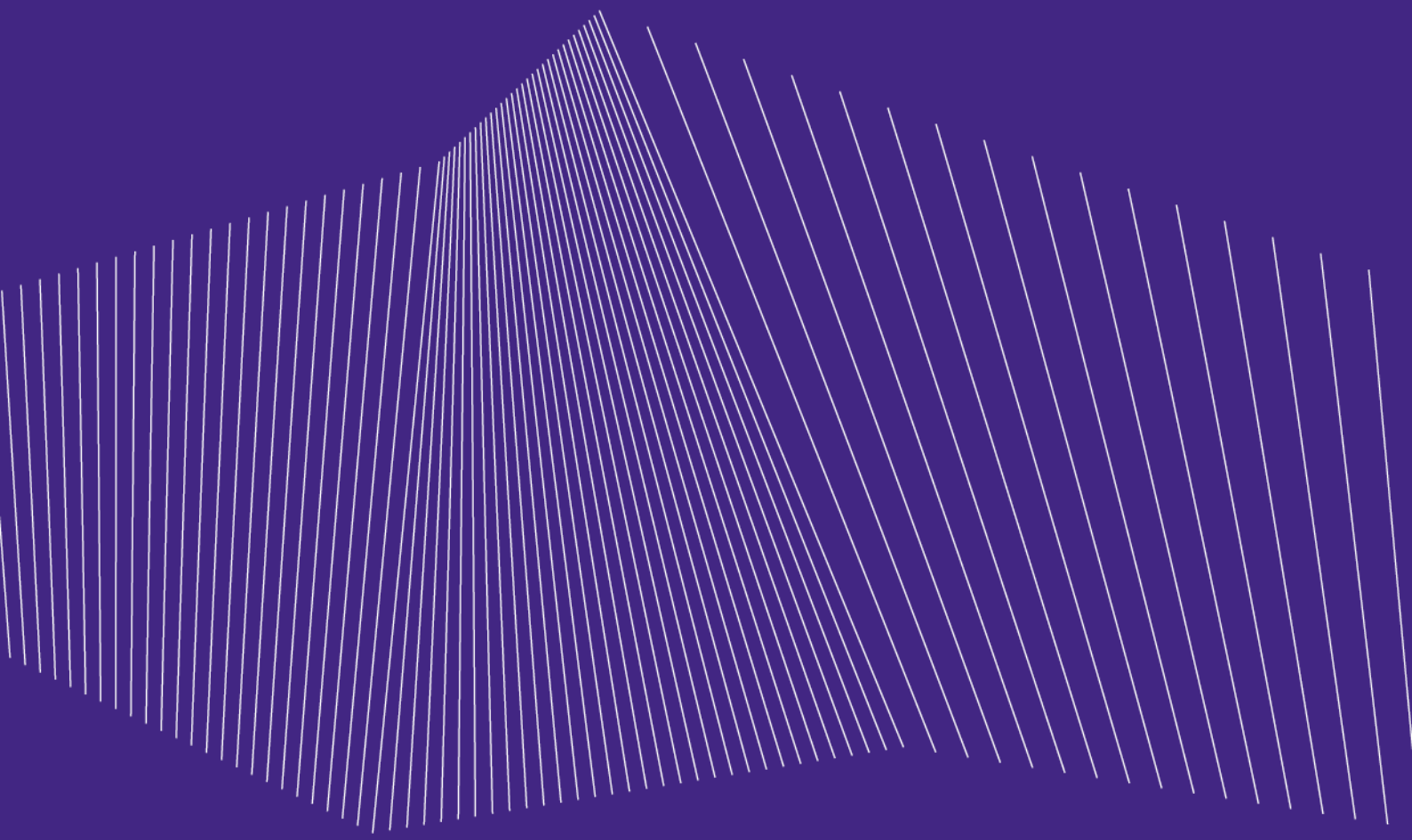
Les contrôles de conformité portent sur l'ensemble des services de confiance d'IDEMIA et visent à vérifier le respect des engagements et pratiques définies dans les politiques et pratiques des services, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 > Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'évaluateur émet auprès de la direction d'IDEMIA un rapport de conformité assorti de recommandations.
La direction d'IDEMIA délègue aux composantes concernées la résolution des points de non-conformité et valide les mesures mises en œuvre.

8.6 > Communication des résultats

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



IDEMIA

www.idemia.com