



	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE – MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS DE CEGEDIM

PUBLIC

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

ADMINISTRATION DU DOCUMENT


▪ APPROBATION - VALIDATION

	AUTEUR	APPROBATEUR
PRENOM – NOM	STEPHANE GALMICHE	HONG GIRAULT
FONCTION	DIRECTEUR DE PROJETS	DIRECTEUR D'ACTIVITE
DATE	02/06/2023	15/06/2023

▪ HISTORIQUE DES VERSIONS

VERSION	DATE	AUTEUR	DESCRIPTIF DES MODIFICATIONS
1.4	02/06/2023	STEPHANE GALMICHE	PRECISION SUR LA PUBLICATION EN CAS DE FIN DE VIE
1.3	17/05/2023	STEPHANE GALMICHE	EXTENSION AU SERVICE D'HORODATAGE
1.2	04/06/2021	STEPHANE GALMICHE	SITE DE PUBLICATION EN HTTPS
1.1	05/05/2021	STEPHANE GALMICHE	EMPREINTES DES DOCUMENTS PUBLIES EN SHA-1
1.0	15/04/2021	STEPHANE GALMICHE	VERSION INITIALE


PUBLIC

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		


SOMMAIRE

1	INTRODUCTION.....	6
1.1	OBJET DU DOCUMENT	6
1.2	DEFINITIONS ET ACRONYMES	6
1.2.1	<i>Définitions</i>	6
1.2.2	<i>Acronymes</i>	9
2	RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	10
2.1	ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS	10
2.2	DESCRIPTION DES INFORMATIONS PUBLIEES	10
2.3	DELAIS ET FREQUENCES DE PUBLICATION	10
2.4	CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES	10
3	IDENTIFICATION ET AUTHENTIFICATION DES PORTEURS DE CERTIFICATS	11
4	EXIGENCES OPERATIONNELLES	12
5	MESURES DE SECURITE NON TECHNIQUES	13
5.1	MESURES DE SECURITE PHYSIQUE.....	13
5.1.1	<i>Situation géographique et construction des sites</i>	13
5.1.2	<i>Accès physique</i>	13
5.1.3	<i>Alimentation électrique et climatisation</i>	13
5.1.4	<i>Vulnérabilité aux dégâts des eaux</i>	13
5.1.5	<i>Prévention et protection incendie</i>	13
5.1.6	<i>Conservation des supports</i>	13
5.1.7	<i>Mise hors service des supports</i>	13
5.1.8	<i>Sauvegardes hors site</i>	13
5.2	MESURES DE SECURITE PROCEDURALES.....	14
5.2.1	<i>Rôles de confiance</i>	14
5.2.2	<i>Nombre de personnes requises par tâche</i>	14
5.2.3	<i>Identification et authentification pour chaque rôle</i>	14
5.2.4	<i>Rôles exigeant une séparation des attributions</i>	14
5.3	MESURES DE SECURITE VIS-A-VIS DU PERSONNEL.....	15
5.3.1	<i>Qualifications, compétences et habilitations requises</i>	15
5.3.2	<i>Procédures de vérification des antécédents</i>	15
5.3.3	<i>Exigences en matière de formation initiale</i>	15
5.3.4	<i>Exigences et fréquence en matière de formation continue</i>	15
5.3.5	<i>Fréquence et séquence de rotation entre différentes attributions</i>	15
5.3.6	<i>Sanctions en cas d'actions non autorisées</i>	15
5.3.7	<i>Exigences vis-à-vis du personnel des prestataires externes</i>	16
5.3.8	<i>Documentation fournie au personnel</i>	16
5.4	PROCEDURE DE CONSTITUTION DES DONNEES D'AUDIT	16
5.4.1	<i>Type d'évènements à enregistrer</i>	16
5.4.2	<i>Fréquence de traitement des journaux d'évènements</i>	17
5.4.3	<i>Période de conservation des journaux d'évènements</i>	17
5.4.4	<i>Protection des journaux d'évènements</i>	17
5.4.5	<i>Procédure de sauvegarde des journaux d'évènements</i>	17
5.4.6	<i>Système de collecte des journaux d'évènements</i>	17
5.4.7	<i>Notification de l'enregistrement d'un évènement au responsable de l'évènement</i>	17
5.4.8	<i>Évaluation des vulnérabilités</i>	17
5.5	ARCHIVAGE DES DONNEES	18
5.5.1	<i>Types de données à archiver</i>	18
5.5.2	<i>Période de conservation des archives</i>	18
5.5.3	<i>Protection des archives</i>	18


PUBLIC

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

5.5.4	<i>Procédure de sauvegarde des archives</i>	18
5.5.5	<i>Exigences d'horodatage des données</i>	18
5.5.6	<i>Système de collecte des archives</i>	18
5.5.7	<i>Procédures de récupération et de vérification des archives</i>	18
5.6	REPRISE SUITE A LA COMPROMISSION ET SINISTRE	19
5.6.1	<i>Procédures de remontée et de traitement des incidents et des compromissions</i>	19
5.6.2	<i>Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données)</i> 19	
5.6.3	<i>Procédures de reprise en cas de compromission de la clé privée d'une composante</i>	19
5.6.4	<i>Capacités de continuité d'activité suite à un sinistre</i>	19
5.7	FIN DE VIE	19
5.8	GESTION DES RISQUES	20
5.8.1	<i>Analyse de risques</i>	20
5.8.2	<i>Homologation</i>	21
5.8.3	<i>Politique de sécurité du système d'information</i>	21
6	MESURES DE SECURITE TECHNIQUES	22
6.1	MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES DISPOSITIFS CRYPTOGRAPHIQUES	22
6.1.1	<i>Standards et mesures de sécurité pour les dispositifs cryptographiques</i>	22
6.1.2	<i>Contrôle de la clé privée</i>	22
6.1.3	<i>Séquestre de la clé privée</i>	22
6.1.4	<i>Copie de secours d'une clé privée d'AC</i>	22
6.1.5	<i>Archivage d'une clé privée</i>	22
6.1.6	<i>Transfert d'une clé privée vers et depuis le dispositif cryptographique</i>	22
6.1.7	<i>Stockage de la clé privée dans un dispositif cryptographique</i>	23
6.1.8	<i>Méthode d'activation de la clé privée</i>	23
6.1.9	<i>Méthode de désactivation de la clé privée</i>	23
6.1.10	<i>Méthode de destruction d'une clé privée</i>	23
6.1.11	<i>Niveau de qualification des dispositifs cryptographiques</i>	23
6.2	AUTRES ASPECTS DE LA GESTION DES BI-CLES	23
6.2.1	<i>Archivage des clés publiques</i>	23
6.2.2	<i>Durées de vie des bi-clés et des certificats</i>	23
6.3	DONNEES D'ACTIVATION DES CLES PRIVEES DES AC	24
6.3.1	<i>Génération et installation des données d'activation</i>	24
6.3.2	<i>Protection des données d'activation</i>	24
6.3.3	<i>Autres aspects liés aux données d'activation</i>	24
6.4	MESURES DE SECURITE DES SYSTEMES INFORMATIQUES	24
6.4.1	<i>Exigences de sécurité technique spécifiques aux systèmes informatiques</i>	24
6.4.2	<i>Niveau de qualification des systèmes informatiques</i>	24
6.5	MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES	24
6.5.1	<i>Mesures de sécurité liées au développement des systèmes</i>	24
6.5.2	<i>Mesures liées à la gestion de la sécurité</i>	25
6.5.3	<i>Niveau d'évaluation sécurité du cycle de vie des systèmes</i>	25
6.6	MESURES DE SECURITE RESEAU	25
6.7	HORODATAGE / SYSTEME DE DATATION	25
7	PROFILS	26
8	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	27
8.1	FREQUENCES ET CIRCONSTANCES DES EVALUATIONS	27
8.2	IDENTITES ET QUALIFICATIONS DES EVALUATEURS	27
8.3	RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES	27
8.4	SUJETS COUVERTS PAR LES EVALUATIONS	27
8.5	ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS	27
8.6	COMMUNICATION DES RESULTATS	27
9	AUTRES PROBLEMATIQUES METIERS ET LEGALES	28

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES eIDAS CEGEDIM	
V 1.4		

9.1	TARIFS	28
9.2	RESPONSABILITE FINANCIERE	28
9.2.1	<i>Couverture par les assurances</i>	28
9.2.2	<i>Autres ressources</i>	28
9.2.3	<i>Couvertures et garantie concernant les entités utilisatrices</i>	28
9.3	CONFIDENTIALITE DES DONNEES PROFESSIONNELLES	28
9.3.1	<i>Périmètre des informations confidentielles</i>	28
9.3.2	<i>Informations hors du périmètre des informations confidentielles</i>	28
9.3.3	<i>Responsabilités en termes de protection des informations confidentielles</i>	28
9.4	PROTECTION DES DONNEES PERSONNELLES	28
9.4.1	<i>Politique de protection des données personnelles</i>	28
9.4.2	<i>Informations à caractère personnel</i>	28
9.4.3	<i>Informations à caractère non personnel</i>	28
9.4.4	<i>Responsabilité en termes de protection des données personnelles</i>	29
9.4.5	<i>Notification et consentement d'utilisation des données personnelles</i>	29
9.4.6	<i>Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives</i> 29	
9.4.7	<i>Autres circonstances de divulgation d'informations personnelles</i>	29
9.5	DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE	29
9.6	INTERPRETATIONS CONTRACTUELLES ET GARANTIES	29
9.7	LIMITE DE GARANTIE	29
9.8	LIMITE DE RESPONSABILITE	29
9.9	INDEMNITES	30
9.10	DUREE ET FIN ANTICIPEE DE VALIDITE D'UNE POLITIQUE DE SERVICE	30
9.10.1	<i>Durée de validité</i>	30
9.10.2	<i>Fin anticipée de validité</i>	30
9.10.3	<i>Effets de la fin de validité et clauses restant applicables</i>	30
9.11	NOTIFICATION INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS	30
9.12	AMENDEMENTS	30
9.12.1	<i>Procédures d'amendements</i>	30
9.12.2	<i>Mécanisme et période d'information sur les amendements</i>	30
9.12.3	<i>Circonstances selon lesquelles l'OID doit être changé</i>	30
9.13	DISPOSITIONS CONCERNANT LA RESOLUTION DE PLAINTES	30
9.14	JURIDICTIONS COMPETENTES	30
9.15	CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS	30
9.16	DISPOSITIONS DIVERSES	31
9.16.1	<i>Accord global</i>	31
9.16.2	<i>Transfert d'activités</i>	31
9.16.3	<i>Conséquences d'une clause non valide</i>	31
9.16.4	<i>Application et renonciation</i>	31
9.16.5	<i>Force majeure</i>	31
9.17	AUTRES DISPOSITIONS	31

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES eIDAS CEGEDIM	
V 1.4		

1 INTRODUCTION

1.1 Objet du document

Le présent document, *Politiques et pratiques des services de confiance – Mesures de sécurité communes aux services eIDAS de Cegedim*, présente des règles et exigences de sécurité applicables à tous les services de confiance eIDAS mis en œuvre par Cegedim, ce qui recouvre :

- Les services de certification de l'IGC Cegedim sous l'AC Racine **CEGEDIM ROOT CA** ;
- Le service d'horodatage électronique Cegedim **CEGEDIM QUALIFIED TIMESTAMP**.

Ce document reprend le chapitre des politiques de certification (PC) de l'IGC. Il présente des mesures de sécurité suivantes :

- Chapitre 2 : Responsabilités concernant la mise à dispositions des informations devant être publiées
- Chapitre 5 : Mesures de sécurité non techniques
- Chapitre 6 : Mesures de sécurité techniques
- Chapitre 8 : Audit de conformité et autres évaluation
- Chapitre 9 : Autres problématiques métier et légales

Les mesures de sécurité sont communes aux AC et AH excepté celles présentées aux §6.1 à §6.4 spécifiques aux AC.

1.2 Définitions et Acronymes

1.2.1 Définitions

Autorité de certification (AC)

Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.

Autorité d'horodatage (AH)

Au sein d'un PSHE, une Autorité d'Horodatage a en charge, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage.

Certificat électronique

Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par un prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Composante

PUBLIC


	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en oeuvre opérationnelle d'au moins une fonction d'un service de confiance. L'entité peut être le PSCE ou le PSHE lui-même ou une entité externe liée par voie contractuelle, réglementaire ou hiérarchique.

Contremarque de temps

Donnée signée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.

Déclaration des pratiques de certification (DPC)

Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Déclaration des pratiques d'horodatage (DPH)

Une DPH identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AH applique dans le cadre de la fourniture de ses services d'horodatage et en conformité avec la ou les politiques d'horodatage qu'elle s'est engagée à respecter.

Dispositif de protection des éléments secrets

Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au porteur (exemples : clé privée, code PIN, etc). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique ou se présenter au format logiciel (exemple fichier PKCS#12).

Entité

Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Infrastructure de gestion de clés (IGC)


Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Jeton d'horodatage

se reporter à « Contremarque de temps ».

Politique de certification (PC)

Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES eIDAS CEGEDIM	
V 1.4		

d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Politique d'horodatage (PH)

Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.

Porteur de certificat

Personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique.

Prestataire de services de certification électronique (PSCE)

Un PSCE est un type de prestataire de service de confiance (Trust Service Provider dans le règlement eIDAS) qui fournit un service de délivrance et de gestion de certificats électroniques. Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Prestataire de services d'horodatage (PSHE)

Un PSHE est un type de prestataire de service de confiance (Trust Service Provider dans le règlement eIDAS) qui fournit un service de génération et de gestion de contremarques de temps. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH

Temps UTC

Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5, aussi nommée Coordinated Universal Time (UTC)


Unité d'Horodatage (UH)

Ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de contremarques de temps

Utilisateur de certificat

Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique provenant d'un porteur de certificat.


Utilisateur de contremarque de temps

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

Entité (personne ou système) qui fait confiance à une contremarque de temps émise sous une politique d'horodatage donnée par une autorité d'horodatage donnée.

1.2.2 Acronymes

AC	Autorité de Certification
AH	Autorité d'Horodage
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CRL	<i>Certificate Revocation List</i>
DN	<i>Distinguished Name</i>
DPC	Déclarations des Pratiques de Certification
ETSI	<i>European Telecommunications Standards Institute</i>
HSM	<i>Hardware Security Module</i>
IGC	Infrastructure de Gestion de Clés
LCP	<i>Lightweight Certificate Policy</i>
MIE	Moyen d'identification électronique
NCP	<i>Normalized Certificate Policy</i>
OID	<i>Object Identifier</i>
OCSP	<i>Online Certificate Status Protocol</i>
PC	Politique de certification
PCA	Plan de continuité d'activité
PSCE	Prestataire de service de certification électronique
PSSI	Politique de sécurité des systèmes d'information
PVID	Prestataire de vérification d'Identité à distance
QCP	<i>Qualified Certificate Policy</i>
QSCD	<i>Qualified Signature Creation Device</i>
QSealCD	<i>Qualified Seal Creation Device</i>
RL	Représentant légal
UC	Utilisateurs de certificat
UH	Unité d'Horodatage
UUID	<i>Universally unique Identifier (identifiant unique)</i>

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

2 RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 Entités chargées de la mise à disposition des informations

Le Groupe Cegedim est chargé de la mise en place et de la mise à disposition aux personnes et entités concernées par ses services de confiance, ainsi qu'au public, des informations devant être publiées (tel que défini par les normes applicables).

Ces informations sont publiées sur le site de publication suivant :

<https://psco.cegedim.com>

2.2 Description des informations publiées

Le Groupe Cegedim publie au minimum les informations suivantes à destination des porteurs et utilisateurs de certificats ainsi qu'aux abonnés ou utilisateurs du service d'horodatage :

- Pour les services de certification :
 - Les politiques et pratiques de certification ;
 - Les certificats de l'AC en cours de validité et leur empreinte cryptographique (SHA-1) ;
 - La liste des certificats révoqués émise par l'AC ;
 - Le certificat de l'AC Racine et son empreinte cryptographique (SHA-1) ;
- Pour le service d'horodatage :
 - La politique et déclaration de pratiques du service d'horodatage ;
 - Les certificats des Unités d'Horodatage et leur chaîne de certification, et le cas échéant une information sur leur compromission y compris au-delà de leur date d'expiration ;
 - Les Conditions Générales d'Utilisation du service d'horodatage.

Par ailleurs, les AC donnent aussi accès aux porteurs de certificats aux documents suivants :

- Formulaire de gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.) ;
- Conditions Générales d'Utilisation des certificats (CGU)

Le moyen utilisé pour la publication de ces informations garantit l'intégrité, la lisibilité, la compréhensibilité et la clarté des informations publiées.

2.3 Délais et fréquences de publication

Les informations liées aux services sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations délivrées et les engagements, moyens et procédures du Groupe Cegedim.


Le Groupe Cegedim garantit la disponibilité et l'intégrité des informations publiées.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est libre d'accès en lecture.


L'accès en modification au système de publication des informations est strictement limité aux fonctions internes habilitées du Groupe, au moins au travers d'un contrôle d'accès de type mots de passe régi par une politique de gestion stricte des mots de passe.

PUBLIC

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

3 IDENTIFICATION ET AUTHENTIFICATION DES PORTEURS DE CERTIFICATS


Ce chapitre est propre à chacune des PC de l'IGC Cegedim.

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

4 EXIGENCES OPERATIONNELLES

Les exigences opérationnelles sur le cycle de vie des certificats sont présentées dans chacune des PC de l'IGC Cegedim.

Les exigences opérationnelles relatives aux unités d'horodatage sont présentées dans les PH de Cegedim.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

L'ensemble des ressources matérielles des services de confiance sont hébergées dans deux centres de données séparés d'un minimum de 20 km.

Ces deux centres sont situés sur le territoire français.

5.1.2 Accès physique

L'accès au site d'hébergement des services de confiance est contrôlé et est strictement limité aux seules personnes autorisées à pénétrer dans les locaux. Les personnes non autorisées doivent toujours être accompagnées par des personnes autorisées.

5.1.3 Alimentation électrique et climatisation

Le Groupe Cegedim assure que les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences des services de confiance en matière de disponibilité de leurs fonctions.

5.1.4 Vulnérabilité aux dégâts des eaux

Les sites d'hébergement sont conformes aux exigences de protection contre les dégâts des eaux, et permettent de respecter les exigences des services de confiance en matière de disponibilité de ses fonctions.

5.1.5 Prévention et protection incendie

Les risques d'incendie ont été pris en compte pour l'installation des services de confiance. Les règles de sécurité incendie permettent de respecter les exigences prévues en matière de disponibilité de ses fonctions, notamment, les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Les différents supports utilisés par les services de confiance sont stockés de manière sécurisée.

Les documents papiers sont conservés par le Groupe Cegedim dans des locaux fermés à clés et sont stockés dans un coffre-fort fermé à clé, que seul le responsable ou les personnes autorisées peuvent ouvrir.

Le Groupe Cegedim assure que les différentes informations nécessaires intervenant dans l'activité des services de confiance sont listées, et les besoins en sécurité sont définis. Les supports correspondant à ces informations sont gérés en fonction de leur besoin en sécurité.


Le Groupe Cegedim met en œuvre les moyens nécessaires pour que les supports soient protégés contre l'obsolescence et la détérioration pendant la période de temps durant laquelle le service s'est engagé à conserver ces informations.

5.1.7 Mise hors service des supports

En fin de vie, les supports sont détruits de manière sécurisée ou réinitialisés en vue d'une réutilisation.

5.1.8 Sauvegardes hors site

Des sauvegardes hors site sont mises en œuvre par les services de confiance vers un site de secours afin d'assurer une reprise des fonctions des services de confiance le plus rapidement possible après

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

incident, conformément aux engagements des différents services en matière de disponibilité et, plus particulièrement, en ce qui concerne la fonction d'information de l'état de révocation des certificats.

Le site de secours offre un niveau de sécurité au moins équivalent au site principal et garantit notamment que les informations sauvegardées hors site sont protégées en confidentialité et en intégrité au même niveau que sur le site principal.

La procédure de sauvegarde hors site est détaillée dans la procédure de sauvegarde.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiance suivants sont définis :

- Security Officer : Responsable de la sécurité du service de certification, chargé de définir et de vérifier la mise en œuvre de la politique de sécurité des services de confiance ;
- System Administrator : Administrateur système des composantes, chargé de la mise en route, de la configuration et de l'administration des équipements informatiques, ainsi que de leur restauration dans le cadre de la continuité ou reprise d'activité ;
- System Operator : Opérateur système des composantes, chargé de la surveillance, de la maintenance des systèmes informatiques, et de la sauvegarde des configurations et données de ces systèmes ;
- System Auditor : Contrôleur autorisé à consulter les traces et les archives du service afin de détecter de potentielles violations de la politique de sécurité ;
- Application Administrator : Administrateur fonctionnel des services de confiance, chargé de la configuration logicielle des différentes composantes ;
- Registration and revocation officer : Opérateur d'enregistrement et de révocation de l'AE ou de l'AED de l'IGC, en charge de la constitution du dossier de demande de certificat ou de vérification d'une demande de révocation.

Les rôles de confiance sont définis et attribués de telle sorte qu'il n'y ait aucun conflit d'intérêt possible entre ces rôles.

5.2.2 Nombre de personnes requises par tâche

En fonction des opérations réalisées, une ou plusieurs personnes avec des rôles différents sont requises.

5.2.3 Identification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement d'un service de confiance doit avoir préalablement reçu le rôle correspondant.


L'accès physique est autorisé aux seules personnes qualifiées. L'accès logiciel est protégé par des politiques de sécurité fortes.

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 cumuls des rôles suivants par une même personne physique sont interdits :

- Un responsable de la sécurité ne peut avoir aucun autre rôle de confiance ;
- Un contrôleur ne peut avoir aucun autre rôle de confiance ;

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

- Un ingénieur système peut être à la fois administrateur et exploitant système, mais ne peut avoir aucun autre rôle supplémentaire ;
- Un opérateur d'enregistrement et de révocation ne peut avoir aucun autre rôle de confiance

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tout le personnel du Groupe Cegedim contribuant aux services de confiance est soumis à une clause de confidentialité et a notamment signé la charte de sécurité.

Les fonctions demandées à chaque membre du personnel sont compatibles avec ses compétences. Le personnel d'encadrement dispose de l'expertise nécessaire et est familier des procédures de sécurité.

Le responsable des services de confiance informe toute personne intervenant dans les rôles de confiance :

- Des responsabilités relatives aux services qui lui incombent
- Des procédures liées à la sécurité du système et au contrôle du personnel qu'elle doit respecter

5.3.2 Procédures de vérification des antécédents

Le personnel travaillant pour l'une des composantes des services de confiance est soumis à une procédure de vérification des antécédents lors de leur prise de fonction.

Les vérifications portent sur les points suivants :

- Les éventuelles condamnations en justice de la personne ne devront pas être contraires à ses fonctions
- Les rôles de confiance de la personne ne devront pas se trouver dans un conflit d'intérêt préjudiciable à l'impartialité de ses tâches.

5.3.3 Exigences en matière de formation initiale

Le recrutement du personnel des services de confiance permet de vérifier que chacun dispose de la formation initiale adéquate à la réalisation de ses fonctions.

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met œuvre et doit respecter.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel recevra une formation adaptée préalablement aux évolutions des services de confiance (procédures, organisation, application, etc.) concernant la ou les composantes sur lesquelles il intervient.


D'autre part, le personnel des services de confiance participe annuellement à des séances de formation sur la sécurité des systèmes d'information.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation d'un service de confiance, elle peut faire l'objet de sanctions disciplinaires.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

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

Les exigences de la section §5.3 sont applicables aux prestataires externes.

5.3.8 Documentation fournie au personnel

Tout le personnel des services de confiance a accès à des procédures et manuels complémentaires concernant leurs fonctions et leurs responsabilités.

5.4 Procédure de constitution des données d'audit

5.4.1 Type d'évènements à enregistrer


Les événements ci-dessous sont enregistrés de manière manuelle ou automatique :

- Création / modification / suppression de comptes Utilisateur et des données d'authentification correspondantes
- Démarrage et arrêt des systèmes informatiques et des applications
- Évènement 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
- Les accès physiques
- Les actions de maintenance et de changement de la configuration des systèmes
- Les changements apportés au personnel
- Les actions de destruction des supports

Les évènements spécifiques aux différentes fonctions de l'IGC sont également être journalisés :
réception d'une demande de certificat (initiale et renouvellement) ;

- Validation / rejet d'une demande de certificat ;
- Evènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), Sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- Génération des éléments secrets du porteur (bi-clé, codes d'activation,...) ;
- Génération des certificats des porteurs ;
- Transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs ;
- Remise de son dispositif de protection des éléments secrets au porteur ;
- 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 LCR (et éventuellement des deltaLCR) ou des, requêtes / réponses OCSP.

Les événements spécifiques au service d'horodatage ci-dessous sont enregistrés:

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

- Publication et mise à jour des informations liées à l'AH (PH, certificats d'UH, conditions générales d'utilisation, etc.) ;
- Evènements liés au cycle de vie des clés ;
- Evènements liés au cycle de vie des certificats des unités d'horodatage ;
- Synchronisation de l'horloge des unités d'horodatage, incluant l'information concernant des recalibrages ou des synchronisations normales ;
- Détection de perte de synchronisation.

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

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- Résultat de l'évènement (échec ou réussite).

5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'évènements sont systématiquement analysés afin de détecter tout évènement anormal.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés pendant au moins un mois sur site avant d'être archivés (cf. §5.5.2).

5.4.4 Protection des journaux d'évènements

Le mode de conservation des journaux d'évènements protège leur intégrité et leur disponibilité.

Ils ne sont accessibles qu'au personnel autorisé à les exploiter.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux d'évènement sont régulièrement sauvegardés et exportés sur le site de secours.

5.4.6 Système de collecte des journaux d'évènements

Les journaux d'évènements sont collectés par des agents installés sur chaque système et centralisés dans un outil d'analyse des journaux.


5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

5.4.8 Évaluation des vulnérabilités

Pour détecter les vulnérabilités et plus généralement les anomalies, le Groupe Cegedim met en place les contrôles suivants :

- Réalisation régulière de tests d'intrusion et de scans de vulnérabilités sur les équipements et serveurs des services de confiance
- Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Les vulnérabilités pouvant affecter le système sont étudiées et traitées, par le déploiement de correctifs ou de mesures palliatives, dans des délais cohérents avec la criticité de la menace.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

- La non application d'un correctif de sécurité disponible est motivée (par exemple, l'introduction de vulnérabilités additionnelles ou d'instabilités considérées supérieures au bénéfice du correctif) et tracée.
- Les vulnérabilités critiques affectant le système sont prises en compte dans les 48 heures suivant leur découverte

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont, au minimum, les suivantes :

- Toutes les versions des CGU, politiques et pratiques des services de confiance
- Les accords contractuels entre les services de confiance et les souscripteurs
- La preuve d'acceptation des CGU par les souscripteurs
- Les certificats permettant d'identifier les services de confiance (AC, CRL)
- Les journaux d'événements des différentes composantes
- Les rapports d'audit
- Les différents types de données à archiver sont détaillés dans la procédure d'archivage et des compléments peuvent être apportés par la politique de chacun des services.

5.5.2 Période de conservation des archives

La période de conservation des archives est de 10 ans à compter de la création de l'événement.

5.5.3 Protection des archives

Les archives, qu'elles soient au format papier ou électronique, sont conservées de façon à garantir leur intégrité et leur confidentialité afin que seules les personnes autorisées puissent y accéder.

5.5.4 Procédure de sauvegarde des archives

Une réplication des archives est réalisée automatique sur une site de secours.

5.5.5 Exigences d'horodatage des données

Voir §6.7.


5.5.6 Système de collecte des archives

La collecte des archives est réalisée automatiquement par des outils adaptés au type de données archivées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives, qu'elles soient au format papier ou électronique, peuvent être récupérées dans un délai inférieur à 2 jours ouvrés suite à l'acceptation par le Groupe Cegedim de la demande de récupération de l'archive.

Les détails sur les procédures de récupération et de vérification des archives sont décrits dans la procédure d'archivage et la politique concernée.

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

5.6 Reprise suite à la compromission et sinistre

5.6.1 Procédures de remontée et de traitement des incidents et des compromissions

Le Groupe Cegedim met 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 et au travers de l'analyse des différents journaux d'évènements.

Toute activité anormale est détectée et remontée aux exploitants. Dans ce but, les composantes matérielles et logicielles sont constamment supervisées et les journaux d'évènements sont analysés automatiquement et de façon régulière.

Le Groupe Cegedim dispose d'un *Plan de continuité d'activité* (PCA) qui décrit la procédure à exécuter en cas d'incident majeur affectant le bon fonctionnement des services de confiance.

Un incident majeur tel que la perte, la suspicion de compromission, la compromission ou encore le vol d'une clé privée (AC, UH...), est immédiatement notifié au responsable de la sécurité qui peut alors décider, si cela est nécessaire, de demander la révocation du certificat concerné.

Dans ce cas, il notifiera dans les plus brefs délais, et au maximum dans les 24 heures, le point de contact identifié sur le site <https://www.ssi.gouv.fr> et, concernant les services certifiés ou qualifiés, l'organisme de certification.

En cas d'incident majeur de sécurité ayant un impact important sur des données à caractère personnel, le Groupe Cegedim notifiera la CNIL et les entités concernées (personnes morales ou physiques) sans délai.

Si l'un des algorithmes, ou des paramètres associés, utilisés devient insuffisant pour son utilisation prévue restante, le Groupe Cegedim publiera l'information sur son site Internet et révoquera les certificats concernés.

5.6.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données)

Le PCA définit les procédures de reprise en cas de corruption des ressources informatiques ainsi que les procédures visant à assurer la disponibilité des composantes critiques des services de confiance.

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

Si la clé privée d'une composante est compromise, soupçonnée d'être compromise, perdue ou détruite :


- 1) Le Groupe Cegedim, après enquête, demande la révocation du ou des certificats concernés
- 2) La procédure de révocation est appliquée
- 3) Les porteurs dont le certificat a été révoqué, les entités avec lesquelles le Groupe Cegedim a passé des accords ou d'autres formes de relations établies, sont notifiés dans les plus brefs délais de la révocation
- 4) Le Groupe Cegedim publie sur son site de publication toutes les informations nécessaires (description de l'incident, plan d'action, etc.). L'information de compromission de la clé privée de l'AC est publiée pour une période minimale de 3 mois après l'identification de l'incident de sécurité.

5.6.4 Capacités de continuité d'activité suite à un sinistre

Se référer au PCA.

5.7 Fin de vie

Une ou plusieurs composantes des services de confiance peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses. Par exemple, il se peut que l'entité

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

propriétaire de l'AC fasse l'objet d'un rachat, d'une fusion, ou d'une transformation (changement de statut, de capital...).

Cegedim dispose et maintient à jour un plan de cessation ou de transfert d'activité de ses services de confiance afin de garantir aux porteurs et utilisateurs des certificats un impact minimal. En particulier, ce plan prévoit :

- En cas d'expiration ou de cessation d'activité de l'AC :
 - La révocation de l'ensemble des certificats non expirés émis par cette AC ;
 - La génération et la publication d'une dernière liste de révocation ayant comme date de fin de validité le 31 décembre 9999, 23h59m59s ;
 - En cas de compromission de la clé privée d'une AC, la dernière CRL émise est publiée accompagnée d'une empreinte SHA-256 afin d'en garantir l'intégrité et l'origine.
- En cas de cessation d'activité de l'AH :
 - La révocation de l'ensemble des certificats non expirés des UH du service ;
- Le maintien de la disponibilité des informations nécessaires à la vérification des certificats ou des contremarques de temps qu'elle a émis (chaines de certificats de l'AC, informations de révocation), par les moyens propres du groupe Cegedim ou à défaut par une tierce partie. Les informations restent accessibles pour une durée de 1 an après la cessation d'activité de l'AC ou de l'AH. Cegedim s'efforcera de garantir la publication des informations aux adresses nominales définies par la PC, et à défaut informera les porteurs et utilisateurs des certificats des modalités de récupération de ces éléments ;
- L'information préalable des clients, des porteurs et utilisateurs de certificats, ainsi que des tierces parties impactées et liées aux services de confiance, de la cessation ou du transfert d'activité à venir ;
- L'information des organismes d'audit ayant certifié l'AC, et de l'organe de contrôle national (ANSSI) ;
- La clôture des autorisations et des contrats avec des fournisseurs ou sous-traitants prenant part à la fourniture du service de certification de l'AC et dont les activités ne sont plus nécessaires ;
- Le maintien du service d'archivage de tous les éléments de preuve conservés au titre de la présence PC (dossiers d'enregistrement, informations de statut de révocation des certificats et journaux d'événements) pour l'entièreté de la durée prévue, par les moyens propres du groupe Cegedim ou à défaut par une tierce partie ;
- La destruction définitive des clés privées des composantes de l'AC (en particulier la clé privée de signature de l'AC) et de toutes leurs copies afin qu'elles ne puissent plus être utilisées ;
- La définition des dispositions nécessaires pour couvrir les coûts permettant de respecter les exigences minimales dans le cas où l'AC/AH serait en faillite ou, pour d'autres raisons, serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

En cas de cessation d'activité, l'AC/AH s'efforce d'identifier d'autres AC/AH susceptibles de se voir transférer l'activité ou de fournir des solutions de niveau équivalent aux porteurs disposant de certificats encore valides.


5.8 Gestion des risques

5.8.1 Analyse de risques

Avant le lancement d'un service de confiance, le Groupe Cegedim effectue ou fait effectuer une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques, métier et commerciaux. Cette analyse de risque met en exergue, en particulier, les systèmes « critiques » du service.

Suite à cette analyse de risque, le Groupe Cegedim sélectionne et met en œuvre des mesures de traitement du risque et les procédures opérationnelles associées en alignant le niveau de sécurité soit acceptable sur le degré de risque.

Les risques résiduels identifiés sont acceptés durant le processus d'homologation du service.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

Cette analyse de risque est revue régulièrement, a minima annuellement, et lors de toute évolution significative d'un système ou d'une composante d'un service de confiance.

5.8.2 Homologation

Pour une AC qualifiée, le système d'information du service doit être homologué préalablement à la fourniture du dit service. L'analyse de risque est approuvée par la direction du Groupe, qui accepte ainsi les éventuels risques résiduels identifiés ; cette phase correspond à l'homologation du système d'information du service.

Cette homologation doit être prononcée au moins tous les trois ans.

Pour un service de confiance certifié mais non qualifié, la fourniture du service peut être préalable à son homologation.

5.8.3 Politique de sécurité du système d'information

Le Groupe Cegedim dispose d'une *Politique de sécurité du système d'information* (PSSI). Cette PSSI est approuvée par la direction.


La PSSI est un document de référence, commun à l'ensemble des services de confiance, qui fixe les enjeux, les principes de gouvernance et les fondamentaux de sécurité. Les directives de sécurité associées définissent les exigences de sécurité à mettre en œuvre ; ces dernières peuvent être définies pour tout ou partie des services et du système d'information du Groupe Cegedim.

La PSSI est systématiquement communiquée à l'ensemble des collaborateurs du Groupe Cegedim, et transmise aux sous-traitants concernés ; elle est aussi portée à la connaissance des organismes de certification et de l'organe de contrôle national (ANSSI).

Le Groupe Cegedim demeure responsable de la conformité globale avec les exigences prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvre par des sous-traitants. Le Groupe Cegedim s'assure de la mise en œuvre effective des mesures prévues dans la PSSI.

La PSSI est revue annuellement ainsi qu'à l'occasion d'un changement majeur du SI, afin de maintenir sa pertinence et son exhaustivité.

Tout changement au niveau de la PSSI susceptible d'avoir un impact sur le niveau de sécurité d'un service de confiance doit être approuvé par le comité de pilotage du service. Les modifications apportées à la PSSI sont communiquées aux parties prenantes concernées.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

6 MESURES DE SECURITE TECHNIQUES

6.1 Mesures de sécurité pour la protection des clés privées et pour les dispositifs cryptographiques

6.1.1 Standards et mesures de sécurité pour les dispositifs cryptographiques

Les dispositifs cryptographiques utilisés pour la génération et la mise en œuvre des bi-clés de l'AC sont des HSM certifiés satisfaisant aux exigences définies dans la section 6.1.11.

Les HSM de l'AC sont hébergés dans les sites sécurisées des services de confiance et sont gérés exclusivement par les personnes ayant les rôles de confiance requis.

6.1.2 Contrôle de la clé privée

6.1.2.1 Clé privée de l'AC

L'activation de la clé privée de l'AC est réalisée par plusieurs porteurs de parts de secret qui ont nécessairement participé à la cérémonie des clés de l'AC et au cours de laquelle leur part de secret leur a été remise dans une carte à puce personnelle et protégée par un code PIN qu'ils ont eux-mêmes défini.

6.1.2.2 Clé privée du Sujet

Les mesures relatives aux clés privées du sujet sont détaillées dans les Politiques de Certifications de chacune des AC.

6.1.3 Séquestre de la clé privée

Les clés privées d'AC et des sujets ne font pas l'objet de séquestre.

6.1.4 Copie de secours d'une clé privée d'AC

La clé privée d'une AC est sauvegardée dans le but d'avoir des copies de secours. Elle peut être sauvegardée :

- Soit hors d'un dispositif cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du dispositif cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé.
- Soit dans un dispositif cryptographique équivalent opéré dans des conditions de sécurité similaires ou supérieures.


Les sauvegardes sont réalisées sous le contrôle d'au moins deux personnes ayant les rôles de confiance adéquats dans l'AC.

6.1.5 Archivage d'une clé privée

Les clés privées ne sont pas archivées.

6.1.6 Transfert d'une clé privée vers et depuis le dispositif cryptographique

La clé privée de l'AC est transférée uniquement lors de la génération des copies de secours de la clé privée tel que décrit dans la section 6.1.4. La création d'une copie de secours ou son import dans un HSM sont réalisés dans les locaux sécurisés des services de confiance par au moins deux personnes ayant les rôles de confiance adéquats dans l'AC.

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

6.1.7 Stockage de la clé privée dans un dispositif cryptographique

Le stockage des clés privées d'AC est réalisé dans un HSM satisfaisant aux exigences définies dans la section 6.1.11 ou en dehors d'un tel HSM moyennant le respect des exigences définies à la section 6.1.4.

6.1.8 Méthode d'activation de la clé privée

6.1.8.1 Clé privée d'AC

L'activation de la clé privée de l'AC est réalisée dans le HSM de l'AC par au moins deux personnes ayant les rôles de confiance adéquats.

6.1.8.2 Clé privée d'un Sujet

Les mesures relatives aux clés privées du sujet sont détaillées dans les Politiques de Certifications de chacune des AC.

6.1.9 Méthode de désactivation de la clé privée

La désactivation de la clé privée de l'AC dans le HSM s'opère automatiquement lors de l'arrêt du dispositif cryptographique.

6.1.10 Méthode de destruction d'une clé privée

La destruction de la clé privée d'AC ne peut être effectuée qu'à partir du dispositif cryptographique. En cas de destruction, l'AC s'assure que toutes les copies de secours de sa clé privée sont également détruites.

Les mesures relatives aux clés privées du sujet sont détaillées dans les Politiques de Certifications de chacune des AC.

6.1.11 Niveau de qualification des dispositifs cryptographiques

6.1.11.1 AC

Le dispositif cryptographique utilisé pour générer, conserver et utiliser les clés privées de l'AC est un HSM qualifié renforcé¹ par l'ANSSI.

6.1.11.2 Sujet

Les mesures relatives aux clés privées du sujet sont détaillées dans les Politiques de Certifications de chacune des AC.

6.2 Autres aspects de la gestion des bi-clés

6.2.1 Archivage des clés publiques


Les certificats contenant les clés publiques de l'AC sont archivés conformément à la section 6.1.5.

6.2.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats de l'AC ont une durée de vie maximale de 10 ans.

Les mesures relatives aux clés privées du sujet sont détaillées dans les Politiques de Certifications de chacune des AC.

¹ <https://www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/>

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES eIDAS CEGEDIM	
V 1.4		

6.3 Données d'activation des clés privées des AC

6.3.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation des clés privées d'AC sont réalisées lors de la cérémonie des clés, en présence d'un huissier de justice. Ces données d'activation sont stockées sur des cartes à puce associées au dispositif cryptographique de l'AC et sont remises en main propre, durant la cérémonie, à chacune des personnes ayant le rôle de confiance de porteur de secret. Ces personnes doivent prendre les mesures nécessaires pour se prémunir contre la perte, le vol et l'utilisation non autorisée de leurs cartes à puce et des données d'activation qu'elles contiennent.

6.3.2 Protection des données d'activation

Les données d'activation correspondant à la clé privée d'une AC sont générées durant la cérémonie des clés sur HSM et sont stockées sur des cartes à puce nominatives, personnelles, et remises en main propre aux porteurs de secrets. Chacune de ces personnes est responsable de ses cartes à puce, principales et de secours, protégées par un code PIN qu'elle a spécifiée lors de la cérémonie des clés. Elle a de plus signé une attestation de remise de sa carte à puce.

6.3.3 Autres aspects liés aux données d'activation

La destruction des données d'activation est réalisée par la destruction physique de la carte à puce les contenant ou par leur effacement définitif et irréversible.

6.4 Mesures de sécurité des systèmes informatiques

6.4.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Le Groupe Cegedim définit les objectifs de sécurité suivants :

- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès, notamment pour implémenter les principes de moindres privilèges, de contrôle multiple et de séparation des rôles) ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- La gestion des droits des utilisateurs est mise en œuvre en prenant en compte les différents rôles identifiés dans le présent document (5.2.1). Des procédures assurent que l'octroi et le retrait des habilitations s'effectue en accord avec la gestion des ressources humaines ;
- Identification et authentification forte des utilisateurs pour l'accès aux systèmes ;
- Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée.

Les informations sensibles sont protégées contre la divulgation, y compris en cas de réutilisation de ressources par des personnels non autorisés (p. ex., fichiers effacés).

6.4.2 Niveau de qualification des systèmes informatiques

Pas d'exigence.


6.5 Mesures de sécurité liées au développement des systèmes

6.5.1 Mesures de sécurité liées au développement des systèmes

Tous les développements réalisés par le Groupe Cegedim et affectant les services de confiance sont documentés et réalisés via un processus de manière à en assurer la qualité.

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

Le Groupe Cegedim opère un cloisonnement entre l'environnement de développement et les environnements de pré-production et de production.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

6.5.2 Mesures liées à la gestion de la sécurité

Les configurations et les mises à jour des applications sont effectuées de manière sécurisée par le personnel compétent apparaissant dans les rôles de confiance.

6.5.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.6 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 au sein des services de confiance.

Le réseau et ses systèmes sont protégés contre les attaques via des mesures et des objectifs de sécurité identifiés dans l'analyse de risques (cf. §5.8.1).

Le SI est segmenté en réseaux ou zones en fonction de l'analyse de risque, compte tenu de la relation fonctionnelle, logique et physique entre les composants et les services.

Les mêmes contrôles de sécurité sont appliqués à tous les systèmes partageant la même zone.

Les accès et les communications sont restreints entre les réseaux et les zones et définis au strict nécessaire pour le fonctionnement du service.

Les connexions et les services inutiles sont explicitement interdits ou désactivés.

Les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la PSSI (5.8.3) et des politiques et pratiques des services de confiance.

L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné.

Les systèmes utilisés pour l'administration de la mise en œuvre de la PSSI ne doivent pas être utilisés à d'autres fins.

Les systèmes de production du service sont séparés des systèmes utilisés pour le développement et les tests.


La communication vers les HSM n'est établie qu'à travers des canaux sécurisés, logiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.

Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service est effectuée par une personne ou une entité ayant les compétences, les outils, l'éthique et l'indépendance nécessaires. Cette analyse donne lieu à un rapport.

Un test d'intrusion sur les systèmes du service est réalisé lors de la mise en place et après toute évolution de l'infrastructure ou des applications. Ce test est effectué par une personne ou une entité ayant les compétences, les outils, l'éthique et l'indépendance nécessaires, et donne lieu à un rapport.

6.7 Horodatage / Système de datation


Les différents serveurs utilisés par les services de confiance sont synchronisés au moins une fois par jour à partir de serveurs *Network Time Protocol* (NTP).

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

7 PROFILS

Les profils des certificats et des LCR sont présentés dans chacune des PC de l'IGC Cegedim.

Les profils des requêtes et réponses d'horodatage sont présentés dans la PH de Cegedim.

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquences et circonstances des évaluations

Avant la première mise en service d'une composante d'un service de confiance certifié ou qualifié, ou suite à toute modification significative au sein d'une composante, le Groupe Cegedim fait procéder à un audit de conformité de cette composante vis-à-vis de sa politique et de ses pratiques déclarées.

Le Groupe Cegedim réalise des audits internes annuellement, et fait réaliser tous les deux ans, par un organisme accrédité, un audit de certification ou de qualification.

8.2 Identités et qualifications des évaluateurs

Groupe Cegedim s'engage à mandater des contrôleurs qui sont compétents en sécurité des systèmes d'information et en particulier dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

Pour les audits internes, l'auditeur sera nommé par le responsable de l'AC et pourra appartenir à Groupe Cegedim, mais devra nécessairement être indépendant du service de confiance.

Pour l'audit de certification, l'auditeur ne devra pas appartenir à Groupe Cegedim ou présenter un quelconque conflit d'intérêt.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante du service (contrôles ponctuels) ou sur l'ensemble de l'architecture du service (contrôles périodiques) ; ils visent à vérifier le respect des engagements et pratiques définies dans la politique du service, ses pratiques déclarées et dans les procédures internes associées.

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations qui peuvent être :


- La cessation (temporaire ou définitive) d'activité
- La révocation du certificat de la composante
- Tout autre mesure

Le choix de la mesure à appliquer est effectué par le responsable de l'AC et doit respecter ses politiques de sécurité internes.

En cas de résultat « à confirmer », l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées.

8.6 Communication des résultats

Les résultats des audits sont tenus à la disposition de l'organisme de certification et de l'organe de contrôle national.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

Les tarifs sont définis dans les relations contractuelles liant le client et le Groupe Cegedim.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Le Groupe Cegedim a souscrit une assurance en responsabilité civile professionnelle couvrant ses prestations de PSCO auprès d'une compagnie d'assurance.

9.2.2 Autres ressources

Le Groupe Cegedim dispose des ressources financières suffisantes pour assurer la fourniture de ses services de confiance conformément à leurs engagements.

9.2.3 Couvertures et garantie concernant les entités utilisatrices

Se référer à la politique de chaque service de confiance.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les procédures internes des services
- Les clés privées mis en œuvre par les composantes des services
- Les données d'activation de ces clés privées
- Les journaux d'événements des composantes
- Les rapports d'audit
- D'autres informations peuvent être classées comme confidentielles ; se référer à la politique de chaque service de confiance pour plus d'information.

9.3.2 Informations hors du périmètre des informations confidentielles

Se référer à la politique de chaque service de confiance.

9.3.3 Responsabilités en termes de protection des informations confidentielles

Le Groupe Cegedim s'engage à traiter les informations confidentielles dans le respect de la législation et de la réglementation en vigueur sur le territoire français.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles


Le Groupe Cegedim s'engage à collecter et utiliser les données personnelles en respectant la législation et la réglementation européenne en vigueur relative à la protection des données à caractère personnel.

9.4.2 Informations à caractère personnel

Se référer à la politique de chaque service de confiance.

9.4.3 Informations à caractère non personnel

Sans objet.

	POLITQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

9.4.4 Responsabilité en termes de protection des données personnelles

Le Groupe Cegedim respecte, pour le traitement et la protection des données à caractère personnel, la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 [CNIL], et au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 [RGPD].

9.4.5 Notification et consentement d'utilisation des données personnelles

Les données personnelles ne sont jamais utilisées, sans le consentement exprès et préalable de la personne, à d'autres fins que celles définies :

- Dans la politique et les pratiques du service
- Dans l'accord de souscription ou tout accord contractuel

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

Les données personnelles peuvent être mis à la disposition de la justice en cas de besoin pour servir de preuve dans le cadre d'une procédure judiciaire.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par le Groupe Cegedim sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerces et de services, dessins et modèles, signes distinctifs et droits d'auteur est sanctionnée par le Code de la propriété intellectuelle.

Le Groupe Cegedim détient tous les droits de propriété intellectuelle et est propriétaire des documents publiés sur son site (voir section 2).

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes des services de confiance sont les suivantes


- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes ou privées
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par les politiques et pratiques du service, et les documents qui en découlent ;
- Respecter et appliquer les procédures internes
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par le Groupe Cegedim (cf. section 7) et l'organisme de qualification
- Respecter les accords ou contrats qui les lient entre elles ou aux porteurs
- Documenter leurs procédures internes de fonctionnement
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.7 Limite de garantie

Se référer à la politique de chaque service de confiance.

9.8 Limite de responsabilité

Se référer à la politique de chaque service de confiance.

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité d'une politique de service

9.10.1 Durée de validité

Se référer à la politique de chaque service de confiance.

9.10.2 Fin anticipée de validité

Sauf mention contraire, une politique reste en application jusqu'à son remplacement par une nouvelle version.

9.10.3 Effets de la fin de validité et clauses restant applicables

Se référer à la politique de chaque service de confiance.

9.11 Notification individuelles et communications entre les participants

Après validation, le Groupe Cegedim publie toute nouvelle version sur le site de publication (voir section 2).

9.12 Amendements

9.12.1 Procédures d'amendements

Le Groupe Cegedim est responsable de la création, l'approbation, la maintenance et la modification des politiques et pratiques des services.

Seuls les changements mineurs tels que la correction de fautes d'orthographe ou d'erreurs ne remettant pas en cause le sens de la politique peuvent être réalisés sans nécessiter de notification publique.

9.12.2 Mécanisme et période d'information sur les amendements

Lors de tout changement important, le Groupe Cegedim informera les acteurs au travers d'un communiqué distribué par voie électronique ou sur son site Internet.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Si le Groupe Cegedim juge qu'un changement important est nécessaire, et qu'il a un impact majeur sur le service, ce dernier publiera une nouvelle version, portant un nouvel OID.

9.13 Dispositions concernant la résolution de plaintes


Le Groupe Cegedim a mis en place une procédure interne de résolution des plaintes.

9.14 Juridictions compétentes

L'ensemble des documents contractuels est soumis à la législation et à la réglementation en vigueur sur le territoire français.

9.15 Conformité aux législations et réglementations

Les politiques et pratiques des services sont conformes à la législation et à la réglementation en vigueur sur le territoire français.

	POLITIQUES ET PRATIQUES DES SERVICES DE CONFIANCE MESURES DE SECURITE COMMUNES AUX SERVICES EIDAS CEGEDIM	
V 1.4		

9.16 Dispositions diverses

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Sans objet.

9.16.3 Conséquences d'une clause non valide

Sans objet.

9.16.4 Application et renonciation

Sans objet.

9.16.5 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.

9.17 Autres dispositions

Le Groupe Cegedim s'assure que les activités qu'elle réalise dans le cadre de ses services de confiance sont non discriminatoires.