



**DOCAPOSTE**

l'avenir devient plus simple



# IGC 'Dictao Trust Services G2'

## Mesures de sécurité techniques et non techniques

Fichier	<i>dictao-trust-cp-measures.pdf</i>
Date	18/11/2022
Référence/version	V1.2
Dossier consultation N°	sans objet

## Historique

Version	Date	Objet
1.0	IDEMIA I&S	Version initiale du document.
1.1	DOCAPOSTE T&S	Transfert vers DOCAPOSTE T&S Ajout de l'AC Dictao Trust Services User 03 CA G2
1.2	DOCAPOSTE T&S	Révision pour conformité complète aux procédures Docaposte

## Acronymes

Acronyme	Définition
API	Application Programming Interface
CA	Certificate Authority
CP	Certificate Policy
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DN	Distinguished name
DTS	DOCAPOSTE Trust & Sign
IANA	Internet Assigned Numbers Authority
IGC	Infrastructure de Gestion de Clé, PKI en anglais
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PEN	Private Enterprise Number
PEM	Privacy-Enhanced Mail
QSCD	Qualified Signature and Seal Creation Device
RA	Registration authority
SIREN	Système d'identification du répertoire des entreprises
SN	Serial Number
TSU	Time-Stamping Unit
WS	Web Service

## Objet

**Le présent document décrit les mesures de sécurité communes à tous les services de confiance de l'IGC Legacy DOCAPOSTE Trust & Sign permettant de respecter ces exigences. Le cas échéant, des précisions spécifiques à chaque service sont fournies dans les politiques associées.**

# TABLE DES MATIERES

---

<b>6</b>	<b>Mesures de sécurité non techniques</b>	<b>5</b>
6.1	Mesures de sécurité physique	5
6.1.1	Accès physique	5
6.1.2	Alimentation électrique et climatisation	5
6.1.3	Vulnérabilité aux dégâts des eaux	5
6.1.4	Prévention et protection incendie	5
6.1.5	Conservation des supports	5
6.1.6	Mise hors service des supports	6
6.1.7	Sauvegardes hors site	6
6.2	Mesures de sécurité procédurales	6
6.2.1	Rôles de confiance	6
6.2.2	Nombre de personnes requises par tâches	6
6.2.3	Identification et authentification pour chaque rôle	7
6.2.4	Rôles exigeant une séparation des attributions	7
6.3	Mesures de sécurité vis-à-vis du personnel	7
6.3.1	Qualifications, compétences et habilitations requises	7
6.3.2	Procédures de vérification des antécédents	8
6.3.3	Exigences en matière de formation initiale	8
6.3.4	Exigences et fréquence en matière de formation continue	8
6.3.5	Fréquence et séquence de rotation entre différentes attributions	8
6.3.6	Sanctions en cas d'actions non autorisées	8
6.3.7	Exigences vis-à-vis du personnel des prestataires externes	8
6.3.8	Documentation fournie au personnel	8
6.4	Procédures de constitution des données d'audit	9
6.4.1	Type d'événements à enregistrer	9
6.4.2	Fréquence de traitement des journaux d'événements	10
6.4.3	Période de conservation des journaux d'événements	10
6.4.4	Protection des journaux d'événements	10
6.4.5	Procédure de sauvegarde des journaux d'événements	10
6.4.6	Évaluation des vulnérabilités	10
6.5	Archivage des données	10
6.6	Changement de clé d'AC	11
6.7	Reprise suite à compromission et sinistre	11
6.7.1	Procédures de remontée et de traitement des incidents et des compromissions	11
6.7.2	Procédures de reprise en cas de sinistre	12
6.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante	12
6.7.4	Capacités de continuité d'activité suite à un sinistre	12
6.8	Fin de vie de l'IGC	12
6.8.1	Cessation ou transfert d'activité	12

6.8.2	Cessation d'activité affectant les services de confiance .....	13
6.8.3	Transfert des Archives .....	13
6.8.4	Cas du transfert d'Activité .....	14
6.8.5	Cas de la cessation d'activité .....	14
<b>7</b>	<b>Mesures de sécurité techniques .....</b>	<b>15</b>
7.1	Génération des bi-clés du porteur et installation .....	15
7.1.1	Génération des bi-clés .....	15
7.1.2	Clé d'AC .....	15
7.1.3	Transmission de la clé privée à son propriétaire .....	15
7.1.4	Transmission de la clé publique à l'AC .....	15
7.1.5	Transmission de la clé publique de l'AC aux utilisateurs de certificats .....	15
7.1.6	Taille des clés .....	15
7.1.7	Objectifs d'usage de la clé .....	15
7.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques .....	16
7.2.1	Standards et mesures de sécurité pour les modules cryptographiques .....	16
7.2.2	Contrôle de la clé privée par plusieurs personnes .....	16
7.2.3	Séquestre de la clé privée .....	16
7.2.4	Copie de secours de la clé privée .....	16
7.2.5	Archivage de la clé privée .....	16
7.2.6	Transfert de la clé privée vers / depuis le module cryptographique .....	16
7.2.7	Méthode d'activation de la clé privée .....	16
7.2.8	Méthode de désactivation de la clé privée .....	16
7.2.9	Méthode de destruction des clés privées .....	17
7.3	Autres aspects de la gestion des bi-clés .....	17
7.3.1	Archivage des clés publiques .....	17
7.3.2	Durées de vie des bi-clés et des certificats .....	17
7.4	Données d'activation .....	17
7.4.1	Génération et installation des données d'activation .....	17
7.4.2	Protection des données d'activation .....	17
7.5	Mesures de sécurité des systèmes informatiques .....	17
7.5.1	Exigences de sécurité technique spécifiques aux systèmes informatiques .....	17
7.6	Mesures de sécurité des systèmes durant leur cycle de vie .....	18
7.6.1	Mesures de sécurité liées au développement des systèmes .....	18
7.6.2	Mesures liées à la gestion de la sécurité .....	18
7.7	Mesures de sécurité réseau .....	18
7.8	Horodatage / Système de datation .....	18
<b>8</b>	<b>Audit de conformité et autres évaluations .....</b>	<b>20</b>
8.1	Fréquences et / ou circonstances des évaluations .....	20
8.2	Communication des résultats .....	20

---

# Introduction

DOCAPOSTE TRUST & SIGN, en tant que prestataire de services de confiance doit, entre autres obligations :

- Assurer la protection et la licéité des traitements de données à caractère personnel
- Gérer les risques liés à son activité
- 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 de DOCAPOSTE Trust & Sign permettant de respecter ces exigences. Il englobe ainsi politiques de certification (PC) et politique d'horodatage (PH). 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) et politique d'horodatage (PH) auxquels ils font référence, les chapitres suivants sont respectivement numérotés 6(six), 7(sept) et 9(neuf).

## 6 MESURES DE SECURITE 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.

### 6.1 Mesures de sécurité physique

#### 6.1.1 Accès physique

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est 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)

#### 6.1.2 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 et engagements des services de confiance en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

#### 6.1.3 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement des présents services de confiance, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

#### 6.1.4 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement des présents services de confiance, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

#### 6.1.5 Conservation des supports

Les supports (papier, disque dur, 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.

## 6.1.6 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 sont être conservés au moins 6 mois après la durée de validité du certificat d'entité (en cas de renouvellement, la durée sera prolongée)

## 6.1.7 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.

# 6.2 Mesures de sécurité procédurales

## 6.2.1 Rôles de confiance

Les rôles fonctionnels de confiance sont :

- **Le Responsable de la sécurité des systèmes d'information** de DOCAPOSTE Trust & Sign : 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 de DOCAPOSTE Trust & Sign.
- **Responsable de sécurité physique** : Il est chargé des contrôles d'accès physiques aux équipements des systèmes de la composante. Ce responsable est nommé par le partenaire hébergeur de DOCAPOSTE Trust & Sign.
- **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 réalisent le script de déroulement de la cérémonie de clé.
- **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. L'AC s'assure du transfert de ces secrets dans les mêmes conditions de sécurité en cas de départ de ce rôle (changement de fonction, départ de la société...).
- **Auditeur système** : L'auditeur système est en charge de faire l'analyse des traces et des événements présents dans les logs du système.

## 6.2.2 Nombre de personnes requises par tâches

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

## 6.2.3 Identification et authentification pour chaque rôle

La Direction de DOCAPOSTE Trust & Sign fait vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants.

## 6.2.4 Rôles exigeant une séparation des attributions

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 la sécurité des systèmes d'information et porteur de secret opérateur ;
- Responsable de sécurité et ingénieur système / opérateur ;
- Auditeur système et tout autre rôle ;
- Ingénieur système et opérateur.

## 6.3 Mesures de sécurité vis-à-vis du personnel

### 6.3.1 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.

### 6.3.2 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.

### 6.3.3 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.

### 6.3.4 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.

### 6.3.5 Fréquence et séquence de rotation entre différentes attributions

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

### 6.3.6 Sanctions en cas d'actions non autorisées

La direction de DOCAPOSTE Trust & Sign décide des sanctions à appliquer lorsqu'un agent abuse de ses droits ou effectue une opération non conforme à ses attributions.

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

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

### 6.3.8 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.

## 6.4 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.

### 6.4.1 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 ou d'AH (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...)
    - Génération des certificats des porteurs
    - Publication et mise à jour des informations liées aux services de confiance (PC, PH, certificats d'AC ou d'AH, conditions générales d'utilisation, etc.)
    - Réception d'une demande de révocation
    - Validation / rejet d'une demande de révocation

- Génération puis publication des CRL
- Evènements liés à la synchronisation du temps pour l'AH

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.

## 6.4.2 Fréquence de traitement des journaux d'événements

Voir 6.4.6 ci-dessous.

## 6.4.3 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.

## 6.4.4 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.

## 6.4.5 Procédure de sauvegarde des journaux d'événements

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

## 6.4.6 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 automatiquement afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dès la détection d'une anomalie.

## 6.5 Archivage des données

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

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

Les services de confiance décrivent précisément dans leurs procédures internes les points suivants :

- Types de données à archiver,
- Période de rétention des archives, dont notamment :
  - Les PC, DPC, PH et DPH successives sont conservées pendant toute la durée du service des services de confiance.
  - Toutes les traces des événements liés au cycle de vie des clés gérées par l'AC et aux traces gérées par l'AH sont conservées au minimum 1 an après l'expiration des clés.
  - Les certificats, récépissés, notifications sont conservés au minimum 1 an après l'expiration des clés.
- Protection des archives,
- Duplication des archives,
- Collecte des archives (interne ou externe),
- Récupération et vérification des archives.

## 6.6 Changement de clé d'AC

L'AC change sa bi-clé lorsqu'elle n'est plus conforme au niveau de sécurité nécessaire pour assurer le service.

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.

## 6.7 Reprise suite à compromission et sinistre

### 6.7.1 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.

## 6.7.2 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.

## 6.7.3 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. § 6.7.2 Procédures de reprise en cas de sinistre).

Dans le cas de compromission d'une clé d'AC ou d'AH, le certificat correspondant doit être immédiatement révoqué.

## 6.7.4 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. § 6.7.2 Procédures de reprise en cas de sinistre).

# 6.8 Fin de vie de l'IGC

## 6.8.1 Cessation ou transfert d'activité

La société DOCAPOSTE TRUST & SIGN 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 les services de confiance 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, les services de confiances doivent 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 l'intention de transfert d'activité ;
- Mettre en œuvre tous les moyens dont ils disposent pour informer les partenaires (utilisateurs finaux, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité ;
- Doit préciser dans sa DPC et DPH qui elle doit prévenir, comment se déroule le transfert des obligations (archives et logs à une autre entité), et comment seront traités les certificats encore valides qui seraient amenés à être révoqués.

## 6.8.2 Cessation d'activité affectant les services de confiance

- Lors de l'arrêt du service, les services de confiance doivent :
- S'interdire de transmettre les clés privées ayant permis d'émettre des certificats ;
- Prendre toutes les mesures nécessaires pour les détruire ou les rendre inopérantes ; En particulier :
- Destruction des clés sur l'ensemble des HSM
- Destruction de l'ensemble des sauvegardes des clés
- Chaque fois que cela est possible, destruction des moyens de restauration des sauvegardes.
- Révoquer les certificats valides qu'ils ont signés (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'ils ont signés et qui seraient encore en cours de validité ;
- Révoquer ses certificats ;
- 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'assurer que les clés privées des services de confiance doivent être détruites ou ne doivent plus être utilisées ;
- Communiquer publiquement au plus tôt leur intention de cessation d'activité.

## 6.8.3 Transfert des Archives

Dans le cas d'une fin de vie d'une AE, le contrat liant l'AE aux services de confiance 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 aux services de confiance par une méthode sécurisée permettant de garantir l'intégrité et la confidentialité des archives transférées.

En cas d'arrêt d'activité du service, DOCAPOSTE TRUST & SIGN 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

## 6.8.4 Cas du transfert d'Activité

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

## 6.8.5 Cas de la cessation d'activité

Si les services de confiance arrêtent leur activité, ils doivent transférer leurs archives à un prestataire agréé dans ce domaine et informer leurs clients des coordonnées de cette société.

## 7 MESURES DE SECURITE TECHNIQUES

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

### 7.1 Génération des bi-clés du porteur et installation

#### 7.1.1 Génération des bi-clés d'AC et d'AH

La procédure de génération des bi-clés d'AC et d'AH fait l'objet d'une cérémonie des clés.

#### 7.1.2 Clé d'AC

La génération des clés de signature d'AC et d'AH est effectuée dans un environnement sécurisé.

La génération des clés de signature d'AC et d'AH est effectuée 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 de personnes ayant des rôles de confiance et en présence de témoins qui attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

#### 7.1.3 Transmission de la clé privée à son propriétaire

Sans objet pour des clés d'AC.

#### 7.1.4 Transmission de la clé publique à l'AC ou l'AH

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

#### 7.1.5 Transmission de la clé publique de l'AC ou l'AH aux utilisateurs de certificats

Les clés publiques de l'AC et de l'AH sont disponibles sur le site Internet des services de confiance.

#### 7.1.6 Taille des clés

La taille de la clé de l'AC et de l'AH est de 4096 ou 2048 bits.

#### 7.1.7 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.

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

### 7.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Non applicable.

### 7.2.2 Contrôle de la clé privée par plusieurs personnes

Non applicable.

### 7.2.3 Séquestre de la clé privée

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

### 7.2.4 Copie de secours de la clé privée

Les clés privées d'AC et d'AH font l'objet de copies de secours sous forme chiffrée avec un mécanisme de contrôle d'intégrité.

### 7.2.5 Archivage de la clé privée

Non applicable.

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

Pour les clés privées d'AC ou d'AH, tout transfert est réalisé sous forme chiffrée, conformément aux exigences du § 7.2.4 Copie de secours de la clé privée.

### 7.2.7 Méthode d'activation de la clé privée

L'activation des clés privées d'AC et d'AH est contrôlée via des données d'activation (cf. § 7.4 Données d'activation).

### 7.2.8 Méthode de désactivation de la clé privée

Non applicable.

## 7.2.9 Méthode de destruction des clés privées

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

## 7.3 Autres aspects de la gestion des bi-clés

### 7.3.1 Archivage des clés publiques

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

### 7.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats d'AC et d'AH ont la même durée de vie.

## 7.4 Données d'activation

### 7.4.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation de l'IGC se font lors de la phase d'initialisation.

### 7.4.2 Protection des données d'activation

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

## 7.5 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 menée pour les services de confiance.

### 7.5.1 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 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 les services de confiance, 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.

## 7.6 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.

### 7.6.1 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.

### 7.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante est signalée à DOCAPOSTE TRUST & SIGN pour validation.

## 7.7 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.

## 7.8 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. § 6.4 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.

## 9 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

### 9.1 Fréquences et / ou circonstances des évaluations

Aucun audit de conformité spécifique aux services de confiance de l'IGC n'est réalisé.

L'infrastructure utilisée, et les règles opérationnelles sont audités dans le cadre d'une évaluation ISO 27001 et conforme à la [PSSI].

.

### 9.2 Communication des résultats

Les résultats des audits de conformité ISO 27001 de l'infrastructure sont confidentiels et ne peuvent être communiqués qu'à des tiers en cas de demande explicite.