PUBLIC

POLITIQUE GENERALE DU TSP MEDIACERT

AUTEUR(S) : F. Da Silva
N° DE DOCUMENT : WLM-TSP-F094
VERSION : 1.3
STATUT : Final
SOURCE : Worldline
DATE DU DOCUMENT : 12 octobre 2018
NOMBRE DE PAGES : 52

Rôle	Nom	Signature	Date
Relecteur 1 – Resp. adjoint du TSP	Fanny Lesecq	Fanny Lesecq	12/10/2018
Relecteur 2 – RSSI	Didier Sobkowiak	Didier Sobkowiak	12/10/2018
Fonction d'assurance qualité	Franck Da Silva	Franck Da Silva	12/10/2018
Propriétaire du document	Comité MediaCert	Guillaume Bailleul	12/10/2018
Approbateur – Resp. TSP	Cyril Lootvoet	Cyril Lootvoet	12/10/2018

CYRIL LOOTVOET

Digitally signed by CYRIL LOOTVOET
DN: C=FR, L=SECLIN, O=Atos Worldline, OU=fr01.awl.atosorigin.net, SN=LOOTVOET, G=CYRIL, CN=CYRIL LOOTVOET, OID.0.9.2342.19200300.100.1.1=A536912, E=cyril.lootvoet@worldline.com
Reason: I am approving this document
Location:
Date: 2018-10-12 15:50:17

Table des Matières

Liste des modifications

Version	Date	Description	Auteur(s)
0.1	14/11/2017	Initialisation du document	F. Da Silva N. Abrioux V. Dumond
1.0	30/03/2017	Validation du document en Comité Sécurité	Comité Sécurité
1.1	05/07/2018	Intégration des remarques post-audit interne de la plateforme d'horodatage : Modification du délai de publication de la documentation du TSP MediaCert Modification du schéma de présentation du TSP MediaCert	F. Da Silva C. Lootvoet
1.2	18/09/2018	Intégration du Service d'Archivage Electronique au périmètre du TSP MediaCert Prise en compte de l'intégration d'une nouvelle AC (l'AC OTU LCP) ce qui n'entraîne qu'une modification au niveau du périmètre fonctionnel la PG	F. Da Silva
1.3	12/10/2018	Prise en compte des remarques/écarts détectés lors de l'audit de certification 2018 de l'AC OTU LCP : • séparation des tâches de revue/validation et d'approbation des documents	F. Da Silva

1 Préface

1.1 Références

1.1.1 Réglementations

Référence	Description
[CNIL]	Loi 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
[EIDAS]	REGLEMENT (UE) N°910 DU PARLEMENT EUROPEEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
[SIAF]	Code du Patrimoine Décret n°2011-574 du 24 mai 2011 Livre 2
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

1.1.2 Références réglementaires techniques

Référence	Description
[ETSI 119 312]	ETSI EN 119 312 v1.2.1 (2017-05) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI 319 401]	ETSI EN 319 401 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ISO 27001]	ISO/IEC 27001 : 2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information - Exigences
[ISO 27002]	ISO/IEC 27002 : 2013 Code de bonnes pratiques pour le management de la sécurité de l'information
[Hygiène]	Guide d'hygiène informatique - Renforcer la sécurité de sons système d'information en 42 mesures Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
[Qualification ANSSI]	Prestataires de services de confiance qualifiés Critères d'évaluation de la conformité au règlement eIDAS v1.1 Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
[RGS B1]	Référentiel Général de Sécurité v2.0 - Annexe B1 (2014-02) Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) Mécanismes cryptographiques : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques

Référence	Description
[SOGIS_CRYPTO]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version en vigueur. Disponible sur http://sogis.org

1.2 Définitions

Une liste des principales définitions des termes techniques employés dans la présente PG est présentée ci-dessous :

Abonné : entité/organisation qui bénéficie d'un ou de plusieurs services de confiance délivrés par le TSP MediaCert.

Bi-clé : couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptographie basée sur des algorithmes asymétriques (RSA par exemple).

Certificat : élément de données normalisé X509 permettant d'associer une clé publique à son détenteur. Un Certificat contient des données comme l'identité du détenteur, sa clé publique, l'identité de l'organisme ayant émis le Certificat, la période de validité, un numéro de série, une empreinte (*digest*) ou bien encore les critères d'utilisation. Le tout est signé par la clé privée de l'Autorité de Certification ayant émis le Certificat.

Service d'Archivage : service qui regroupe un ensemble d'actions visant à identifier, recueillir, classer, conserver, communiquer et restituer des documents électroniques, pour la durée nécessaire à la satisfaction des obligations légales ou pour des besoins d'informations ou à des fin patrimoniales.

Service de Certification : service qui produit des Certificats et, plus généralement, assure leur gestion (fabrication, livraison, révocation, publication, journalisation, archivage) conformément à une politique de certification.

Service de Confiance : un service de confiance est un service électronique qui consiste en :

- la délivrance de certificats de signature électronique, de cachet électronique et d'authentification de site internet ; ou
- la validation des signatures électroniques et des cachets électroniques ; ou
- la conservation des signatures électroniques et des cachets électroniques ;
- l'horodatage électronique ;
- l'envoi recommandé électronique.

L'archivage électronique d'information (autre que la conservation des signatures électroniques et des cachets électroniques) n'est pas considéré comme un service de confiance au sens du règlement [eIDAS]. Toutefois, étant opéré dans des conditions similaires que les services de délivrance de certificats et d'horodatage fournis par le TSP MediaCert, l'archivage électronique sera considéré comme un service de confiance au sein du TSP MediaCert et donc du présent document.

Service d'Horodatage : service qui produit des Contremarques de temps et plus généralement assure leur gestion conformément à une politique d'horodatage.

1.3 Acronymes

Une liste des acronymes employés dans la présente PG est présentée ci-dessous :

- **AC :** Autorité de Certification ;
- **AFNOR :** Association Française de Normalisation ;
- **AH :** Autorité d'Horodatage ;
- **DTPG :** Documentation Technique des Pratiques Générales ;
- **EIDAS :** Electronic IDentification And Signature ;
- **HSM :** Ressource Cryptographique Matérielle (*Hardware Security Module*) ;
- **IGC :** Infrastructure de Gestion de Clés (*Public Key Infrastructure*) ;
- **LCR :** Liste des Certificats Révoqués ;
- **OID :** Object IDentifier ;
- **PC-DPC :** Politique de Certification – Déclaration des Pratiques de Certification ;
- **PH-DPH :** Politique d'Horodatage – Déclaration des Pratiques d'Horodatage ;
- **PA :** Politique d'Archivage ;
- **PCRA :** Plan de Continuité et de Reprise d'Activités ;
- **PG :** Politique Générale du TSP MediaCert ;
- **PGI :** Politique de Gestion des Incidents ;
- **PSI :** Politique de Sécurité de l'Information de Worldline ;
- **RGPD :** Règlement Général pour la Protection des Données ;
- **SAE :** Service d'Archivage Electronique ;
- **SIAF :** Service Interministériel des Archives de France ;
- **SIEM :** Security Information & Event Management ;
- **SOC :** Security Operation Center ;
- **SSI :** Sécurité des Systèmes d'Information ;
- **TSP :** Prestataire de Services de Confiance (*Trust Service Provider*) ;
- **UH :** Unité d'Horodatage.

2 Introduction

2.1 Objet

Le *Trust Service Provider* MediaCert, établi par Worldline, fournit un ensemble de Services de Confiance et est, par conséquent, soumis à un ensemble de réglementations (cf. chapitre 1.1.1) telle que le règlement « eIDAS » n°910/2017 du Parlement européen et du Conseil européen en matière d'identification électronique et de services de confiance pour les transactions électronique au sein du marché intérieur.

Ce document décrit la politique générale du TSP MediaCert. Dans ce cadre, il présente :

- les exigences générales auxquelles est soumis le TSP MediaCert ;
- l'organisation mise en place pour assurer la fourniture des services ;
- les mesures de sécurités générales appliquées.

2.2 Identification du document

Eléments	Valeur
Titre	Politique Générale du TSP MediaCert
Référence document	WLM-TSP-F094
OID	1.2.250.1.111.20.1.1
Version	1.3
Auteur	F. Da Silva

La définition de l'OID du présent document est présentée au chapitre 5.3.2.1.

Ce présent document sera appelé « PG » tout le long du document.

2.3 Structure la Politique Générale

Afin de faciliter l'interopérabilité avec les normes applicables, la présente PG est structurée en accord avec :

- les clauses de la norme [ETSI 319 401] ;
- les principales clauses de la norme [ISO 27002].

3 Périmètre d'application de la Politique Générale

3.1 Périmètre fonctionnel

Comme définit en introduction, ce document décrit la politique générale adoptée et appliquée par l'ensemble des Services de Confiance du TSP MediaCert, qu'importe leur niveau de qualification, conformément au règlement eIDAS.

Parmi les Services de Confiance fournis, figurent notamment :

la délivrance de Certificats de signature électronique et de cachet électronique ;

l'horodatage électronique ;

l'archivage électronique (cf. chapitre 1.2).

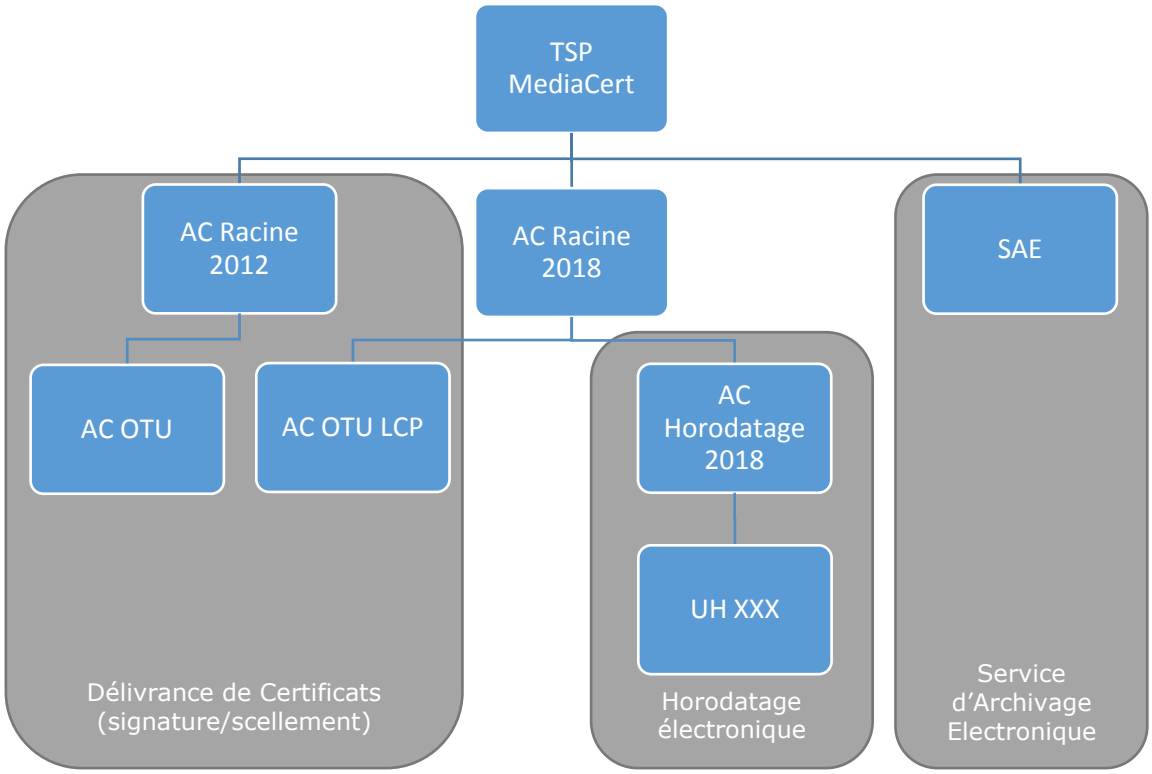

Figure 1 - Périmètre fonctionnel du TSP MediaCert

3.2 Périmètre technique

La présente PG s'applique à l'ensemble du périmètre du TSP MediaCert. Ces composants sont présentés dans la DTPG ainsi que dans la documentation technique spécifique à chaque Service de Confiance du TSP MediaCert.

4 Analyse de risques de sécurité

Dans le cadre des activités du TSP MediaCert, une analyse de risques est réalisée par le responsable sécurité du TSP MediaCert sur le périmètre des Services de Confiance.

Elle a pour objectif de permettre l'identification, l'analyse et l'évaluation des risques SSI fonctionnels et métier, et de permettre la définition de mesures appropriées mises en œuvre pour les traiter, en prenant en compte les résultats de l'évaluation.
Les mesures de traitement du risque permettent de s'assurer que le niveau de sécurité mis en œuvre est proportionné vis-à-vis des risques pesant sur le SI.
Elle permet d'assurer la cohérence de la DTPG (cf. chapitre 5.4) au regard du niveau de risque, en déterminant toutes les exigences de sécurité et les procédures opérationnelles nécessaires.

Ce document permet notamment d'identifier la dépréciation des algorithmes, les actifs et leurs besoins en termes de sécurité applicables aux systèmes du TSP MediaCert. Il tient compte de l'état de l'art en la matière et fait l'objet d'une révision régulière, à minima une (1) fois par an, et en cas d'évolution majeure des infrastructures ou des services. Elle est validée par le Comité MediaCert, qui accepte les risques résiduels exposés, suite à sa révision régulière (cf. chapitre 6.7).

Dans le cas d'un service qualifié, le TSP MediaCert procédera à l'homologation du service suivant les préconisations de l'ANSSI [Qualification ANSSI] préalablement à la fourniture du Service de Confiance qualifié. Cette homologation est revue tous les deux (2) ans.

L'analyse de risque permet également d'identifier les données sensibles. À ce titre, elles font l'objet de mesures de sécurité spécifiques pouvant porter sur la sauvegarde, la journalisation, les accès, etc.

5 Politiques et Pratiques

5.1 Gestion de la documentation du TSP MediaCert

5.1.1 Entité gérant la documentation du TSP MediaCert

Worldline est responsable de l'élaboration, de l'approbation, du suivi et de la révision, dès que nécessaire, de la documentation du TSP MediaCert. À cette fin, un comité appelé « Comité MediaCert » est mis en place comme défini au chapitre 6.7 du présent document.
En particulier, pour chaque Service de confiance opéré par MediaCert, une politique du service de confiance, ainsi que des pratiques supportant cette politique sont élaborés et documentées.
Le présent document définit et documente les exigences et pratiques communes à l'ensemble des services de confiance de MediaCert, des exigences et pratiques complémentaires spécifiques sont détaillées dans la documentation spécifique à chacun des Services de confiances.

Parmi la documentation du TSP MediaCert concernée, on trouve notamment les :

- la présente Politique Générale ;
- Politique de Certification – Déclaration des Pratiques de Certification ;
- Politique d'Horodatage – Déclaration des Pratiques d'Horodatage ;
- Politique d'Archivage ;
- Analyse des risques.

L'ensemble de ces documents, ainsi que le présent document, font l'objet d'une approbation par le Responsable du TSP MediaCert au cours d'une réunion sécurité du Comité MediaCert. Après approbation, ils sont publiés et communiqués aux employés et aux tiers suivant le besoin d'en connaître (cf. chapitre 5.3.1).

L'ensemble de ces documents font également l'objet d'un processus de révision. Ce processus de révision est déclenché après chaque ajout ou changement majeur d'un Service de Confiance et a minima annuellement. Le processus de révision est sous la responsabilité du Comité MediaCert.

La Politique de Sécurité du Système d'Information (PSSI ou PSI) appliquée par le TSP MediaCert est quant à elle gérée (écriture, révision, approbation, publication) par le Comité Sécurité Worldline France (cf. chapitre 5.5). Par ailleurs, toute modification importante de ladite PSSI entraînant un changement de la présente PG déclenchera une notification à l'ANSSI (cf. chapitre 5.3.1).

5.1.2 Point de contact

Le point de contact habilité pour toute remarque, demande d'information complémentaire, réclamation ou remise de dossier de litige concernant la documentation du TSP MediaCert est :

Comité MediaCert
Worldline
23 rue de la Pointe
Zone Industrielle A
59113 SECLIN
France
dl-mediacert-tsp@worldline.com

5.1.3 Entité déterminant la conformité d'une déclaration des pratiques avec la politique qui lui est associée

La cohérence d'une déclaration des pratiques avec la politique qui lui est associée est déterminée par le Comité MediaCert lorsqu'il valide la politique.

La cohérence d'une documentation technique avec la politique qui lui est associée est déterminée par le Comité MediaCert lorsqu'il valide la politique.

5.1.4 Procédure d'approbation de conformité d'une déclaration des pratiques avec la politique qui lui est associée

Le processus de vérification de la conformité d'une déclaration des pratiques avec la politique qui lui est associée est garanti par l'unicité du document. Une relecture et une validation sont effectuées par le Comité MediaCert lors de toute modification majeure (cf. chapitre 6.7).
Le Comité MediaCert est responsable de l'implémentation et de l'application effective des pratiques décrites.

La conformité d'une documentation technique avec la politique – déclaration des pratiques qui lui est associée est garantie par le rédacteur de ladite documentation technique. En effet, toute modification d'une documentation technique se fait en parallèle avec la politique – déclaration des pratiques concernée. Une relecture et une validation sont effectuées par le Comité MediaCert lors de toute modification majeure (cf. chapitre 6.7).

En cas de modification importante dans la fourniture de ses Services de Confiance qualifiés, le TSP MediaCert informe l'ANSSI selon les modalités préconisées par celle-ci au sein de [Qualification ANSSI]. En particulier dans les cas suivants (non-limitatifs) :

- les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées ;
- les changements de sous-traitants ;
- les modifications des conditions d'hébergement ;
- les changements de matériels cryptographiques ;
- les modifications d'architecture technique ;
- les changements de procédures d'enregistrement et d'identification ;
- les changements dans la gouvernance des Services de Confiance du TSP MediaCert.

Les modifications entraînant des changements dans la liste de confiance publiée par l'ANSSI sont également notifiées dans les meilleurs délais.
De plus, le TSP MediaCert adresse à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses Services de Confiance qualifiés, impactant les constats présentés dans le rapport d'évaluation de la conformité, à une fréquence annuelle.

5.2 Mise à disposition des informations

5.2.1 Entité chargée de la mise à disposition des informations

Le Comité MediaCert est l'entité qui se charge de mettre à disposition les informations devant être publiées.

5.2.2 Informations devant être mises à disposition

La définition des informations devant être publiées est propre à chaque Service de Confiance et est donc disponible dans les politiques spécifiques aux divers services de confiance.

Cependant, certains éléments font forcément l'objet d'une publication sur le site précisé en 5.2.3 :

- la présente Politique Générale, commune à l'ensemble des Services de Confiance ;
- les CGU de chacun des Services de Confiance.

Les CGU d'un Service de Confiance sont mises à disposition des Utilisateurs et Abonnés avant toute utilisation du service.

5.2.3 Lieu de mise à disposition des informations

Les informations devant être publiées sont mises à disposition sur le site web du TSP MediaCert, disponibles 7j/7 24h/24, dont l'adresse est : https://www.mediacert.com
Ce site web vise une exigence de disponibilité élevée.

5.2.4 Délais et fréquence de publication

Les délais et fréquences de publication des informations sont propres à chaque Service de Confiance du TSP MediaCert et sont donc disponibles dans les politiques concernées, - excepté pour la documentation qui doit être publiée immédiatement, indépendamment du Service de Confiance concerné.

Il est précisé que les versions antérieures des documents contractuels (politiques, conditions générales, …) régissent exclusivement les périodes de temps couvertes par ces versions, soit jusqu'à leur remplacement notifié aux Abonnés. En effet, dès lors qu'une nouvelle version est notifiée aux Abonnés puis publiée, elle aura vocation à s'appliquer immédiatement pour l'avenir, les changements intervenus ne concernant que des précisions rédactionnelles, des modifications liées à l'état de l'art et de la réglementation, sans incidence sur les clauses du contrat liant l'Abonné au TSP MediaCert mais nécessaires pour le suivi qualitatif des prestations de confiance. Si toutefois elles devaient avoir une incidence sur l'économie du contrat liant l'Abonné au TSP MediaCert, les parties se reporteront aux modalités prévues dans les conditions générales applicables.

5.2.5 Contrôle d'accès aux informations mises à disposition

L'ensemble des informations publiées sur le site web du TSP MediaCert est accessible aux utilisateurs en lecture. De plus, les documents déposés sur ce site web font l'objet d'une signature électronique afin d'en certifier l'authenticité.

L'accès en modification des informations publiées sur le site web du TSP MediaCert est strictement limité aux fonctions d'administration internes habilitées. Le contrôle d'accès est effectué par des serveurs dédiés à cette fonction.

Par ailleurs, des mesures supplémentaires spécifiques à des Services de Confiance peuvent être mises en place, comme définies dans les sous-chapitres suivants.

5.2.5.1 Services de Certification

L'accès en modification aux systèmes de publication des informations sur l'état des Certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions habilitées du TSP MediaCert et se fait à travers une authentification forte sur des serveurs dédiées au contrôle d'accès.

5.2.5.2 Services d'Horodatage

Les Services d'Horodatage ne font pas l'objet de mesures supplémentaires autres que celles décrites au chapitre 5.2.5.

5.2.5.3 Services d'Archivage

Les Services d'Archivage ne fait pas l'objet de mesures supplémentaires autres que celles décrites au chapitre 5.2.5.

5.3 Amendements à la PG, aux PC-DPC, aux PH-DPH et à la PA

5.3.1 Procédures d'amendements

Le Comité MediaCert procède régulièrement à la révision des documents dont il a la charge.

Lors de l'amendement de l'un de ces documents, celui-ci procède généralement à une relecture puis à une validation dudit document. L'approbation de l'amendement est quant à elle sous la responsabilité du Responsable du TSP MediaCert qui n'effectue aucune modification documentaire. L'ensemble des actions susvisées étant réalisé au cours d'une réunion du Comité MediaCert. Les Abonnés et Utilisateurs concernés sont préalablement notifiés des amendements par les acteurs du Comité MediaCert.

Cependant, des amendements aux documents révisés ne sont pas toujours nécessaires. En effet, les modifications de forme (orthographe, …) ou les clarifications rédactionnelles ne sont pas soumises à validation et les documents soumis à une notification préalable aux Abonnés et Utilisateurs peuvent alors être mis à jour sans que la notification soit effectuée.

En cas de changement majeur de ces documents, les entités suivantes pourront également être notifiées du changement :

- l'organisme en charge de l'évaluation de la conformité ;
- l'ANSSI, en tant qu'organisme national de contrôle des Services de Confiance ;
- le SIAF, en tant qu'organisme national de contrôle des archives de France.

5.3.2 Gestion des OID

5.3.2.1 Construction de l'OID

L'OID des documents du TSP MediaCert est basé sur l'OID « **1.2.250.1.111** » attribué par l'AFNOR à Worldline et est construit comme suit : 1.2.250.1.111.**x**.**y**.**z**.**w** où :

- **x** : activité Worldline. Ici il s'agit du TSP MediaCert (Prestataire de Services de Confiance → 20) ;

- **y** : numéro attribué à la politique du Service de Confiance concerné ;
- **z** : numéro majeur de la version du document (ex : v3.1 → 3) ;
- **w** : spécifique à chaque Service de Confiance.

5.3.2.2 Circonstances selon lesquelles l'OID doit être changé

Si le Comité MediaCert estime qu'une modification de ces documents a un impact sur le niveau de sécurité ou sur le niveau de confiance au Service de Confiance concernée, il pourra définir une nouvelle version du document et lui attribuer alors un nouvel OID.

Si l'OID du présent document est amené à évoluer, le Comité MediaCert prendra en compte cette évolution au sein des documents référents (PC-DPC, PH-DPH, PA, …).

5.4 Documentation Technique des Pratiques Générales

Le TSP MediaCert possède une Documentation Technique des Pratiques Générales pour son propre usage. Ce document détaille les mesures de sécurité et légales communes aux différents Services de Confiance mis en place par Worldline. Ces mesures peuvent être d'ordre organisationnel, fonctionnel ou bien technique.

5.5 Politiques de sécurité de l'information applicables

Les mesures définies dans la Politique de Sécurité de l'Information Worldline sont appliquées sur le périmètre du TSP MediaCert et ce lors de toutes les phases de son cycle de vie. Cette politique définit les objectifs en matière de disponibilité, d'intégrité et de confidentialité de l'information à travers une série de règles de sécurité. Elle démontre l'engagement de Worldline envers la sécurité de l'information. Il faut la considérer comme une référence pour toutes les décisions relatives à la sécurité. Celle-ci s'appuie notamment sur des référentielles sécurités reconnus tels que la norme [ISO 27001] et le guide de l'hygiène informatique de l'ANSSI [Hygiène] pour le niveau standard.

Des mesures de sécurité de l'information spécifiques à chaque Service de Confiance peuvent être définies dans les documentations techniques concernées afin de répondre à leurs besoins de sécurité spécifiques.

Le TSP MediaCert s'assure que la PSI Worldline est documentée et maintenue par Worldline et implémentée sur le périmètre de l'ensemble des Services de Confiance. Cela inclut la responsabilité de la mise en place des contrôles de sécurité et des procédures opérationnelles pour l'ensemble des sites, des systèmes, des informations et des biens participant à la fourniture du Service de Confiance. La PSI Worldline est publiée et est communiquée à l'ensemble des employés impactés par son périmètre.

Le Comité MediaCert est responsable de la bonne application de la PSI Worldline sur l'ensemble des Services de Confiance. En particulier, le Comité MediaCert s'assure de sa bonne application même en cas de sous-traitance d'une fonction d'un Service de Confiance à un tiers. Pour ce faire, en cas de sous-traitance, le TSP MediaCert définit, le cas échéant, les responsabilités de ses sous-traitants et s'assure que les sous-traitants se soumettent à l'ensemble des contrôles nécessaires (cf. chapitre 6.6) ainsi qu'à l'obligation de formation de ses employés (cf. chapitre 7.3 et 7.4).

Les mesures de sécurité appliquées sur les Services de Confiance sont définies et validées par le Comité MediaCert. Elles sont révisées régulièrement et en cas d'évolution majeure, en particulier en cas d'évolution ayant un potentiel impact sur la conformité, l'adéquation ou l'efficacité du

service. Tout changement impactant le niveau de sécurité doit faire l'objet d'une approbation par le Comité MediaCert.

6 Organisation de la gestion des Services de Confiance

6.1 Fonctions et responsabilités liées aux Services de Confiance

Le TSP MediaCert définit explicitement les rôles de confiance requis pour assurer le fonctionnement et la sécurité de celle-ci. Les définitions des rôles de confiance sont rendus disponibles à l'ensemble des personnels concernés.
Les fonctions opérées sur toutes les composantes des services du TSP MediaCert sont réparties sur plusieurs types d'intervenants afin de veiller à la séparation des connaissances pour les tâches ou rôles sensibles. Les rôles de confiance intervenants dans l'organisation du TSP MediaCert sont les suivants :

- Administrateur HSM : il est en charge des installations et configurations des boîtiers cryptographiques (HSM) du TSP MediaCert ;
- Administrateur système : il est en charge des installations, configurations et maintenances des systèmes de confiance du TSP MediaCert pour la gestion des services. Il est autorisé à effectuer la restauration de ces systèmes ; Il joue également le rôle d'opérateur système en étant notamment responsable de l'exploitation quotidienne des systèmes de confiance du TSP MediaCert.
- Auditeur système : il est autorisé à consulter les archives et l'ensemble des journaux d'évènements des systèmes de confiance du TSP MediaCert ;
- Maître de cérémonie : il est en charge de gérer la préparation et le déroulement des cérémonies de clés ;
- Officier de sécurité : il est en charge d'administrer l'implémentation des pratiques de sécurité et d'appliquer les contraintes techniques définies dans l'analyse de risque ;
- Opérateur d'enregistrement : il est chargé d'intervenir dans le processus de création de Certificats ;
- Porteur de secrets : il assure la confidentialité, l'intégrité et la disponibilité des secrets. Il est dépositaire des secrets et des clés physiques d'accès à leurs coffres. Il est membre d'une équipe dont l'ensemble des membres dispose des mêmes droits sur les accès aux coffres ;
- Responsable d'application : il est en charge d'assurer le suivi du service et de ses performances. Il coordonne et/ou réalise la maintenance corrective et évolutive de l'application ;
- Responsable du TSP MediaCert : il est en charge de la mise en œuvre de la présente PG, des PC-DPC et des PH-DPH ainsi que de la vérification de leur application. Il est notamment en charge de la révocation d'un Certificat émis par les AC du TSP MediaCert. Membre du Comité MediaCert, il est aussi en charge de l'approbation du présent document, des politiques (PC-DPC, PH-DPH et PA) et des analyses de risques du TSP MediaCert ;
- Responsable adjoint du TSP MediaCert : il est en charge des mêmes fonctions supportées par le Responsable du TSP MediaCert ;
- Responsable sécurité : il est en charge de la définition des règles de sécurité autour du TSP MediaCert.

Lors de l'enrôlement d'un nouveau membre dans un rôle de confiance au sein du TSP MediaCert, un document actant de sa désignation doit être signé par la personne concernée, pour acceptation du rôle, par la responsable des ressources humaines et par le responsable du TSP MediaCert ou l'un de ses adjoints. Ce document fait référence à la DTPG afin que le futur membre du personnel de confiance ait connaissance de la description de son rôle et des responsabilités qui lui sont affectées. Il spécifie notamment :

- les engagements du signataire et leur bonne compréhension ;
- en cas de modification du document DTPG, le signataire en sera informé.

De même, lors de la cessation d'un rôle de confiance au sein du TSP MediaCert, un document actant de la cessation doit être signé par la personne concernée.

6.2 Nombre de personnes requises

6.2.1 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et les rôles des personnes devant être présentes, en tant qu'acteurs ou témoins, peut être différent. En effet, certaines tâches sensibles, telle que la génération du Certificat d'une AC, nécessitent plus d'une personne occupant un rôle de confiance au sein du TSP MediaCert pour des raisons de sécurité.

6.2.2 Nombre de personnes requises par rôles

Certains rôles de confiances sont occupés par plusieurs personnes pour que le TSP MediaCert puisse assurer la continuité de ses services sans dégrader la sécurité des services offerts.

Il est régulièrement vérifié que l'ensemble des rôles de confiance définis ci-dessus sont pourvus.

6.3 Identification et authentification pour chaque rôle

Chaque personnel en rôle de confiance est clairement identifié par le TSP MediaCert au travers d'un inventaire des rôles.

Chaque entité opérant une composante d'un service du TSP MediaCert vérifie, pour chacun de ses composants, l'identité et les autorisations de tout membre du personnel ainsi que d'éventuelles personnes extérieures intervenant sur les tâches sensibles.

Avant d'utiliser une application critique contribuant à un Service de Confiance, tout personnel est obligatoirement identifié et authentifié au préalable. Toutes les opérations réalisées sur les systèmes par les personnels font l'objet d'une traçabilité (cf. chapitre 12.5) garantissant l'imputabilité des actions.

Chaque attribution d'un rôle de confiance à un membre du personnel du TSP MediaCert est notifiée et documentée par écrit.

6.4 Séparation des rôles

Il est autorisé par la présente PG que plusieurs rôles soient opérés par une même personne. Cependant, dans le cadre des activités du TSP MediaCert et pour des raisons de sécurité, certains rôles ne peuvent pas être opérés par la même personne. La séparation des rôles identifiés ci-dessus est spécifiée dans le DTPG.

De façon générale, les rôles et responsabilités sont attribués sur le principe du moindre privilèges afin de limiter le risque de conflit d'intérêt et limiter les opportunités de réalisation d'actions non autorisées ou de mauvaise utilisation des biens mis en œuvre par le Service de Confiance.

6.5 Relations avec les autorités

Les relations avec les autorités légales et réglementaires sont assurées par les responsables du TSP MediaCert tels que définis au chapitre 6.1 du présent document, en s'appuyant au besoin sur les différentes directions adéquates de Worldline (direction administrative et juridique, …).

Ils ont notamment la responsabilité de la notification aux autorités compétentes en cas d'incident de sécurité comme spécifié dans la DTPG.

6.6 Relations avec les fournisseurs

La PSI Worldline définit les mesures à appliquer aux fournisseurs afin de garantir l'application d'un niveau de sécurité au moins équivalent à celui définit dans la PSI Worldline, pour les activités qui leur sont confiées. Les mesures intègrent les notions de formation et de contrôle.

Les relations avec les fournisseurs externes sont systématiquement formalisées à travers un accord contractuel avec le fournisseur. Cet accord précise les responsabilités de chacun.

En tout état de cause, le TSP MediaCert, en amont, évalue les risques spécifiques à l'infogérance (maîtrise du système d'information, actions à distance, hébergement mutualisé, etc.) afin de prendre en compte, dès la rédaction des exigences applicables au futur prestataire, les besoins et mesures de sécurité adaptés.
Le TSP MediaCert exige de ses prestataires externes un plan d'assurance sécurité (PAS) formalisant ses engagements ou impose des exigences de sécurité adéquates dans le contrat de service.

6.7 Instances de gouvernance

Le TSP MediaCert met en place une unique instance de gouvernance appelée « Comité MediaCert » dont les missions sont multiples (validation de la documentation, révision des analyses de risques, …). Les personnes présentes lors des réunions de ce comité diffèrent en fonction du sujet de la réunion. Cependant, le responsable du TSP MediaCert, ou l'un de ses adjoints, est systématiquement présent. Le détail est disponible au sein de la DTPG associée.

6.8 Indépendance des parties et non-discrimination

L'organisation mise en place dans le cadre du TSP MediaCert, dédiée à ses activités avec une étanchéité des rôles, permet de préserver l'impartialité des opérations. Par ailleurs, le TSP MediaCert assure que les activités de confiance fournies sont pratiquées de façon équivalente pour l'ensemble des bénéficiaires ayant accepté les conditions du service et respectant les obligations qui leur incombent.

Dans la mesure de ses possibilités, le TSP MediaCert mettra en œuvre des approches appropriées pour rendre son service accessible à toute personne en situation de handicap, en prenant en compte au cas par cas les spécificités de chaque demandeur.

D'une manière générale, les services fournis par le TSP MediaCert tels que la génération de Certificats, la gestion de la révocation de Certificats, l'archivage électronique ou encore l'émission de Contremarques de temps sont exercés de façon indépendante et ne sont donc sujets à aucune

éventuelle pression commerciale qui pourrait nuire à l'éthique et à la déontologie de ces services de confiance fournis par le TSP MediaCert. Ceci est garanti par le fait que le TSP MediaCert est centralisé au sein d'une *Global Business Line*, une unité transversale aux autres unités de Worldline (cf. Figure 2 - Schéma organisationnel).

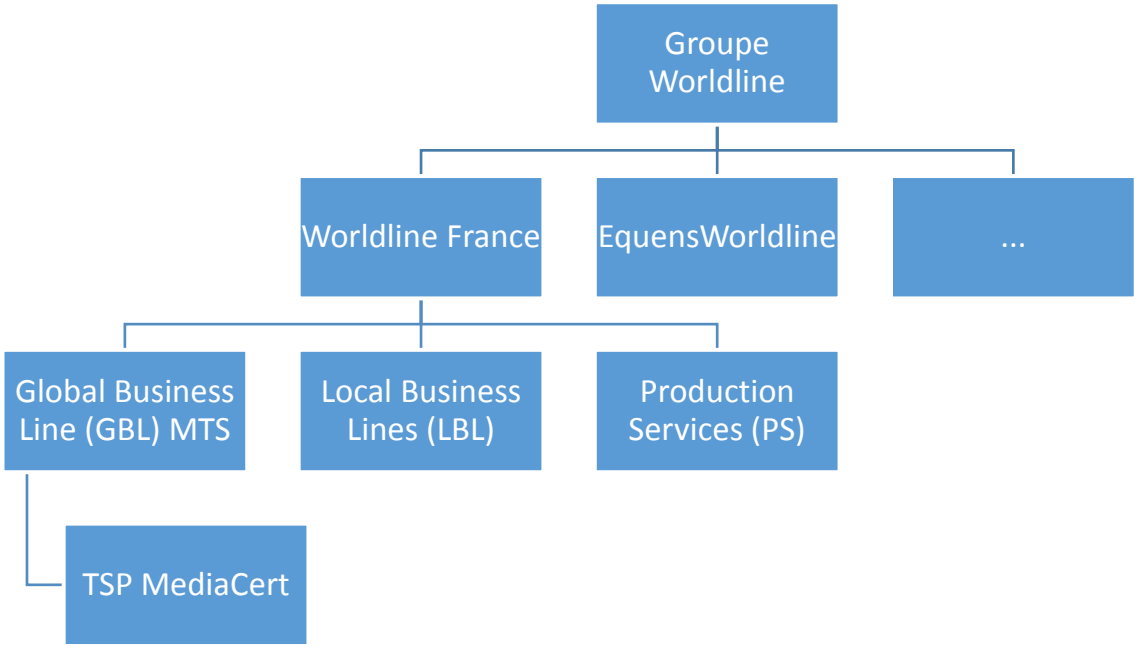

Figure 2 - Schéma organisationnel

7 Sécurité liée aux ressources humaines

Le TSP MediaCert met en place une politique de ressource humaine contribuant à la confiance dans les opérations du service de confiance. En particulier, le TSP MediaCert met en œuvre les moyens légaux à sa disposition pour s'assurer de l'honnêteté des personnels impactant les services de confiance.

De plus, les droits et les accès au système d'information sont mis à jour en fonction des évolutions des personnels (arrivée, départ, changement d'affection). En particulier, l'ensemble des droits affectés à une personne sont révoqués lors de son départ ou en cas de changement de fonction. Les procédures d'arrivée et de départ sont définies, en lien avec la fonction ressources humaines. Elles prennent en compte :

- la création et la suppression des comptes informatiques et boîtes aux lettres associées ;
- les droits et accès à attribuer et retirer à une personne dont la fonction change ;
- la gestion des accès physiques aux locaux (attribution, restitution des badges et des clés, etc.) ;
- l'affectation des équipements mobiles (ordinateur portable, clé USB, disque dur, smartphone, etc.) ;
- la gestion des documents et informations sensibles (transfert de mots de passe, changement des mots de passe ou des codes sur les systèmes existants).

Ces procédures sont formalisées.

7.1 Qualification, compétences et habilitations requises

Le TSP MediaCert emploie des personnels et, le cas échéant, des fournisseurs possédant l'expérience, les compétences, les qualifications et l'expertise nécessaire aux opérations d'un Service de Confiance.

Le personnel opérant des rôles de confiance au sein du TSP MediaCert est informé de ses responsabilités ainsi que des procédures liées à la sécurité des systèmes et au contrôle du personnel auxquelles il doit se conformer.

Le personnel d'encadrement est formé et sensibilisé à la sécurité et à la gestion des risques, sont familiers des procédures de sécurité en place et ont une expérience de la sécurité informatique suffisante pour assumer pleinement ses responsabilités vis-à-vis des services fournis par le TSP MediaCert.
Les procédures administratives et d'encadrement des personnels sont conçues et maintenues en ligne avec les procédures de gestion de la sécurité de l'information.

Le TSP MediaCert s'assure de la qualification et de la compétence de son personnel opérant un rôle de confiance.

7.2 Procédures de vérification des antécédents

Des procédures de vérification des antécédents judiciaires sont mises en place pour les personnes qui sont appelées à endosser un rôle de confiance au sein du TSP MediaCert. Ces personnes ne doivent notamment pas avoir fait l'objet de condamnation judiciaire susceptible de compromettre

leur participation aux activités du TSP MediaCert, ni être en situation de conflit d'intérêt avec leurs attributions. Pour cela, les personnes concernées doivent remettre une copie du bulletin n°3 de leur casier judiciaire aux Ressources Humaines de Worldline lors de la signature du document (cf. chapitre 6.1) par lequel ils acceptent leur rôle, leurs obligations et leurs responsabilités dans le cadre de leur participation à ces activités. Ils sont notamment chargés de communiquer tout changement dans ce domaine. Toutefois, le TSP MediaCert met en place une vérification régulière de l'adéquation des antécédents judiciaires de ses membres avec le rôle qu'ils opèrent pour son compte.

Le dossier de candidature du postulant est soumis à la validation du service Ressources Humaines et à celle du responsable du TSP MediaCert (cf. chapitre 6.3). Aucun droit d'accès n'est attribué tant que le dossier n'est pas validé.

Les personnels chargés d'opérer les services de confiance du TSP MediaCert ne sont pas chargés des aspects commerciaux liés à ces services et sont dégagés de tout conflit d'intérêts qui pourraient influencer la manière de mener les opérations dont ils sont chargés et obérer la confiance (cf. chapitre 6.8). A cet égard, ils s'engagent à confirmer par écrit, lors de leur acceptation du rôle de confiance au sein du TSP MediaCert, l'absence de tout conflit d'intérêt lié à l'exercice de cette nouvelle activité.
Tout personnel ayant une situation connue du TSP MediaCert pouvant engendrer conflit d'intérêt jugé incompatible ou pouvant porté préjudice à l'impartialité des opérations de service de confiance :

- ne pourra se voir attribuer un rôle de confiance ;
- pourra se voir retirer un rôle de confiance précédemment attribué.

7.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement du TSP MediaCert. Il est également sensibilisé à la sécurité de l'information et en particulier :

- aux enjeux de sécurité ;
- aux règles à respecter ;
- aux bons comportements à adopter en matière de sécurité des systèmes d'information.

Ce personnel a pris la mesure et la connaissance de ce qu'impliquent les opérations dont il a la responsabilité.

L'ensemble des personnels de confiance reçoit une formation concernant typiquement :

- la sécurité et la protection des données personnelles ;
- la législation en vigueur ;
- les principaux risques et menaces ;
- le maintien en condition de sécurité ;
- l'authentification et le contrôle d'accès ;
- le paramétrage fin et le durcissement des systèmes ;
- le cloisonnement réseau ;

- la journalisation.

Cette formation est éventuellement adaptée suivant le service et le poste occupé. Elle peut prendre la forme d'une formation théorique, d'une formation pratique à travers un accompagnement de personnels déjà formés ou d'une combinaison des deux.

7.4 Exigences et fréquences en matière de formation continue

Le personnel reçoit la formation nécessaire préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation ou autres en fonction de la nature de ces évolutions. Il est notamment formé sur les enjeux en matière de sécurité des systèmes d'information et sensibilisé au traitement des incidents.

En particulier, les personnes reçoivent des formations régulières afin de maintenir leur niveau d'expertise, de connaissance et de qualifications.

De plus, des actions de sensibilisation destinées à l'ensemble des personnels sont régulièrement mises en œuvre. Celles-ci abordent des sujets tel que :

- les objectifs et enjeux que rencontre le TSP MediaCert en matière de sécurité des systèmes d'information (nouvelles menaces et pratiques courantes de sécurité) ;
- les informations considérées comme sensibles ;
- les réglementations et obligations légales ;
- les règles et consignes de sécurité régissant l'activité quotidienne : respect de la politique de sécurité, non-connexion d'équipements personnels au réseau de l'entité, non-divulgation de mots de passe à un tiers, non-réutilisation de mots de passe professionnels dans la sphère privée et inversement, signalement d'événements suspects, etc. ;
- les moyens disponibles et participant à la sécurité du système : verrouillage systématique de la session lorsque l'utilisateur quitte son poste, outil de protection des mots de passe, etc.

7.5 Fréquence et séquence de rotation entre différentes attributions

Il n'y a pas de rotation définie dans le cadre de la présente PG entre les différentes attributions.

7.6 Sanctions en cas d'actions non-autorisées

Le règlement intérieur de Worldline indique que des sanctions disciplinaires administratives appropriées sont applicables en cas de faute (non-respect de la présente PG, …). Ceci est notamment rappelé au personnel dans l'engagement de responsabilités qu'il accepte lors de l'acceptation de son rôle au sein du TSP MediaCert.

Les entités externes à Worldline et participantes aux activités du TSP MediaCert s'exposent à des sanctions définies lors de la contractualisation en cas de faute (non-respect de la présente PG, …).

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

Le personnel des éventuels prestataires externes intervenant dans les locaux et/ou sur les composantes du TSP MediaCert doit respecter les exigences énoncées dans les chapitres 7.1 à 7.4 du présent document.

7.8 Documentation fournie au personnel

Chaque personne dispose au minimum de la documentation relative aux procédures opérationnelles et aux outils spécifiques qu'il met en œuvre, ainsi que des politiques et pratiques générales de la composante du service au sein duquel il travaille.

8 Gestion des actifs

8.1 Responsabilités relatives aux actifs

Conformément aux règles définies dans la PSI Worldline, le TSP MediaCert :

- inventorie régulièrement l'ensemble des actifs des Services de Confiance qu'il fournit ;
- désigne un propriétaire/responsable des actifs concernés.

8.2 Classification de l'information

Les données du TSP MediaCert sont classifiées selon la Politique de Classification des Données Worldline. Par ailleurs, celui-ci suit les règles de manipulation des informations en fonction de leur sensibilité comme définies dans le Standard de protection des informations de Worldline.

Cette classification de l'information découle de l'analyse de risque et est maintenue en accord avec les résultats de celle-ci (cf. chapitre 4).

Cette classification permet de mettre en œuvre un niveau de protection adéquat. L'ensemble des biens sont manipulés en conformité avec ce document de classification de l'information et les procédures associées. En particulier, des mesures de fin de vie sont mises en places afin que les biens en fin de vie contenant des informations sensibles puissent être détruits ou décommissionnés en toute sécurité (cf. chapitre 11.5).

9 Contrôle d'accès

9.1 Accès physique

Les sites et locaux qui accueillent le TSP MediaCert garantissent la sécurité physique des moyens mis en œuvre pour fournir les Service de Confiance. L'ensemble des moyens mis en place pour s'assurer de cela est spécifié dans la DTPG.

Des mesures de contrôle d'accès physiques sont mis en places afin que les systèmes critiques des services de confiances ne puissent être accéder par des personnes non-autorisées. Ces mesures de contrôle permettent de minimiser les risques associés à la sécurité physique des biens. En particulier :

- les composants critiques[1] sont isolés dans des périmètres de sécurité clairement définis ne sont accessibles qu'aux personnes autorisées ;
- les périmètres de sécurité font l'objet de mesures de protection physique contre les intrusions, de mesures de contrôle d'accès et d'alarmes en cas d'intrusion ;
- des mesures sont en place pour éviter le vol, la destruction ou la compromission des composants, ainsi que l'interruption de service ;
- des mesures sont en place contre la compromission ou le vol d'informations sensibles ;
- des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services du TSP MediaCert soient sortis du site sans autorisation.

9.2 Accès logique

Les accès logiques aux serveurs, aux outils de développement collaboratifs et aux applications du TSP MediaCert sont contrôlés et régulièrement vérifiés (cf. chapitre 9.4).

9.3 Accès réseau

Les mesures de contrôles d'accès aux réseaux sont présentées au chapitre 13.1 du présent document. Les connexions d'équipements personnels sont notamment interdites sur le réseau du TSP MediaCert.

9.4 Gestion des droits d'accès

Le TSP MediaCert met en place une gestion des droits d'accès sur la base du principe de moindre privilège et procède régulièrement à une revue de l'attribution de ces droits d'accès.

Cette gestion des droits d'accès aux systèmes et informations du TSP MediaCert est interne et est spécifiée dans le document DTPG.

[1] La criticité est définie par la classification de l'information découlant de l'analyse de risque.

9.5 Gestion des comptes, mots de passe et sessions

Des règles de gestion des comptes, des mots de passe et sessions d'accès aux systèmes du TSP MediaCert sont en place afin de garantir une robustesse minimum des informations d'identification et une protection minimale des accès aux systèmes.

Ces règles sont internes et sont spécifiées dans le document DTPG.

10 Mesures cryptographiques

Des mesures de sécurité appropriés et des procédures de contrôle sont mises en place pour la gestion des clés cryptographiques et des modules cryptographiques (HSM) tout au long de leur cycle de vie.

10.1 Standards et mesures de sécurité pour les modules cryptographiques

Les HSM utilisés par le TSP MediaCert, pour la génération des Bi-clés d'AC, d'UH et celles correspondants aux différents Certificats délivrés par les AC, sont des HSM répondant aux exigences définies dans les politiques associées à chaque service de confiance concernées.

Ces HSM sont dédiés aux services fournis par le TSP MediaCert.

Le TSP MediaCert s'assure de la sécurité des HSM qu'elle utilise tout au long de leur cycle de vie. Des procédures sont notamment mises en place pour :

- s'assurer de l'intégrité de ces HSM durant leur transport ;
- s'assurer de l'intégrité de ces HSM durant leur stockage ;
- s'assurer de l'intégrité de ces HSM durant leur fonctionnement ;
- s'assurer du bon fonctionnement de ces HSM.

Pour les services qualifiés au sens du Règlement eIDAS, le TSP MediaCert utilise exclusivement des HSM ayant fait l'objet d'une qualification au niveau renforcé par l'ANSSI.

10.2 Gestion des Bi-clés

10.2.1 Générations des Bi-clés

10.2.1.1 Bi-clés d'AC et d'UH

La génération des Bi-clés d'AC ou d'UH est réalisée au cours d'une Cérémonie de clés. Ces cérémonies de clés se déroulent :

- à l'aide d'un HSM physiquement isolé répondant aux exigences définies au chapitre 10.1 du présent document ;
- dans les locaux sécurisés du TSP MediaCert (cf. chapitre 11) ;
- sous le contrôle permanent d'au moins deux (2) personnes occupant un rôle de confiance au sein du TSP MediaCert parmi : le porteur de secrets, le maître de cérémonie, l'administrateur HSM et le responsable d'application (cf. chapitre 6.1) ;
- suivant un document organisationnel et un document technique tous deux signés par l'ensemble des participants, notamment par le maître de cérémonie.

La clé privée de chaque AC et UH est mise en œuvre et reste dans les locaux sécurisés du TSP MediaCert.

10.2.1.2 Bi-clés d'authentification d'une composante d'un service du TSP MediaCert

Les Bi-clés d'authentification d'une composante d'un service du TSP MediaCert sont générées lors d'une Cérémonie de clés. Cela peut être effectué en même temps que pour les clés d'AC ou d'UH. Cette cérémonie se déroule dans les mêmes conditions que celles décrites au chapitre 10.2.1.1 ci-dessus.

10.2.1.3 Autres

Chaque service du TSP MediaCert peut définir ses propres besoins en termes de génération de Bi-clé pour d'autres usages en conformité avec les exigences cryptographiques applicables.

10.2.2 Transmission de la clé publique aux utilisateurs

Le moyen de transmission de la clé publique aux Utilisateurs est propre à chaque service du TSP MediaCert. Cette information se trouve donc dans les politiques associées à chaque service de confiance.

10.2.3 Taille et algorithme des Bi-clés

La taille des Bi-clés et les algorithmes utilisés par le TSP MediaCert sont conformes aux exigences [ETSI 119 312], aux exigences [RGS B1] ainsi qu'aux recommandations de l'ANSSI [SOGIS_CRYPTO].

10.2.4 Contrôle de la clé privée

Le contrôle des clés privées d'AC, des copies de sauvegarde correspondantes et des clés privées d'UH est assuré par du personnel de confiance : porteur de secrets et administrateur HSM (cf. chapitre 6.1) ; dans un environnement protégé. Ce contrôle est assuré à l'aide de données d'activations, appelées « secrets », réparties entre plusieurs personnes identifiés dans le rôle de porteur de secrets.

10.2.5 Séquestre de la clé privée

Le TSP MediaCert ne propose pas de service de séquestre des clés privées à des fins de recouvrement.

10.2.6 Copie de secours de la clé privée

Cette opération est réalisée sous le contrôle de plusieurs personnes au cours d'une Cérémonie de clés. En effet, les sauvegardes des clés privées sont réalisées dans les mêmes conditions que celles présentées au chapitre 10.2.1.1.

Les procédures de sauvegardes sont opérées selon les spécifications du fournisseur des HSM du TSP MediaCert.

Le nombre de copies est limité au minimum requis pour assurer la continuité des services du TSP MediaCert.

10.2.7 Archivage de la clé privée

Le TSP MediaCert ne propose pas de service d'archivage des clés privées.

10.2.8 Transfert de la clé privée vers/depuis le module cryptographique

Les clés privées d'AC sont générées au sein d'un HSM (cf. chapitre 10.2.1.1) et ne sont transférées vers un autre HSM uniquement dans le cas des copies de sauvegarde (cf. chapitre 10.2.6).

Lors d'un transfert, la clé privée est chiffrée avec un algorithme préconisé par le constructeur de HSM permettant d'assurer la sécurité de l'information. La clé privée chiffrée ne peut alors pas être déchiffrée sans l'utilisation de composants cryptographiques matériels et sans l'action des personnes identifiées dans les rôles de confiances nécessaires.

10.2.9 Stockage de la clé privée

Les clés privées d'AC et d'UH sont stockées au sein d'un HSM physiquement sécurisé répondant aux exigences définies au chapitre 10.1 du présent document. Il en est de même pour le stockage des copies de sauvegarde des clés privées d'AC.

Des procédures autour de ces HSM sont en place afin de s'assurer de la confidentialité de leur contenu.

10.2.10 Méthode d'activation de la clé privée

Les clés privées d'AC ne peuvent être activées qu'avec des données d'activation détenues par deux (2) personnes occupant un rôle de confiance au sein du TSP MediaCert.

L'activation d'une clé privée d'AC ne peut se faire qu'au cours d'une Cérémonie de clés, documentée et tracée.

10.2.11 Méthode de désactivation de la clé privée

La désactivation des clés privées d'AC dans le HSM est automatique dès qu'il y a arrêt de celui-ci.

10.2.12 Méthode de destruction des clés privées

Les clés privées d'AC, les copies de sauvegarde correspondantes et les clés privées d'UH sont détruites par effacement sur la ressource cryptographique conformément aux procédures du constructeur. Les opérations de destruction sont effectuées au cours d'une procédure auditée de type Cérémonie de clés.

En fin de vie normale ou anticipée (pour cause de révocation) d'une clé privée d'AC ou d'UH, celle-ci est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer. Par ailleurs, dans le cas où la ressource cryptographique matérielle hébergeant les clés privées susvisées doit être mise hors service, alors celles-ci le sont aussi.

10.3 Données d'activation des clés privées d'AC

10.3.1 Génération et installation

Les données d'activation des clés privées d'AC sont générées dans un HSM durant les cérémonies de clés sous le contrôle de deux (2) personnes dans des rôles de confiance, stockées sur des

cartes à puces puis sont remises aux porteurs de secrets qui détiennent alors les données d'activation (cf. chapitre 10.2.10). Ces données d'activations ne sont connues que par les responsables nommément identifiées dans le cadre du rôle de confiance qui leur est attribué.

10.3.2 Protection

Les données d'activation sont protégées par des mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de secret sont responsables de la protection des secrets dont ils ont la responsabilité. Un porteur de secret ne détient pas plus d'une donnée d'activation par AC.

11 Sécurité physique et environnementale

Un ensemble de mesures de sécurité physique est mis en place par le TSP MediaCert afin de garantir que :

- les moyens, systèmes d'informations et données utilisés dans le cadre de la mise en œuvre opérationnelle du TSP MediaCert sont installés dans des locaux sécurisés dont les accès sont contrôlés et réservés aux personnels strictement habilités. Le système de contrôle des accès physiques permet de garantir la traçabilité nominative des accès aux locaux hébergeant les moyens et informations du TSP MediaCert (cf. chapitre 9.1) ;

- la mise en œuvre de ces contrôles permet de respecter la séparation des rôles de confiance telle que prévue dans la présente PG (cf. chapitre 6.4).

Ci-dessous figure un panel de mesures environnementales mises en place afin d'assurer la disponibilité des équipements hébergés ainsi que la continuité des services fournis par le TSP MediaCert. Des précisions sont apportées dans le document DTPG.

11.1 Situation géographique et construction des sites

Les environnements du TSP MediaCert sont installés sur les sites sécurisés de production informatique Worldline européens. Ces sites sont conçus pour héberger des systèmes informatiques et télécom.
Les équipes administratives et opérationnelles du TSP MediaCert opèrent sur les sites Worldline européens.

11.2 Alimentation électrique et climatisation

Un certain nombre de mesures (générateurs de secours, …) sont mis en place afin de prévenir les pannes électriques et de simplifier les interventions de maintenance. De même, des mesures (redondance du système, …) sont mises en place pour parer à des défaillances au niveau du système de climatisation. Ces mesures de prévention sont régulièrement maintenues et testées.

11.3 Vulnérabilité aux dégâts des eaux

Des moyens de surveillances (capteurs, monitoring, …) sont en place pour prévenir les dégâts des eaux. Ces moyens de surveillances sont régulièrement maintenus et testés.

11.4 Prévention et protection incendie

Des mesures de prévention et de lutte contre les incendies (détecteurs, portes coupe-feu, …) sont en place pour prévenir tout risque d'incendie et protéger les systèmes du TSP MediaCert le cas échéant. Ces mesures de prévention et de protection sont régulièrement maintenues et testées.

11.5 Mise hors service des supports

Tous les documents papier contenant des données confidentielles (PIN code, mot de passe, …) devenus inutiles ou obsolètes sont physiquement détruits.

Pour les supports physiques (disque, HSM, …) une procédure spéciale de stockage tampon en vue d'un broyage est mise en place. Cette destruction donne lieu à la production d'un Procès-Verbal.

Notamment, en cas de mise hors service d'un HSM, les clés sont effacées au préalable en s'appuyant sur les fonctions de « zeroization » du HSM.

Les équipements, données, supports et logiciels opérés dans la zone sécurisée ne peuvent être retirés du site sans autorisation.

12 Gestion de l'exploitation

12.1 Mesures de sécurité des systèmes informatiques

12.1.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les exigences minimales de sécurité technique mises en œuvre par le TSP MediaCert répondent aux objectifs suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (cf. chapitre 9.2) ;
- protection du réseau contre tout accès non-autorisé (cf. chapitre 9.3) ;
- gestion des droits des utilisateurs et des comptes (cf. chapitre 9.4 et 9.5) ;
- gestion de sessions d'utilisation : déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur (cf. chapitre 9.5) ;
- fonctions d'audits : non-répudiation, imputabilité et nature des actions effectuées (cf. chapitre 15) ;
- application de procédures de changement pour les actions de livraison, modification et résolution urgente de problèmes logiciels (cf. chapitre 12.2) ;
- protection contre les virus, les logiciels malveillants ou non-autorisés et mises à jour des logiciels (cf. chapitre 12.3) ;
- application de procédures de changement pour toute modification des configurations logicielles (cf. chapitre 12.8) ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent (cf. chapitre 13) ;
- redondance des connexions réseau pour assurer l'accessibilité en cas de panne simple.

Des dispositifs de surveillance, avec enregistrement et alarme automatique, ainsi que des procédures d'audit des paramétrages du système, en particulier des éléments de routage, et des procédures de réaction en cas d'incident sont mis en place.

12.1.2 Niveau de qualification des systèmes informatiques

Le TSP MediaCert utilise des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière à ce que :

- les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;
- seules des personnes autorisées puissent introduire et modifier les données conservées ;
- l'authenticité de ces données puisse être vérifiée.

Les précisions sont apportées si nécessaire dans les politiques associées à chaque service.

12.1.3 Manipulation et sécurité des supports

Les supports employés par le TSP MediaCert sont manipulés de manière sécuritaire, suivant des procédures définies, pour les protéger des dégâts, du vol, de l'accès non-autorisé et de l'obsolescence.

Les mesures adressent particulièrement la réutilisation des supports ayant contenu des informations dans un autre contexte, afin que ces dernières ne puissent être accédées par des personnes non-autorisées.

Les supports contenant des données sensibles sont mis au rebus conformément à ce qui est défini au chapitre 11.5 du présent document.

Les supports de sauvegardes font l'objet de mesures spécifiques décrites en 12.4.1.

12.2 Procédures et responsabilités liées à l'exploitation

Les procédures d'exploitation du TSP MediaCert sont documentées et sont mises à disposition des équipes concernées, en particulier tous les personnels administratifs ou en rôle de confiance pouvant avoir un impact sur la fourniture du Service de Confiance.

Des procédures de suivi des changements sont notamment en places afin de contrôler les déploiements, les mises à jour et les corrections d'urgence des logiciels, ainsi que les modifications des configurations des systèmes impliqués dans la fourniture des Services de Confiance. Le TSP MediaCert s'appuie notamment sur un outil interne à Worldline pour assurer le suivi des changements et des incidents liés à l'exploitation de ses services. L'outil permet de documenter tous les changements opérés.

Le TSP MediaCert s'assure de distinguer les différents environnements de l'environnement de production pour l'ensemble des systèmes des Services de Confiances opérés.

12.3 Protection contre les logiciels malveillants

Le TSP MediaCert met en place un ensemble de solutions dans le but de protéger ses plateformes de production et stations d'administration contre les virus et les logiciels malveillants ou non-autorisés. Ces solutions sont spécifiées dans la DTPG.

12.4 Sauvegardes

12.4.1 Conservation des supports

Dans le cadre des activités du TSP MediaCert, des sauvegardes de nature différente sont effectués. Des mesures sont alors mises en place pour assurer la disponibilité, la confidentialité et l'intégrité des supports de sauvegarde utilisés. Ces mesures sont décrites au sein de la DTPG. Ces mesures adressent éventuellement, le cas échéant, les problématiques d'obsolescence et de détérioration des supports, en particulier lorsqu'il est nécessaire de conserver des données sur des périodes longues.

12.4.2 Sauvegardes hors site

Dans le cadre de la présente PG, le TSP MediaCert met en place des sauvegardes hors site conformément aux procédures définies par Worldline.

12.5 Journalisation et surveillance

12.5.1 Journalisation

Les mesures de journalisation mises en œuvre sont décrites dans le chapitre 15.1 du présent document.

12.5.2 Surveillance des journaux d'évènements

Les journaux d'évènements sont inspectés lors de leur émission par des outils spécifiés dans la DTPG. Ces outils permettent notamment de déclencher automatiquement des alarmes afin de notifier un potentiel incident détecté, en particulier un incident critique de sécurité, au responsable de l'évènement.

12.5.3 Surveillance de capacité

Une projection des futures exigences de capacité sur les plateformes du TSP MediaCert est régulièrement effectuée, généralement lors de réunions organisées par le Comité MediaCert. Ces plateformes font notamment l'objet d'une surveillance de capacité (disponibilité et utilisation des services) afin de garantir une capacité de traitement et de stockage adéquats.

12.5.4 Surveillance sécurité

Un outil (SIEM) est mis en place pour traiter les journaux d'évènements (analyse, corrélation) afin d'identifier et remonter des alertes sécurités. Le TSP MediaCert s'appuie notamment sur une équipe dédiée à ces activités (SOC) pour remonter des alertes sécurités et répondre ainsi aux exigences auxquelles il est soumis.

En particulier, les événements suivants font l'objet d'une surveillance :

- arrêt et démarrage des fonctions de génération des traces ;
- activité anormale sur le réseau.

Les alertes sont traitées par le TSP suivant les procédures décrites au chapitre 14.

Une revue régulière est réalisée avec cette équipe afin de faire le point sur les évènements anormaux et de prévenir des changements de configuration.

12.5.5 Surveillance des systèmes

Les systèmes du TSP MediaCert sont surveillés à l'aide de divers outils afin de s'assurer de leur bon fonctionnement.

12.6 Maîtrise des logiciels en exploitation

Le TSP MediaCert maîtrise les logiciels (inventaire, versions, …) installés sur ses systèmes. Par ailleurs, seuls les logiciels nécessaires sont installés sur les systèmes en production. Ces logiciels ont été sélectionnés pour leur fiabilité et leur capacité à assurer la sécurité et la continuité des services qu'ils fournissent. Ils font l'objet de mesures de sécurité afin de les protéger de toutes modifications ou altérations.

Les systèmes sont durcis en retirant les comptes, applications, services, protocoles et ports non-utilisés.

Les droits d'installation sur les différents environnements des Services de Confiance du TSP MediaCert sont limités et soumis à des procédures de changements (cf. chapitre 12.2).

12.7 Gestion des vulnérabilités techniques

Le TSP MediaCert assure une gestion des vulnérabilités techniques via :

- la mise en place de processus de patch management ;
- la mise en place d'une veille technique ;
- de scans vulnérabilités.

Ces processus sont disponibles dans le document DTPG.
Ces processus permettent de détecter des potentielles vulnérabilités et de créer des plans de corrections de vulnérabilité afin de maintenir le système d'information en conditions de sécurité optimales. Il est possible qu'une vulnérabilité ne fasse pas l'objet d'un plan de correction, cependant, le TSP MediaCert documente alors les éléments qui justifie cet arbitrage.

Toute vulnérabilité critique doit être adressée dans les quarante-huit (48) heures après sa découverte.
Ces processus permettent également de s'assurer que :

- les patchs sont appliqués dans un délai raisonnable après leur mise à disposition ;
- les patchs ne sont pas appliqués s'ils introduisent des vulnérabilités ou des instabilités qui contrebalancent leurs bénéfices théoriques ;
- si un patch n'est pas appliqué, les raisons de cette décision font l'objet d'une documentation.

Les scans de vulnérabilité sont réalisés de façon régulière par des personnels ayant les compétences, les outils, l'éthique et l'indépendance nécessaire pour produire un rapport fiable.

12.8 Acquisition, développement et maintenance des systèmes d'information

L'implémentation, la configuration et toute modification ou mise à jour d'un système permettant de mettre en œuvre les composantes d'un service du TSP MediaCert est documentée et contrôlée (cf. chapitre 12.6). Tout changement ayant un impact sur le niveau de sécurité doit être approuvé par le Comité MediaCert.

Les développements se font selon la politique de développement sécurisée de Worldline. Celle-ci couvre les aspects de conception, développements, tests et déploiement en production. Elle s'appuie sur les bonnes pratiques de sécurité reconnues. Une analyse des exigences de sécurité est réalisée au moment de la conception ou de la sélection de chacun des composants de l'architecture afin d'être assuré que la sécurité est bien prise en compte dans les systèmes informatiques.

Le TSP MediaCert ne fait pas appel à des développements externalisés pour les services de confiance.

Les développements sont systématiquement passés dans un outil d'analyse automatique visant à contrôler la qualité du code.

Les développements font l'objet de tests fonctionnels et de recette avant livraison en production.

Les données de production ne sont pas recopiées sur les environnements de pré-production, test ou développement. Des jeux de données de tests ou de données anonymisées sont utilisés pour les tests et développements.

13 Sécurité des communications

13.1 Gestion de l'accès aux réseaux

Le TSP MediaCert met en place des mesures pour protéger son réseau contre d'éventuelles attaques.

13.1.1 Cloisonnement réseau

Les plateformes du TSP MediaCert sont hébergées dans des zones réseau distinctes en fonction de leur rôle et sensibilité. Les composants critiques du réseau sont maintenus dans un environnement sécurisé. La sensibilité des différents éléments est établie en ligne avec les résultats de l'analyse de risque. Le TSP MediaCert applique les mêmes contrôles de sécurité à l'ensemble des composants d'une zone réseau.

Les flux réseaux en direction du TSP MediaCert, ainsi qu'entre chaque zone réseau distincte, sont notamment contrôlés (cf. chapitre 13.2) afin d'interdire tout flux non autorisés (y compris des flux émanant d'utilisateurs ou d'abonnés aux services). En particulier, les dispositifs de contrôle réseau sont configurés pour interdire l'ensemble des protocoles et accès qui ne sont pas nécessaires pour les opérations des services de confiance.
Les configurations font l'objet d'une revue régulière.

Les environnements de production et de test/développement font également l'objet d'un cloisonnement.

Afin de documenter le cloisonnement, le TSP MediaCert crée et maintien à jour un schéma simplifié du réseau (ou cartographie) représentant les différentes zones IP et le plan d'adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs, etc.) et les interconnexions avec l'extérieur (Internet, réseaux privés, etc.) et les partenaires. Ce schéma permet de localiser les serveurs détenteurs d'informations sensibles de l'entité.

13.1.2 Accès aux plateformes

Les plateformes du TSP MediaCert sont soumises à des restrictions d'accès logiques (cf. chapitre 9.3) et ne sont pas en accès direct. Le processus d'accès logique aux plateformes du TSP MediaCert est interne et décrit dans la DTPG. La gestion de contrôle d'accès est sous le contrôle du TSP MediaCert. Cette gestion inclut la gestion des comptes et permet de modifier ou de supprimer des accès sans délai. Les droits et privilèges d'accès aux plateformes sont attribués suivant la politique d'accès logique définie par le TSP MediaCert.

Le système de contrôle d'accès en place permet une gestion efficace et adéquate des accès, en particulier :

- il permet une séparation des rôles, en particulier entre les opérations d'administration et les autres opérations de niveau métier par l'utilisation de réseaux dédiés à chacun des usages ;
- il permet de contrôler et de restreindre l'utilisation des différentes applications et utilitaires.

Les systèmes utilisés pour l'administration sont dédiés à cet usage.

Des tests de pénétration sont effectués lors de la mise en place de l'infrastructure des services puis à chaque évolution ou modification majeure. Du fait de leur criticité, et de l'importance de fourniture un rapport fiable, les tests de pénétrations ne peuvent être effectués que par des personnels sélectionnés sur des critères tels que leurs compétences, connaissances, efficacité, éthique et indépendance.

13.1.3 Accès aux services

Les services du TSP MediaCert ne sont pas en contact direct avec des réseaux ouverts sur internet. Les passerelles permettant les accès sont protégées contre des tentatives d'intrusion ou d'attaque.

Ces passerelles limitent les services ouverts et protocoles aux seuls services indispensables au fonctionnement des services délivrés par le TSP MediaCert. Elles sont régulièrement mises à jour pour prendre en compte les évolutions des systèmes anti-intrusions et combler les failles de sécurité potentielles.

13.2 Transfert de l'information

Dans le cas où ils ne se trouvent pas dans un réseau dédié, tous les flux de communication entre matériels du TSP MediaCert se font exclusivement via des protocoles de communication réseau sécurisés garantissant la confidentialité et l'intégrité de la communication.

13.3 Redondance

La connexion externe fait l'objet d'une redondance afin de fournir un haut niveau de disponibilité du service.

14 Gestion des incidents

En cas de remontée d'alerte, le TSP MediaCert a mis en place un système de gestion des incidents permettant de répondre de façon coordonnée et rapide aux incidents, afin de limiter leur impact.

14.1 Gestion des incidents de sécurité

Des processus de gestion des incidents sont mis en place afin de limiter les conséquences de tels incidents et d'informer dans les délais adéquats les parties concernées. En particulier, le suivi des alertes pouvant être liées à un incident de sécurité est réalisé par des personnels en rôle de confiance. Ces personnels s'assurent que la remontée et le traitement de ces incidents est réalisé en conformité avec les procédures de gestions des incidents établies par le TSP MediaCert.

Par ailleurs, en cas de compromission des Services de Confiance, les autorités légales compétentes sont notifiées si la nature de la compromission le requiert. En particulier, un incident de sécurité avéré portant atteindre à l'intégrité du service de confiance ou compromettant des données personnelles devra faire l'objet d'une notification dans les vingt-quatre (24) heures :

- à l'ANSSI dans tous les cas, en suivant la procédure préconisée par l'ANSSI ;
- à la CNIL dans le cas où l'incident impact des données personnelles.

Le TSP MediaCert notifiera également les Abonnés impactés.

Ces processus prévoient notamment la revue des incidents afin d'assurer le suivi des plans d'actions correctifs et préventifs visant à éviter la récidive de tels incidents.

Ils prévoient aussi la mise en place d'une surveillance pour détecter des incidents de sécurité dans les meilleurs délais (cf. chapitre 12.5.4).

14.2 Procédures de gestion des incidents de sécurité

Des procédures sont établies afin d'assurer une réponse appropriée aux incidents envisagés. Pour cela, le TSP MediaCert s'appuie sur la Politique de Gestion des Incidents Worldline qui traite notamment de la classification des incidents de sécurité et de leur déclaration. A ce sujet, le TSP MediaCert possède sa propre procédure de notification, décrite au sein de la DTPG.

Ces procédures adressent notamment le cas de compromission des Services de Confiance et les interruptions de service. De plus, dans le cas de corruption des ressources informatiques ou d'incident technique, le TSP MediaCert a mis en place un Plan de Continuité et de Reprise d'Activité pour chacun des services de confiance qu'il délivre (cf. chapitre 16.2).

15 Collection de preuves

15.1 Journalisation

Les évènements intervenants dans la vie du TSP MediaCert sont journalisés sous forme de fichiers à partir de générations automatisées par logiciel et complétées, s'il y a lieu, de saisies manuelles. Ces fichiers ont pour but d'assurer la traçabilité et l'imputabilité des opérations effectuées (auteurs, horodatages, …).

Les journaux d'évènements comprennent explicitement l'identifiant de l'exécutant (logiciel ou humain), la date et l'heure de l'opération ainsi que la nature de l'évènement.

Ils peuvent être mis à disposition de la justice lors d'une requête légale les requérants.

15.1.1 Type d'évènements journalisés

Le TSP MediaCert journalise les évènements liés :

- à la sécurité (incluant les accès ou tentatives d'accès) ;
- aux activités et au cycle de vie des systèmes des services de confiances qu'il fournit.

Ces journaux d'évènements peuvent être sous forme électronique ou manuscrite. L'ensemble de ces évènements est listé dans la documentation technique DTPG relative au présent document.

15.1.2 Fréquence de traitement des journaux d'évènements

Les systèmes de surveillance mis en œuvre (cf. chapitre 12.5.2) traitent les journaux dès lors qu'ils sont collectés.

15.1.3 Fréquence de conservation des journaux d'évènements

Les journaux d'évènements sont exportés au fil de l'eau sur un serveur distant.

15.1.4 Période de conservation des journaux d'évènements

Les journaux d'évènement sont conservés sur des périodes de temps qui diffèrent en fonction du type d'évènement et du service de confiance concerné. Ces périodes de temps de conservation sont spécifiées dans les politiques associées aux différents services de confiance du TSP MediaCert.

15.1.5 Protection des journaux d'évènements

Les journaux d'évènements électroniques sont collectés via le système décrit au chapitre 15.1.7 du présent document puis externalisés vers deux types d'environnement (supervision et notarisation) dont les administrations sont différentes. L'accès à ces éléments sont donc rendus possible uniquement au personnel autorisé par le TSP MediaCert comme défini dans le document DTPG et ne sont pas modifiables ou effaçables sans autorisation.

Les journaux d'évènements manuscrits sont protégés grâce à des systèmes physiques sécurisés de type coffre-fort ou armoire forte dont les accès sont contrôlés par le TSP MediaCert.

Ces systèmes garantissent l'intégrité et la confidentialité des journaux d'événements.

15.1.6 Procédure de sauvegarde des journaux d'évènements

La procédure de sauvegarde des journaux d'évènements du TSP MediaCert est interne et est spécifiée dans le document DTPG.

15.1.7 Système de collecte des journaux d'évènements

Le système de collecte des journaux d'évènements du TSP MediaCert est interne et est spécifié dans le document DTPG.
Celui-ci tient compte de la sensibilité de l'information collectée et analysée.

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

Il n'y a pas systématiquement de notification de l'enregistrement d'un évènement au responsable de l'évènement.

15.2 Archivage

15.2.1 Protection des archives

La confidentialité des archives est assurée par une gestion d'accès physique, système et réseau appropriée. Elle permet d'assurer la complétude et la confidentialité des archives.

Durant leur période de rétention au sein des locaux sécurisés du TSP MediaCert, les archives sont protégées en intégrité et ne sont accessibles qu'aux personnes habilitées. En effet, la demande d'accès à une archive ne peut être uniquement faite que par le responsable du TSP MediaCert, un responsable adjoint du TSP MediaCert ou l'officier sécurité du TSP MediaCert afin d'assurer la confidentialité des informations.

Des procédures sont en place afin de parer à l'obsolescence et à la détérioration des archives. Celles-ci sont notamment stockées dans des locaux sujets à des mesures de protection contre les menaces naturelles.

15.2.2 Procédure de sauvegarde des archives

Le niveau de protection des archives est équivalent au niveau de protection des sauvegardes. Les procédures de sauvegarde des archives sont internes et sont spécifiées dans le document DTPG.

15.2.3 Exigences d'horodatage des données

L'ensemble des évènements sont datés précisément avec l'heure système des serveurs du TSP MediaCert. Les serveurs du TSP MediaCert synchronisent leur horloge interne régulièrement (au moins toutes les 24h) sur des serveurs de référence afin de garantir la cohérence de l'heure (UTC) indiquée dans les différents journaux électroniques.

15.2.4 Système de collecte des archives

Le système de collecte des archives d'évènements du TSP MediaCert est interne et est spécifié dans le document DTPG.

15.2.5 Procédure de récupération et de vérification des archives

Les archives peuvent être récupérées dans un délai inférieur à deux (2) jours ouvrés à compter de l'enregistrement de la demande. L'accès aux archives est sujet à des restrictions (cf. chapitre 15.2.1).

Les archives seront rendues disponibles en cas de réquisition judiciaire.

16 Continuité d'activité

16.1 Engagements de disponibilité

L'objectif de disponibilité pour le site web du TSP MediaCert est précisé au chapitre 5.2.3 du présent document.

Par ailleurs, le TSP MediaCert possède des engagements de disponibilités propres à chaque service de confiance qu'il fournit.

16.1.1 Services de Certification

La fonction d'information sur l'état des Certificats est disponible 7j/7 24h24. Le TSP MediaCert vise un niveau d'indisponibilité le plus faible possible.

16.1.2 Services d'Horodatage

La disponibilité visée pour la fourniture du service est définie au sein de la politique concernée.

16.1.3 Services d'Archivage

La disponibilité visée à la fois pour le service de capture et pour le service de consultation d'archive(s) est définie au sein des diverses politiques d'archivage.

16.2 Continuité et reprise d'activité

En cas d'interruption ou de corruption des ressources informatiques (matériels, logiciels et/ou données), notamment en cas de compromission de la clé privée d'une composante, le TSP MediaCert appliquera alors le Plan de Continuité et de Reprise d'Activité du service concerné afin d'assurer la continuité et/ou le rétablissement du service dans les plus brefs délais.
Des mesures de remédiation sont mises en places afin de limiter les risques d'occurrence d'un nouvel incident.

La PGI et le PCRA sont régulièrement tenus à jour respectivement par les équipes sécurité de Worldline et par les équipes en charge du TSP MediaCert.

17 Fin d'activités

Le TSP MediaCert met en place un plan d'arrêt d'activité visant à minimiser l'impact d'un arrêt d'activité pour les Abonnés et Utilisateurs.

Dans le cas où le TSP MediaCert déciderait d'interrompre la fourniture d'un de ses services de confiance, le plan de cessation d'activité du service concerné serait alors appliqué. Chacun des plans de cessation d'activité des services de confiance comprend les points suivants :

- information de la décision du TSP MediaCert aux personnes concernées (organes de contrôle tel que l'ANSSI, partenaires, Abonnés, utilisateurs) avant la cessation des activités du service en respectant un préavis ;
- abrogation des autorisations données aux éventuels sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de fourniture du service ;
- transfert à Worldline de ses obligations de maintien des journaux d'évènements et des archives nécessaires pour démontrer le fonctionnement correct du service durant une période raisonnable ;
- destruction des clés privées (nominales et sauvegardes) concernées par le service de telle façon qu'elles ne puissent pas être recouvrées ;
- maintien ou transfert à Worldline de ses obligations de rendre disponible ses clés publiques ainsi que les Certificats concernés par le service aux Utilisateurs pendant une période raisonnable.

Les plan de cessation d'activité des différents services de confiance du TSP MediaCert sont régulièrement revus et maintenus à jour conformément à l'état de l'art.

Dans le cas où le TSP MediaCert ferait faillite, celui-ci se raccrochera à Worldline afin de couvrir les obligations de fin vie des services de confiances qu'il délivre.

Chaque politique d'un Service de Confiance du TSP MediaCert peut compléter ces points de dispositions spécifiques au type de service de confiance mis en œuvre.

18 Conformité

18.1 Assurance

18.1.1 Couverture par les assurances

Worldline dispose, auprès d'une compagnie notoirement solvable, d'une police d'assurance garantissant les dommages pouvant survenir à ses biens, son personnel, ainsi qu'une police couvrant sa responsabilité professionnelle dans le cadre des prestations fournies.

18.1.2 Autres ressources

Worldline dispose des ressources financières pour assurer la fourniture des services du TSP MediaCert.

18.1.3 Couverture et garantie concernant les entités utilisatrices

Le TSP MediaCert ne pourra pas être tenu pour responsable d'une utilisation non-autorisée ou non-conforme des services qu'il fournit (Certificats, Contremarques de temps).
En effet, la responsabilité du TSP MediaCert ne peut être engagée qu'en cas de non-respect prouvé de ses obligations.

De plus, dans la mesure des limitations de la loi, le TSP MediaCert ne saurait être tenu responsable :

- d'aucune perte financière ;
- d'aucune perte de données ;
- d'aucun dommage indirect lié à l'utilisation d'un Certificat ou d'une Contremarque de temps.
- d'aucun autre dommage.

Le TSP MediaCert n'est d'une façon générale pas responsable des documents et informations transmises par l'Abonné et ne garantit pas leur exactitude ni les conséquences de faits, actions, négligences ou omissions dommageables de l'Abonné.

En toute hypothèse, la responsabilité du TSP MediaCert sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant pour l'accès au service de confiance concerné tel que précisé notamment dans le contrat de service associé et ce, dans le respect et les limites de la loi applicable.

18.2 Confidentialité des données professionnelles

18.2.1 Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- les informations techniques relatives à la sécurité des fonctionnements des HSM et de certaines composantes des services du TSP MediaCert ;
- les clés privées des AC, de leurs composantes et des Certificats émis ;

- les clés privées des UH ;
- les données d'activations des clés privées d'AC et d'UH ;
- la documentation technique relative aux politiques des différents services de confiance ;
- les procédures internes d'exploitation ;
- le plan de continuité et de reprise d'activité des différents services de confiance ;
- le plan de cessation d'activité des différents services de confiance ;
- les dossiers d'enregistrements ;
- les rapports d'audit.

Seules les personnes habilitées par Worldline et ayant le besoin ou l'autorisation d'en connaître le contenu ont la possibilité de consulter, à la demande, les informations susvisées. Cette demande doit être transmise au responsable du TSP MediaCert ou à un de ses adjoints.

18.2.2 Informations hors du périmètre des informations confidentielles

Les informations du TSP MediaCert considérées comme publiques et donc non-confidentielles sont celles définies au chapitre 5.2.2 du présent document.

18.2.3 Responsabilité en terme de protection des informations confidentielles

Le TSP MediaCert s'engage à traiter les informations confidentielles collectées dans le respect des lois et règlements en vigueur.

18.3 Protection des données personnelles

18.3.1 Politique de protection des données personnelles

Worldline veille à la protection des données personnelles qu'elle détient ou est amenée à détenir, conformément aux règles relatives à la protection des données personnelles en vigueur sur le territoire à partir duquel elle exerce ses prestations de service.

Ces données sont protégées suivant la loi française nationale applicable à ses prestations laquelle en France, s'inscrit en conformité à la réglementation Européenne tant eIDAS qu'au RGPD (cf. chapitre 18.7).

Ainsi, conformément au règlement eIDAS, le TSP MediaCert prend les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'elle fournit. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

En cas de violation des données personnelles, le TSP MediaCert se réfère à la Procédure de Traitement des Violations de Donnés Personnelles Worldline mise à sa disposition.

Le TSP MediaCert agit conformément aux obligations de type LRC (Légales Réglementaires et Contractuelles).

18.3.2 Responsabilité en terme de protection des données personnelles

Worldline traite les données personnelles en respectant la législation et la réglementation définie au chapitre 18.7 du présent document, laquelle s'inscrit en conformité de celle prévalant sur le territoire Européen, en matière de protection des données à caractère personnel.

18.3.3 Droit d'accès aux données

Conformément à l'Article 40 de la loi informatique et libertés modifiée par LOI n°2016-1321 du 7 octobre 2016 - art. 63, toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé auxdites opérations.

Le droit d'accès peut s'exercer par écrit : courrier postal auprès du point de contact du TSP MediaCert, adresse présente au chapitre 5.1.2 de ce document ou présente sur le site web du TSP MediaCert (cf. chapitre 5.2.3), accompagné d'une copie d'une pièce d'identité. Idéalement, en recommandé avec accusé de réception.

18.3.4 Conditions de divulgation d'information personnelles aux autorités judiciaires ou administratives

Worldline peut devoir mettre à disposition des informations à caractère personnel collectées à des tiers habilités dans le cadre de procédures judiciaires ou dans le cadre d'audits aux fins de vérifier la validité de l'opération des services du TSP MediaCert. Celui-ci dispose de procédures sécurisées pour permettre ces accès qui sont tracés nominativement et conservés.

18.4 Droits sur la propriété intellectuelle et industrielle

Le TSP MediaCert agit conformément à la législation et à la réglementation définie au chapitre 18.7 du présent document. Les documents publics, hors périmètre des informations confidentielles, demeurent propriété de Worldline.

18.5 Dispositions concernant la résolution de conflits

Pour tout litige, il convient de contacter le TSP MediaCert au point de contact décrit en 5.1.2.
Les parties s'efforceront de régler à l'amiable tout litige concernant l'interprétation ou l'exécution du contrat dans les meilleurs délais. En l'absence de conciliation tout litige relatif à la validité, l'interprétation ou l'exécution de la présente Politique Générale, des Politiques des services ou des CGU sera soumis aux tribunaux compétents indiqué en 18.6.

Des dispositions complémentaires concernant la résolution de conflits propre à chaque service de confiance du TSP MediaCert pourront être indiquées dans les politiques et CGU de ces services. Elles sont donc définies dans les politiques et/ou conditions générales associées.

18.6 Juridictions compétentes

En cas de litige relatif aux Services de Confiance fournis par le TSP MediaCert, en ce compris la documentation y afférente et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

18.7 Conformité aux législations et réglementations

Le TSP MediaCert, dans toutes ses composantes et y compris documentaires, est régie par la législation et la réglementation française qui lui est applicable, elle-même généralement issue des textes européens, et ce bien que ses activités qui découlent de la présente PG puissent avoir des effets juridiques en dehors du territoire français.

Une veille régulière est effectuée pour vérifier le respect de ces contraintes légales.

Par ailleurs, seule la version française des documents contractuels (dont la présente PG) est opposable aux parties, même en présence de traductions. En effet, les traductions de convention expresse sont prévues à titre de simple commodité et ne peuvent avoir aucun effet juridique, notamment sur l'interprétation du Contrat d'Abonnement ou de la commune intention des parties.

18.8 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par la jurisprudence des Cours et tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible. A ce titre, le TSP MediaCert ne peut être tenu pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure.

18.9 Audits

Le TSP MediaCert soumet ses services à des audits de conformité ou à d'autres moyens d'évaluation. Chaque service donne des précisions sur le sujet au sein de leur politique spécifique.

18.9.1 Fréquences et/ou circonstances des évaluations

Worldline procède à un audit de conformité aux politiques en vigueur de ses différents services de confiance (Service de Certification, Service d'Horodatage et Service d'Archivage) lors de la mise en œuvre opérationnelle d'une composante d'un service de confiance et lors de toute modification significative au sein d'une composante par un organisme accrédité.

Worldline peut être amenée à effectuer un audit de surveillance (interne ou externe) entre deux audits externe de Certification aux normes en vigueur sur le service de confiance du TSP MediaCert concerné.

18.9.2 Identités / qualifications des évaluateurs

18.9.2.1 Audit de certification

Le contrôle de la composante du service de confiance est effectué par une équipe d'auditeurs faisant partie d'un organisme d'audit habilité et accrédité à procéder à des évaluations selon les spécifications des normes applicables au service de confiance du TSP MediaCert évalué.

18.9.2.2 Audit de surveillance

Le contrôle de la composante du service de confiance est effectué par une équipe en charge des contrôles de conformité et indépendante du service de confiance du TSP MediaCert évalué.

18.9.3 Relations entre évaluateurs et entités évaluées

18.9.3.1 Audit de certification

Le ou les évaluateurs effectuant le contrôle de la ou des composantes du service de confiance évalué sont indépendants et exempt de tout conflit d'intérêts.

18.9.3.2 Audit de surveillance

Le ou les évaluateurs effectuant le contrôle de la ou des composantes du service de confiance évalué n'ont pas un quelconque rôle de confiance au sein du TSP MediaCert.

18.9.4 Sujets couverts par les évaluations

Les contrôles effectués par les auditeurs portent sur une partie ou sur l'ensemble des composantes d'un service de confiance du TSP MediaCert afin de contrôler le respect de la mise en œuvre de la présente PG ainsi que la conformité des procédures et pratiques du service de confiance vis-à-vis des exigences auxquelles il est sujet.

A cet égard, avant chaque audit, l'évaluateur responsable de l'audit envoie au TSP MediaCert un plan d'audit, spécifiant les composantes et procédures qu'il souhaitera contrôler lors de l'audit avec son ou ses confrères ainsi que le programme détaillé de l'audit.

18.9.5 Actions prises suite aux conclusions des évaluations

A l'issue d'une évaluation, l'équipe d'audit rend à Worldline son avis parmi les possibilités suivantes :

- réussite : l'audit n'a relevé aucune non-conformité et aucune action nouvelle n'est à mener. Worldline confirme la conformité de la composante auditée aux engagements du présent document et aux pratiques annoncées ;
- à confirmer : l'audit a relevé une ou plusieurs non-conformités non-bloquantes. Worldline doit alors présenter un plan d'actions correctives avec un délai de réalisation. Un nouveau contrôle pourra être effectué pour vérifier la mise en place des corrections ;
- échec : l'audit a relevé une ou plusieurs non-conformités bloquantes. L'équipe d'audit émet alors des recommandations à Worldline qui peuvent être la cessation temporaire ou définitive d'activité, etc. Le choix de la mesure à appliquer appartient à Worldline.

18.9.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme d'audit en charge de la Certification du service de confiance du TSP MediaCert évalué.