Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Certificate Policy and Public Certificate Practice Statement

Certificats Numériques Personnels RGS et/ou ETSI

Signed by:
Maxime Hambersin
9A097E002C47437...

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

CERTIFICATS NUMERIQUES PERSONNELS RGS ET/OU ETSI

Version du document :	2.8	**Nombre total de pages :**	88
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	DocuSign France		

Liste de diffusion :	☒ Externe	☒ Interne DocuSign France
	Public	Public

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
02/09/2011	1.0	EM	Passage en v1.0	JYF
07/10/2013	1.1	DV	Mise à jour de la charte graphique, corrections mineures et ajout de la fonctionnalité de déblocage des cartes	EM – JYF
28/05/2014	1.2	EM	Intégration de l'ensemble des offres RGS de DocuSign France pour les personnes physiques professionnelles (support matériel uniquement)	
04/06/2014	1.3	EM	Intégration des remarques issues de l'audit RGS	
23/06/2014	1.4	EM	Intégration de l'offre RGS * signature seulement (support logiciel).	JYF
14/08/2014	1.5	EM	Rajout des URL OCSP correctes et correction d'erreurs	
19/02/2015	1.6	EM	Intégration modification Sylae double usage	JYF
12/03/2015	1.7	EM	Correction coquille	
13/01/2016	1.8	EM	Modification suite au rachat de TDT par DocuSign	
31/03/2017	1.9	EM	Passage aux nouveau	

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

			standards ETSI EN 319 411	
26/05/2017	2.0	EM	Intégration des commentaires LSTI.	
28/09/2018	2.1	EM	Modification du profil de certificat OID 1.3.6.1.4.1.22234.2.9.3.15 pour le passer en double usage. Cet OID n'est plus RGS *** à cause du double usage à partir du 01/10/2018.	
16/10/2018	2.2	EM	Intégration de la vérification d'email pour Mozilla, mise à jour de coquille par rapport au déblocage pour l'OID 1.3.6.1.4.1.22234.2.9.3.15 et autres et explicitation des exigences sur l'opération de déblocage uniquement en face à face.	
03/06/2019	2.3	EM	Mise à jour des contacts PMA et des profils de certificats et mis à jour de la PC.	
09/08/2019	2.4	EM	Mise à jour pour intégrer les résultats d'audit de LSTI.	
19/09/2019	2.5	EM	Mise à jour pour intégrer les résultats d'audit de LSTI.	
08/11/2019	2.6	EM	Mise à jour pour intégrer les résultats d'audit de LSTI.	
17/03/2021	2.7	EM	End of all services described in the present CP expect revocation service and CRL and OCSP validation service.	
26/02/2025	2.8	EM	End of CRL issuance and OCSP response services. Last CRL has been issued in 2024.	

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

SOMMAIRE

AVERTISSEMENT 12

1 INTRODUCTION 13

1.1 Présentation générale 13
1.2 Identification du document 14
1.3 Entités intervenant dans l'IGC 16
1.3.1 DocuSign France Policy Management Authority (PMA) 17
1.3.2 Autorité de Certification (AC) 17
1.3.3 Autorité d'Enregistrement (AE) 17
1.3.4 Autorité d'Enregistrement Déléguée (AED) 17
1.3.5 Service de Publication (SP) 18
1.3.6 Opérateur de Service de Certification (OSC) 18
1.3.7 Porteurs de certificats 18
1.3.8 Autres participants 18
1.4 Usage des certificats 19
1.4.1 Domaines d'utilisation applicables 19
1.4.2 Domaines d'utilisation interdits 19
1.5 Gestion de la PC 20
1.5.1 Entité gérant la PC 20
1.5.2 Point de contact 20
1.5.3 Entité déterminant la conformité d'une DPC avec cette PC 20
1.5.4 Procédure d'approbation de la conformité de la DPC 20
1.6 Définitions et Acronymes 20
1.6.1 Définitions 20
1.6.2 Acronymes 23

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES 24

2.1 Entités chargées de la mise à disposition des informations 24
2.2 Informations devant être publiées 24
2.3 Délais et fréquences de publication 24
2.4 Contrôle d'accès aux informations publiées 25

3 IDENTIFICATION ET AUTHENTIFICATION 26

3.1 Nommage 26

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

3.1.1 Types de noms....26
3.1.2 Nécessité d'utilisation de noms explicites....26
3.1.3 Pseudonymisation des porteurs....26
3.1.4 Règles d'interprétation des différentes formes de noms....26
3.1.5 Unicité des noms....26
3.1.6 Identification, authentification et rôle des marques déposées....26
3.2 Validation initiale de l'identité....27
3.2.1 Méthode pour prouver la possession de la clé privée....27
3.2.2 Validation de l'identité d'un organisme....27
3.2.3 Validation de l'identité d'un individu....28
3.2.4 Informations non vérifiées du Porteur....29
3.2.5 Validation de la capacité du demandeur....29
3.2.6 Critère d'interopérabilité....29
3.3 Identification et validation d'une demande de renouvellement des clés....29
3.3.1 Identification et validation pour un renouvellement courant....29
3.3.2 Identification et validation pour un renouvellement après révocation....29
3.4 Identification et validation d'une demande de révocation....30
4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 31
4.1 Demande de certificat....31
4.1.1 Origine d'une demande de certificat....31
4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat....31
4.2 Traitement d'une demande de certificat....32
4.2.1 Exécution des processus d'identification et de validation de la demande....32
4.2.2 Acceptation ou rejet de la demande....32
4.2.3 Durée d'établissement du certificat....33
4.3 Délivrance du certificat....33
4.3.1 Actions de l'AC concernant la délivrance du certificat....33
4.3.2 Notification par l'AC de la délivrance du certificat au porteur....33
4.4 Acceptation du certificat....34
4.4.1 Démarche d'acceptation du certificat....34
4.4.2 Publication du certificat....34
4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat....34
4.5 Usage de la bi-clé et du certificat....34
4.5.1 Utilisation de la clé privée et du certificat par le porteur....34
4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat....34
4.6 Renouvellement d'un certificat....34

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé 34
4.8 Modification du certificat 34
4.9 Révocation et suspension des certificats 35
4.9.1 Causes possibles d'une révocation 35
4.9.2 Origine d'une demande de révocation 35
4.9.3 Procédure de traitement d'une demande de révocation 37
4.9.4 Délai accordé au porteur pour formuler la demande de révocation 37
4.9.5 Délai de traitement par l'AC d'une demande de révocation 37
4.9.6 Exigences de vérification de révocation pour les utilisateurs de certificats 38
4.9.7 Fréquences d'établissement des LCR 38
4.9.8 Délai maximum de publication d'une LCR 38
4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats 38
4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats 38
4.9.11 Autres moyens disponibles d'information sur les révocations 39
4.9.12 Exigences spécifiques en cas de compromission de la clé privée 39
4.9.13 Causes possibles d'une suspension 39
4.9.14 Origine d'une demande de suspension 39
4.9.15 Procédure de traitement d'une demande de suspension 39
4.9.16 Limites de la période de suspension d'un certificat 39
4.10 Fonction d'information sur l'état des certificats 39
4.10.1 Caractéristiques opérationnelles 39
4.10.2 Disponibilité de la fonction 39
4.11 Fin de la relation entre le porteur et l'AC 40
4.12 Séquestre de clé et recouvrement 40

5 MESURES DE SECURITE NON TECHNIQUES 41

5.1 Mesures de sécurité physiques 41
5.1.1 Situation géographique et construction des sites 41
5.1.2 Accès physique 41
5.1.3 Alimentation électrique et climatisation 41
5.1.4 Vulnérabilité aux dégâts des eaux 41
5.1.5 Prévention et protection incendie 41
5.1.6 Mise hors service des supports 41
5.1.7 Sauvegardes hors site 41
5.2 Mesures de sécurité procédurales 41
5.2.1 Rôles de confiance 41

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5.2.2 Nombre de personnes requises par tâches 41
5.2.3 Identification et authentification pour chaque rôles 42
5.2.4 Rôles exigeant une séparation des attributions 42
5.3 Mesures de sécurité vis-à-vis du personnel 42
5.3.1 Qualifications, compétences et habilitations requises 42
5.3.2 Procédures de vérification des antécédents 42
5.3.3 Exigences en matière de formation initiale 42
5.3.4 Exigences et fréquence en matière de formation continue 42
5.3.5 Fréquence et séquence de rotation entres différentes attributions 43
5.3.6 Sanctions en cas d'actions non autorisées 43
5.3.7 Exigences vis-à-vis du personnel des prestataires externes 43
5.3.8 Documentation fournie au personnel 43
5.4 Procédures de constitution des données d'audit 43
5.4.1 Type d'événements à enregistrer 43
5.4.2 Fréquence de traitement des journaux d'événements 44
5.4.3 Période de conservation des journaux d'événements 44
5.4.4 Procédures de sauvegarde des journaux d'événements 44
5.4.5 Système de collecte des journaux d'événements 44
5.4.6 Evaluation des vulnérabilités 44
5.5 Archivage des données 45
5.5.1 Type de données à archiver 45
5.5.2 Période de conservation des archives 45
5.5.3 Protection des archives 46
5.5.4 Exigences d'horodatage des données 46
5.5.5 Système de collecte des archives 46
5.5.6 Procédures de récupération et de vérification des archives 46
5.6 Changement de clé d'AC 46
5.6.1 Certificat d'AC 46
5.6.2 Certificat de Porteur 47
5.7 Reprise suite à compromission et sinistre 47
5.7.1 Procédures de remontée et de traitement des incidents et des compromissions 47
5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) 47
5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante 47
5.7.4 Capacités de continuité d'activité suite à un sinistre 48
5.8 Fin de vie d'IGC 48
5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC 48

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5.8.2 Cessation d'activité affectant l'AC 48

6 MESURES DE SECURITE TECHNIQUES 50

6.1 Génération et installation de bi-clés 50
6.1.1 Génération des bi-clés 50
6.1.2 Transmission de la clé privée à son propriétaire 51
6.1.3 Transmission de la clé publique à l'AC 51
6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats 51
6.1.5 Taille des clés 51
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité 52
6.1.7 Objectifs d'usage de la clé 52
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 52
6.2.1 Standards et mesures de sécurité pour les modules cryptographiques 52
6.2.2 Contrôle de la clé privée par plusieurs personnes 52
6.2.3 Séquestre de clé privée 53
6.2.4 Copie de secours de de clé privée 53
6.2.5 Archivage de la clé privée 53
6.2.6 Transfert de la clé privée vers / depuis le module cryptographique 53
6.2.7 Stockage de la clé privée dans un module cryptographique 53
6.2.8 Méthode d'activation de la clé privée 53
6.2.9 Méthode de désactivation de la clé privée 54
6.2.10 Méthode de destruction des clés privées 54
6.2.11 Niveau de qualification du module cryptographique et des dispositifs d'authentification et de signature 54
6.3 Autres aspects de la gestion des bi-clés 54
6.3.1 Archivage des clés publiques 54
6.3.2 Durée de vie des bi-clés et des certificats 55
6.4 Données d'activation 55
6.4.1 Génération et installation des données d'activation 55
6.4.2 Protection des données d'activation 55
6.4.3 Autres aspects liés aux données d'activation 56
6.5 Mesures de sécurité des systèmes informatiques 56
6.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques 56
6.5.2 Niveau de qualification des systèmes informatiques 57
6.6 Mesures de sécurité des systèmes durant leur cycle de vie 57
6.6.1 Mesures de sécurité liées au développements des systèmes 57
6.6.2 Mesures liées à la gestion de la sécurité 57

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes 57
6.7 Mesures de sécurité réseau 57
6.8 Horodatage / Système de datation 58

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR 59

7.1 Profil de Certificats 59
7.1.1 Extensions de Certificats 59
7.1.2 Identifiant d'algorithmes 59
7.1.3 Formes de noms 59
7.1.4 Identifiant d'objet (OID) de la Politique de Certification 59
7.1.5 Extensions propres à l'usage de la Politique 59
7.1.6 Syntaxe et Sémantique des qualificateurs de politique 59
7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies" 59
7.2 Profil de LCR 59
7.2.1 LCR et champs d'extensions des LCR 59
7.3 Profil OCSP 59

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 60

8.1 Fréquence et / ou circonstances des audits 60
8.2 Identités / qualifications des évaluateurs 60
8.3 Relation entre évaluateurs et entités évaluées 60
8.4 Sujets couverts par les évaluations 60
8.5 Actions prises suite aux conclusions des évaluations 60
8.6 Communication des résultats 61

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES 62

9.1 Tarifs 62
9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats 62
9.1.2 Tarifs pour accéder aux certificats 62
9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats 62
9.1.4 Tarifs pour d'autres services 62
9.1.5 Politique de remboursement 62
9.2 Responsabilité financière 62
9.2.1 Couverture par les assurances 62
9.2.2 Autres ressources 62
9.2.3 Couverture et garantie concernant les entités utilisatrices 62
9.3 Confidentialité des données professionnelles 62
9.3.1 Périmètre des informations confidentielles 62

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

9.3.2 Informations hors du périmètre des informations confidentielles 63
9.3.3 Responsabilité en termes de protection des informations confidentielles 63
9.4 Protection des données personnelles 63
9.4.1 Politique de protection des données personnelles 63
9.4.2 Informations à caractère personnelles 63
9.4.3 Informations à caractère non personnel 63
9.4.4 Responsabilité en termes de protection des données personnelles 63
9.4.5 Notification et consentement d'utilisation de données personnelles 64
9.4.6 Condition de divulgation d'informations personnelles aux autorités judiciaires ou administratives 64
9.4.7 Autres circonstances de divulgation d'informations personnelles 64
9.5 Droits sur la propriété intellectuelle et industrielle 64
9.6 Interprétations contractuelles et garanties 64
9.6.1 Obligations communes 64
9.6.2 Obligations et garanties de la PMA 65
9.6.3 Obligations et garanties de l'AC 65
9.6.4 Obligations de l'AE 66
9.6.5 Obligations et garanties du porteur 67
9.6.6 Obligations et garanties du SP 67
9.6.7 Obligations et garanties des autres participants 67
9.7 Limite de garantie 67
9.8 Limite de responsabilité 68
9.9 Indemnités 69
9.10 Durée et fin anticipée de validité de la PC 69
9.10.1 Durée de validité 69
9.10.2 Fin anticipée de validité 69
9.10.3 Effets de la fin de validité et clauses restant applicables 69
9.11 Amendements à la PC 69
9.11.1 Procédures d'amendements 69
9.11.2 Mécanisme et période d'information sur les amendements 69
9.11.3 Circonstances selon lesquelles l'OID doit être changé 69
9.12 Dispositions concernant la résolution de conflits 69
9.13 Juridictions compétentes 69
9.14 Conformité aux législations et réglementations 70
9.15 Disposition diverses 70
9.15.1 Accord global 70
9.15.2 Transfert d'activités 70

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

9.15.3 Conséquence d'une clause non valide 70
9.15.4 Application et renonciation 70
9.15.5 Force majeure 70
9.16 Autres dispositions 70

10 REFERENCES **71**

11 PROFIL DE CERTIFICAT, CRL AND OCSP **72**

11.1 "KEYNECTIS ICS QUALIFIED CA" CA 72
11.1.1 Signature (Entreprise et administration) : RGS *** (sans déblocage) : 1.3.6.1.4.1.22234.2.9.3.172
11.1.2 Signature (Entreprise et administration) : EN 319 411 – 2 (Qualified with SSCD) : 1.3.6.1.4.1.22234.2.9.3.15 74
11.1.3 Certificate Revocation List 76
11.2 AC : KEYNECTIS ICS ADVANCED Class 3 CA 77
11.2.1 Authentification (Entreprise et administration) : RGS ** : 1.3.6.1.4.1.22234.2.9.3.13 77
11.2.2 Signature et authentification (Entreprise et administration) : RGS ** et EN 319 411 – 1 NCP+ : 1.3.6.1.4.1.22234.2.9.3.10 79
11.2.3 Signature et authentification (Offre SPM) (Entreprise et administration) : RGS * et EN 319 411 – 1 LCP : 1.3.6.1.4.1.22234.2.9.3.12 82
11.2.4 Certificate Revocation List 84
11.3 AC « Keynectis CA for Enterprise signature » 85
11.3.1 Offre Cert ID : Classic : 1.3.6.1.4.1.22234.2.12.3.3 85
11.3.2 CRL 87
11.4 OCSP 87

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de DocuSign France.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par DocuSign France ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'Article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (Article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les Articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

1 INTRODUCTION

1.1 Présentation générale

La dématérialisation, ou conversion au format électronique des transactions quotidiennes traditionnelles (contrats, courrier, factures, formulaires administratifs, etc.), permet avant tout d'accélérer les processus métier et documentaires. En raison de l'aspect innovant et technique de ces processus, les entreprises doivent faire appel à des prestataires de services spécialisés à même d'assurer le rôle de tierce partie de confiance et de fait, de fournir une preuve de la transaction. Les certificats électroniques et les opérations de certification signature électronique se trouvent au cœur de ces technologies.

Pour fournir leurs services, les tierces parties de confiance (Autorité de Certification - AC, Autorité d'Horodatage - AH, Autorité de Validation - AV), les entreprises et organisations utilisant des certificats électroniques, s'appuient sur les autorités de DocuSign France (AC, AH et AV).

La présente PC contient également l'information publique du Certificate Practice Statement (CPS ou DPC en français), mais le document s'appelle PC.

Dans cette perspective, DocuSign France a mis en place pour la délivrance de certificats électroniques les Autorité de Certification dénommées :

- « KEYNECTIS ICS Advanced Class 3 CA »;
- « KEYNECTIS ICS QUALIFIED CA » ;
- « Keynectis CA for Enterprise signature ».

qui s'appuient sur une Infrastructure de Gestion de Clés (IGC).

L'AC « KEYNECTIS ICS Advanced Class 3 CA » (notée AC dans la suite du présent document) est certifiée par l'autorité de certification « OpenTrust CA for AATL G1 ». L'AC est inclue dans le domaine de confiance de DocuSign France car l'autorité de confiance « OpenTrust CA for AATL G1 » est elle-même signée par l'AC racine « OPENTRUST ROOT CA G1 ». L'AC est incluse dans le domaine de confiance de l'éditeur logiciel Adobe car l'autorité de confiance « OpenTrust CA for AATL G1 » est référencé par Adobe.

L'AC « KEYNECTIS ICS QUALIFIED CA » (notée AC dans la suite du présent document) est certifiée par l'autorité de certification « OpenTrust CA for AATL G1 ». L'AC est inclue dans le domaine de confiance de DocuSign France car l'autorité de confiance « OpenTrust CA for AATL G1 » est elle-même signée par l'AC racine « OPENTRUST ROOT CA G1 ». L'AC est incluse dans le domaine de confiance de l'éditeur logiciel Adobe car l'autorité de confiance « OpenTrust CA for AATL G1 » est référencé par Adobe.

L'AC « Keynectis CA for Enterprise signature » (notée AC dans la suite du présent document) est certifiée par l'AC racine « Keynectis Root CA - 2011 ». L'AC est inclue dans le domaine de confiance de DocuSign France.

Les certificats délivrés par les AC sont remis à des porteurs personnes physiques, agissant pour le compte d'entreprises ou d'administrations. Les porteurs de certificats (seulement pour l'usage signature et l'usage signature et authentification, à l'exception des certificats émis par l'AC « Keynectis CA for Enterprise signature ») peuvent ainsi signer des documents au format PDF avec les logiciels de la gamme ADOBE (Reader, Adobe, LiveCycle), les utilisateurs de certificats peuvent ainsi valider facilement les signatures électroniques de documents PDF, en utilisant les fonctionnalités de signature des produits de l'éditeur Adobe.

La présente PC a pour objet de décrire la gestion du cycle de vie des :

- Certificats de porteurs délivrés par les AC et des bi-clés associées,
- Certificats des AC et de leurs bi-clés.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Les AC sont des AC qualifiées selon les exigences prévues par la réglementation française sur la signature électronique et par le Référentiel Général de Sécurité (RGS), elles sont aussi conformes aux exigences des normes ETSI pour les services listés dans la présente PC.

L'AC met en œuvre les services décrit dans cette PC de manière non discriminatoire dans les limites de ce que les technologies actuelles autorisent.

La présente PC est élaborée conformément :

- Au RFC 3647 : « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;
- Au document ANSSI :
    - « Référentiel Général de Sécurité, version 2.0, Annexe A2, Politique de Certification Type, « certificats électroniques de personne », Version 3.0 du 27 février 2014 »
    - « Référentiel Général de Sécurité, version 2.0, Annexe A4, Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques, Version 3.0 du 27 février 2014 »
    - « Référentiel Général de Sécurité, version 2.0, Annexe B1, Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014, (Annule et remplace la version 1.20 du 26 janvier 2010) ».
- ETSI documents:
    - [119 312]: "ETSI TS 119 312 V1.1.1 (2014-11): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.";
    - [319 401]: « ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers. »;
    - [319 412]:
        - « ETSI EN 319 412-1 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 1: Overview and common data structures. »;
        - « ETSI EN 319 412-2 V2.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 2: Certificate profile for certificates issued to natural persons » ;
        - « ETSI EN 319 412-5 V2.2.1 (2017-11): Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 5: QCStatements »;
    - [319 411]:
        - « ETSI EN 319 411-1 V1.2.2 (2018-04) »: « Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements »
        - « ETSI EN 319 411-2 V2.2.2 (2018-04) »: « Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates ».

1.2 Identification du document

La présente PC appelée : « PC Certificats Numériques personnels Professionnels » est la propriété de DocuSign France. Cette PC contient les OID suivants (un seul OID par type de certificats) :

- AC « KEYNECTIS ICS QUALIFIED CA »
    - Offre Cert ID Qualified *** (usage unique signature, Entreprises/Administration), RGS *** :

        - 1.3.6.1.4.1.22234.2.9.3.1 : sans déblocage de support. Ce profil n'est plus certifié ETSI à cause du profil de certificat. Ce profil de certificat n'est plus émis depuis le 31 janvier 202 et tous les services sont arrêtés (y compris CRL et OCSP).
    - Offre Cert ID Qualified (usage unique signature, Entreprises/Administration), ETSI EN 319 411-2 QCP-n-qscd :
        - 1.3.6.1.4.1.22234.2.9.3.15 : avec déblocage de support. Ce profil n'est plus certifié RGS *** depuis le 01/10/2018 car l'usage de la clé authentification TLS a été rajouté ce qui en fait un certificat double usage. Ce profil de certificat n'est plus émis depuis le 31 janvier 2021 et tous les services sont arrêtés (y compris CRL et OCSP).
    - Une dernière CRL avec une date de fin de « 9999/31/12 23:59:59Z » a été émise en 2024 avec la date de début du « 2024/06/15 00:00:00 Z » et elle est publiée à l'URL suivante : https://www.docusign.com/fr-fr/mentiones-legales/politiques-de-certifications.

- AC "KEYNECTIS ICS ADVANCED Class 3 CA"
    - Offre Cert ID Office ** (usage signature et authentification, Entreprises/Administration), RGS ** et ETSI EN 319 411-1 NCP+ :
        - 1.3.6.1.4.1.22234.2.9.3.10 : avec déblocage de support et envoi de code d'activation par courrier électronique ou SMS ou enveloppe sécurisée. Ces fonctions seront mises en place à des dates ultérieures et feront l'objet d'une communication auprès des Clients, des AE et des porteurs concernés. Ce profil de certificat n'est plus émis depuis le 31 janvier 2021 et tous les services sont arrêtés (y compris CRL et OCSP).
    - Offre « Authentification seulement » (usage unique authentification, Entreprises/Administration), RGS ** :
        - 1.3.6.1.4.1.22234.2.9.3.13 : sans déblocage de support. Ce profil n'est plus certifié ETSI à cause du profil de certificat. Ce profil de certificat n'est plus émis depuis le 31 janvier 2021 et tous les services sont arrêtés (y compris CRL et OCSP).
    - Offre Cert ID : Classic Plus* (usage signature et authentification, Entreprises/Administration), RGS * et ETSI EN 319 411-1 LCP :
        - 1.3.6.1.4.1.22234.2.9.3.12 : avec déblocage de support et envoi de code d'activation par courrier électronique ou SMS. Ce profil de certificat n'est plus émis depuis le 31 janvier 2021 et tous les services sont arrêtés (y compris CRL et OCSP).
    - Une dernière CRL avec une date de fin de « 9999/31/12 23:59:59Z » a été émise en 2024 avec la date de début du « 2024/06/15 00:00:00 Z » et elle est publiée à l'URL suivante : https://www.docusign.com/fr-fr/mentiones-legales/politiques-de-certifications.

- AC « Keynectis CA for Enterprise signature ».
    - Offre Cert ID : Classic (usage unique signature et authentification, Entreprises/Administration), RGS * :
        - 1.3.6.1.4.1.22234.2.12.3.3 : génération de la bi-clé par l'AC au format logiciel (conteneur PKCS#12) et envoi de code d'activation par courrier électronique. Ce profil n'est plus certifié ETSI à cause du profil de certificat. Ce profil de certificat n'est plus émis depuis le 31 janvier 2021 et tous les services sont arrêtés (y compris CRL et OCSP).

La présente PC contient les exigences communes et particulières liées aux services et aux types de certificats RGS gérés par les AC. La PC précise également les évolutions nécessaires pour le renouvellement de certificat de porteur.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Les particularités sont identifiées dans le corps de texte directement en utilisant les acronymes RGS avec le nombre d'étoile et/ou l'OID quand ce n'est pas suffisamment précis.

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins le seul identifiant de la version applicable de la PC est l'OID.

1.3 Entités intervenant dans l'IGC

Pour délivrer les certificats, l'AC s'appuie sur les services suivants :

- Service d'enregistrement : ce service collecte et vérifie les informations d'identification du porteur qui demande un certificat, avant de transmettre la demande de certificat au service de demande de certificat ;
- Service de demande de certificat : ce service crée une demande de certificat, à l'aide des informations fournies par le service d'enregistrement dans le but de créer et de transmettre une demande de certificat au service de génération de certificat ;
- Service de génération de certificat : ce service génère les certificats électroniques des porteurs à partir des informations transmises par le service de demande de certificat ;
- Service de personnalisation et de gestion des supports de bi-clés matériels (EAL4+) : ce service permet de personnaliser graphiquement et électriquement (génération de bi-clés) les supports de bi-clé(s) cryptographique(s) selon les données fournies par le service de génération de certificats. Ce service permet également de générer et d'insérer les données d'activation des supports de clés privées. Ces données d'activation sont composées d'un code d'activation initial à destination du porteur afin de protéger/activer sa clé privée cryptographique et de données de déblocage de support ;
- Service de personnalisation et de gestion des supports de bi-clés logiciels (seulement pour l'OID 1.3.6.1.4.1.22234.2.12.3.3) : ce service permet de générer des bi-clés au format Pkcs#12 et un code P12 afin de protéger la bi-clé ;
- Service de remise au porteur (seulement pour l'OID 1.3.6.1.4.1.22234.2.12.3.3) : ce service remet au porteur son certificat et sa bi-clé protégée par un code P12 ainsi que le code P12 qui sont fournis par le service de personnalisation et de gestion des bi-clés ;
- Service de remise au porteur : ce service remet au porteur au minimum son certificat ainsi que les autres éléments fournis par le service de personnalisation des supports de bi-clés (support matériel des bi-clés cryptographiques et données d'activation) ;
- Service de déblocage de support de Porteur : ce service permet de débloquer des supports. Uniquement pour les certificats avec les OIDs suivants : 1.3.6.1.4.1.22234.2.9.3.10, 1.3.6.1.4.1.22234.2.9.3.12, 1.3.6.1.4.1.22234.2.9.3.15.
- Service de révocation de certificats : ce service traite les demandes de révocation des certificats des porteurs et détermine les actions à mener, dont la génération des Liste de Certificats Révoqués (LCR) ;
- Service de Publication : ce service met à disposition des utilisateurs de certificat (UC) les informations nécessaires à l'utilisation des certificats émis par l'AC, ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations ;
- Service de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audit consultables. Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus dans la délivrance des certificats par l'AC aux porteurs. La Déclaration des Pratiques de Certification (notée DPC) donnera les détails des pratiques de l'IGC dans cette même perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

Les changements majeurs au sein du TSP ou de ses partenaires AE sont notifiés à l'ANSSI.

1.3.1 DocuSign France Policy Management Authority (PMA)

La PMA est DocuSign France. La PMA est responsable de l'AC dont elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité de l'AC est composé de la présente PC, de la DPC associée, des conditions générales d'utilisation et des procédures mises en œuvre par les composantes de l'IGC. La PMA valide le référentiel de sécurité composé de la PC et de la DPC. Elle autorise et valide la création et l'utilisation des composantes de l'AC. Elle suit les audits et/ou contrôle de conformités effectuées sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application. Elle valide que le Client possède des procédures spécifiques pour les services de l'AE qu'il met en œuvre.

1.3.2 Autorité de Certification (AC)

L'AC génère des certificats et révoque des certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. L'AC met en œuvre les services de génération de certificats, de révocation de certificats et de journalisation et d'audit.

DocuSign France s'appuie sur les capacités d'Opérateur de Service de Certification (OSC) afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des certificats.

L'AC agit conformément à la présente PC et à la DPC associée qui sont établies par la PMA. Dans la présente PC, l'AC est identifiée par son « CN ».

DocuSign France est AC au sens de la responsabilité de gestion du cycle de vie des certificats.

1.3.3 Autorité d'Enregistrement (AE)

L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, service de personnalisation et de gestion des supports de bi-clés, de remise aux porteurs, de révocation de certificats, service de déblocage de support de Porteur et journalisation et d'audit. L'AE est chargée d'authentifier et d'identifier les porteurs, les AED et les MC. L'AE est mise en œuvre par DocuSign France ou par une entité tierce désignée par DocuSign France.

Toutefois, l'AE peut déléguer l'enregistrement de demandes de certificats à une entité tierce. Cette entité tierce est alors appelée Revendeur (AED). En ce cas, un contrat entre le Revendeur, en qualité d'AED, et l'AE permet de définir précisément les obligations et les services mis en œuvre par cette AE déléguée. La DPC précise les délégations possibles et les procédures associées lorsqu'un revendeur est utilisé et agit en tant qu'AE déléguée.

De même, DocuSign France en tant qu'AC peut déléguer l'ensemble de l'AE à une entité tierce. En ce cas, un contrat est établi entre l'entité tierce qui sera AE et DocuSign France. Dans ce cas, ceux sont l'ensemble des fonctions d'AE qui sont déléguées suivant les procédures définies par DocuSign France. De même, une AE totalement déléguée peut aussi mettre en place des AED (Cf. § 1.3.4) et des MC (Cf. § 1.3.8.2). Cette mise en place d'AED et de MC s'effectue toujours suivant les règles définies dans la PC, la DPC et les procédures fournies par DocuSign France.

Dans tous les cas, l'AE agit conformément à la PC et à la DPC associée qui sont établies par la PMA.

1.3.4 Autorité d'Enregistrement Déléguée (AED)

L'AED peut être utilisée par la mise en œuvre des services d'enregistrement de demandes de certificats, de remise aux porteurs, de révocation de certificats, service de déblocage de support de Porteur et

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

journalisation et d'audit. L'AED est, dans tous les cas, chargée d'authentifier et d'identifier les porteurs et les MC et établir ainsi l'identité du porteur et des MC. L'AED est mise en œuvre par des entités légales en relation contractuelle avec l'AE.

En aucun cas, l'AED n'a accès aux moyens qui lui permettrait d'activer et d'utiliser la clé privée, associée à la clé publique contenue dans le certificat, délivré au porteur. Le porteur reste seul capable de mettre en œuvre la clé privée qui lui est remise par l'AE ou l'AED.

Dans tous les cas, l'AED agit conformément à la PC et à la DPC associée qui sont établies par la PMA et au contrat qui la lie à l'AE. En fonction des services qu'elle met en œuvre, l'AED respecte les exigences qui incombent à l'AE pour les services supportés. La PC ne précise donc pas les procédures avec ou sans AED. La DPC apporte ces précisions.

1.3.5 Service de Publication (SP)

Le SP est utilisé pour la mise en œuvre du service de publication (Se reporter au § 2).

Le SP agit conformément à la PC et à la DPC associée.

1.3.6 Opérateur de Service de Certification (OSC)

L'OSC assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC. L'OSC est techniquement dépositaire de la clé privée de l'AC utilisée pour la signature des certificats. Sa responsabilité se limite au respect des procédures que l'AC définit afin de répondre aux exigences de la présente PC.

Dans la présente PC, son rôle et ses obligations ne sont pas distingués de ceux de l'AC. Cette distinction sera précisée dans la DPC.

1.3.7 Porteurs de certificats

Désigne la personne physique titulaire d'un Certificat agissant pour le compte d'entreprises ou d'administrations avec une identité professionnelle Cert ID. Le porteur met en œuvre une clé privée, à l'aide d'un code PIN, correspondant à la clé publique certifiée par l'AC afin de réaliser des opérations permises par l'usage des clés comme indiqué par l'extension « Key Usage » et « Extented Key Usage » dans chaque certificat et les CGU.

Le porteur (encore appelé « utilisateur » ou « signataire »), lorsqu'il appartient à une entité légale qui est aussi appelé Client.

1.3.8 Autres participants

1.3.8.1 Utilisateurs de certificats (UC)

L'utilisateur de certificat est une personne qui valide le certificat d'un porteur dans le cadre de la validation de signature électronique de document ou message électronique élaboré par le porteur et/ou dans le cadre de contrôle d'accès en SSL en fonction du type de certificat qu'il valide et donc de l'usage autorisé du certificat.

1.3.8.2 Mandataire de Certification (MC)

Un Mandataire de Certification est une personne physique, n'appartenant pas forcément à l'entité légale du Client, mandatée par un Client afin d'authentifier des porteurs du Client, de procéder aux enregistrements et demande de certificat auprès de l'AE ou de l'AED, et de remettre les supports de bi-clés aux porteurs. En aucun cas, le MC n'a accès aux moyens qui lui permettrait d'activer et d'utiliser la clé privée, associée à la clé publique contenue dans le certificat, délivré au porteur. Le porteur reste seul capable de mettre en œuvre la clé privée qui lui est remise par l'AE, l'AED ou le MC.

Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité qui souhaite délivrer des certificats à ses porteurs. Une même entité peut s'appuyer sur un ou plusieurs MC. Dans le cas où elle y a recours, le MC est formellement désigné par un représentant légal de l'entité concernée (Cf. dossier d'enregistrement au § 4.1.2). Le MC est en relation directe avec l'AE ou l'AED.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Les engagements du MC à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable du MC (assimilé au mandat cf. § 3.2). Dans tous les cas, le MC agit conformément à la PC et à la DPC associée qui sont établies par la PMA et au contrat qui la lie à l'AE via les CGU qu'il signe. En fonction des services qu'il met en œuvre, le MC respecte les exigences qui incombent à l'AE pour les services supportés. La PC ne précise donc pas les procédures avec ou sans MC. La DPC apporte ces précisions.

Ce mandat stipule notamment que le MC doit :

- Effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC ;
- Respecter les engagements décrits dans les CGU ;
- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

Un mandat de MC est valable tant que la personne est toujours habilitée par le Client à être MC et que le Client n'a pas communiqué la fin du mandat de MC pour une personne désignée à l'AE ou l'AED.

L'entité signale à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigne un successeur.

1.3.8.3 Client

Désigne une entité légale qui est client du de l'AED ou de l'AE, auprès de laquelle est revendu des Supports Cert ID par l'AED ou l'AE. Le Client représente aussi l'entité légale des utilisateurs qui souhaite avoir des certificats à titre professionnel. Le Client est aussi l'entité légale qui nomme les MC pour les utilisateurs qui sont sous sa responsabilité. Le Client est représenté par un Représentant Habilité ou une personne autorisée par le Représentant habilité.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Certificat de l'AC

Le certificat de l'AC sert à authentifier les certificats de porteurs. La clé privée associé au certificat d'AC sert pour :

- La signature de certificat de porteur ;
- La signature de certificat de répondeur OCSP.
- La signature de LCR.

1.4.1.2 Certificat de Porteur

Les certificats délivrés aux porteurs sont exclusivement utilisés par les porteurs identifiés à l'article 1.3.6 ci-dessus pour signer électroniquement des documents et/ou s'authentifier auprès d'application dans le cadre d'échanges dématérialisés avec les utilisateurs de certificats identifiés à l'article 1.3.7.1 ci-dessus.

Il est rappelé que l'utilisation de la clé privée du porteur et du certificat associé doit rester strictement limitée au service indiqué dans les CGU et les informations portées dans le Certificat du Porteur (« Key Usage » et « Extented Key Usage »). Dans le cas contraire, leur responsabilité pourrait être engagée.

1.4.2 Domaines d'utilisation interdits

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au § 1.4.1 ci-dessus ne sont pas autorisées. En pratique, cela signifie que l'AC ne peut être en aucun cas tenue pour responsable d'une utilisation des certificats qu'elle émet autre que celles prévues dans la présente PC.

Les certificats ne peuvent être utilisés que conformément aux lois applicables en vigueur, en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation et les lois, décrets, arrêtés et directives propres à la signature électronique.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Cette PC décrit la gestion du cycle de vie des certificats de signature et de leurs supports, elle n'a pas vocation de remplacer une politique de signature ou de contrôle d'accès qui elles décrivent la gestion du cycle de vie des signatures et des accès établies à l'aide des certificats délivrés par l'AC.

Il convient au porteur ou au Client ou au responsable d'application(s) utilisée(s) par le(s) porteur(s) d'élaborer leur propre politique de signature afin de définir notamment les engagements et les limites de responsabilités qu'une signature électronique confère au document signé électroniquement, ainsi que les moyens et conditions d'établissement de la vérification de la signature électronique. La mise en place d'une telle politique de signature et le recours éventuel à des services d'horodatage est vivement recommandé pour les signatures électroniques devant pouvoir être vérifiées potentiellement longtemps (plusieurs années) après la fin de validité des certificats correspondants. Il en va de même pour la politique de contrôle d'accès.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

La présente PC est sous la responsabilité de la PMA.

1.5.2 Point de contact

La PMA est l'entité à contacter pour toutes questions concernant le présent document :

- PMA de DocuSign France.
- https://www.docusign.fr/ (Les informations de contacts sont disponibles sur cette page).
- DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France.

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

La PMA procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour les composantes de l'IGC de gérer des certificats.

1.5.4 Procédure d'approbation de la conformité de la DPC

La PMA possède ses propres méthodes pour approuver le présent document. La PMA approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet.

1.6 Définitions et Acronymes

1.6.1 Définitions

PMA : Se reporter au § 1.3.1.

Autorité de Certification : Se reporter au § 1.3.2.

Accord d'utilisation de LCR : Un accord spécifiant les termes et conditions sous lesquels une Liste de Certificats Révoqués ou les informations qu'elle contient peuvent être utilisées.

Audit : Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures. [ISO/IEC POSIX Security].

Autorité de Certification (AC) : Se reporter au § 1.3.2.

Autorité d'Enregistrement (AE) : Se reporter au § 1.3.3.

Communauté de l'utilisateur : Se reporter au § 1.3.7.

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettent en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC ou AE est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.

Certificat : clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

Certificat d'AC : certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509]. Dans ce contexte, les certificats AC (certificat auto signé).

Certificat auto signé : certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification : (ou chaîne de confiance, ou chaîne de certification) chaîne constituée de multiples certificats nécessaires pour valider un certificat.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : clé de la bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1].

Client(s) : Cf. § 1.3.8.3.

Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité : La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

Déclaration des Pratiques de Certification (DPC) : une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) utilise pour approuver ou rejeter des demandes de certificat (émission, gestion, renouvellement et révocation de certificats). [RFC 3647].

Disponibilité : La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux deux propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie ;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1] ;
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Identité professionnelle Cert ID : c'est l'identité construite à partir des informations recueillies par le revendeur en tant qu'AED ou l'AE auprès de l'Utilisateur et de son Client et celles définies par OPENTRUST. Cette identité est utilisée pour authentifier l'utilisateur ainsi que son appartenance à une entité légale. Le cas échéant, cette identité sert aussi à authentifier une qualité professionnelle de l'utilisateur.

Infrastructure de Gestion de Clés (IGC) : également appelée IGC (Infrastructure de Gestion de Clés), c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Intégrité : fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Interopérabilité : implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles ; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Mandataire de Certification (MC) : Cf. § 1.3.8.2.

Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.

OSC : Se reporter au § 1.3.6.

Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10 : (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'IGC après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR ***:*** entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (PC) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Porteur : Se reporter au § 1.3.7.

Porteur de secret : personnes qui détiennent une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Qualificateur de politique : Des informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647]

Revendeur : Se reporter au § 1.3.4.

RSA : algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adelman.

SP : Se reporter au § 1.3.5.

Utilisateur de Certificat : Se reporter au §.1.3.8.1.

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaine de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification. Le concept de validation exposé dans cette PC et les CGU y afférente et les contrats liés à cette PC sont différent du concept de

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

validation tel qu'exposé par l'ANSSI dans le document « Référentiel Général de Sécurité, « Chapitre 6. Validation des certificats par l'État ».

1.6.2 Acronymes

- AC : Autorité de Certification ;
- AE : Autorité d'Enregistrement ;
- CC : Critères Communs ;
- DN : Distinguished Name ;
- DPC : Déclaration des pratiques de certification ;
- EAL : Evaluation assurance level, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité ;
- HTTP : Hypertext Transport Protocol ;
- IGC : Infrastructure de Gestion de Clés ;
- IP : Internet Protocol ;
- ISO : International Organization for Standardization ;
- LCR : liste de certificats révoqués ;
- LDAP : Lightweight Directory Access Protocol ;
- OCSP : Online Certificate Status Protocol ;
- OID : Object Identifier ;
- PC : Politique de Certification ;
- PIN : Personal Identification Number ;
- PKCS : Public-Key Cryptography Standard ;
- PMA : Policy Management Authority ;
- RFC : Request for comment ;
- RSA : Rivest, Shamir, Adleman ;
- SHA : Secure Hash Algorithm (norme fédérale américaine) ;
- SP : Service de Publication ;
- URL : Uniform Resource Locator.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

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

2.1 Entités chargées de la mise à disposition des informations

Le SP est en charge de la publication des données identifiées au § 2.2 ci-dessous.

2.2 Informations devant être publiées

La PMA, via le SP, rend disponibles les informations suivantes :

- La PC des AC : https://www.docusign.fr/societe/politiques-de-certifications ;
- Les certificats des AC : https://www.docusign.fr/societe/politiques-de-certifications ;
- Les certificats de la chaîne de confiance auxquels les AC sont rattachées à savoir : https://www.docusign.fr/societe/politiques-de-certifications ;
- Le formulaire de demande de certificat : sur demande auprès de l'AE ou de l'AED ;
- Le formulaire de non consentement : sur demande auprès de l'AE ou de l'AED ;
- Le formulaire et/ou les modalités de révocation d'un certificat : sur demande auprès de l'AE ou de l'AED ;
- Les conditions générales d'utilisation (CGU) : sur le Portail Register (https://register.dsf.docusign.net/) ;
- Le PDS est publié pour les certificats qualifiés seulement (l'URL est dans le profil de certificat en annexe).
- CRL : cf. § 11.

La dernière CRL de chaque AC expirée est mise en ligne de manière durable avec toute la chaîne d'AC dans le site utilisé pour la publication des PC. Elle sera aussi accessible en ligne en utilisant l'adresse CRL DP.

La DPC n'est pas publiée mais consultable auprès de la PMA sur demande justifiée et autorisée par la PMA.

La PMA s'assure que les conditions générales d'utilisation, en fonction du besoin des acteurs et des utilisateurs des services de l'IGC, sont rendues disponibles de la manière suivante :

- Porteur, Client et MC : les CGU sont contenues dans les demandes de certificats et demandes de créations de MC et sont donc signées par le MC, le Porteur et le Représentant Habilité du Client ou une personne autorisée par le Représentant Habilité du Client.
- Utilisateur de certificat : les conditions d'utilisation du service IGC sont décrites dans la présente PC aux paragraphes : 1.4, 4.4, 4.5.2, 4.9.6, 5.5, 9, 9.6, 9.7, et 9.8 et sont publiées sur le site internet de DocuSign.

2.3 Délais et fréquences de publication

Les informations identifiées au 2.2 ci-dessus sont disponibles :

- PC
  - Avant la mise en service initiale du service.
  - Dans les meilleurs délais après une mise à jour de PC approuvée par la PMA.
- Certificat d'AC :
  - Avant la mise en service initiale du service.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- Dans les meilleurs délais après la génération d'un certificat d'AC suivant un renouvellement.

Le système de publication doit avoir une disponibilité de 24h/24 et 7j/7 avec un taux de disponibilité de 99,9.

2.4 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées. L'AC s'assure que toute information conservée dans une base documentaire de son IGC et dont la diffusion publique ou la modification n'est pas prévue est protégée.

L'ensemble des informations publiques et publiées (Se reporter au § 2.2) est libre d'accès en lecture et téléchargement sur Internet.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X.509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN).

3.1.1.1 Certificat d'AC

L'identité de l'AC dans le certificat est donnée dans le § 11.

3.1.1.2 Certificat Porteur

L'identité du porteur dans le certificat est donnée dans le § 11.

3.1.2 Nécessité d'utilisation de noms explicites

Dans tous les cas, l'identité du porteur (Se reporter au § 3.1.1.2) est construite à partir des nom et prénom de son état civil tel que porté sur le document officiel d'identité présenté lors de son enregistrement (sauf pour l'OID 1.3.6.1.4.1.22234.2.9.3.12, Cf. 3.1.3).

Lorsque le certificat est pour un porteur au sein d'une Entreprise ou d'une Administration, alors l'identité de l'Entreprise ou de l'Administration est aussi contenue dans le certificat.

3.1.3 Pseudonymisation des porteurs

L'identité utilisée pour les certificats de porteurs n'est ni un pseudonyme ni un nom anonyme (Se reporter au § 3.1.2).

Seuls les certificats pour le RGS * (1.3.6.1.4.1.22234.2.9.3.12) peuvent avoir des identités qui sont des pseudonymes. En ce cas, le certificat possède une mention explicite dans un champs « OU » du DN du Porteur et qui indique la valeur « OU = PSEUDONYME » afin qu'aucune ambiguïté ne soit apportée à l'UC. De même, en ce cas l'AE conserve le lien entre les nom et prénoms et le pseudonyme demandé (contenus dans la demande de certificat).

3.1.4 Règles d'interprétation des différentes formes de noms

Les UC peuvent se servir de l'identité incluse dans les certificats (Se reporter au 3.1.1) afin d'authentifier les porteurs.

3.1.5 Unicité des noms

Les identités portées par l'AC dans les certificats (Se reporter au § 3.1.1) sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, une identité attribuée à un porteur (Se reporter au 3.1.1.2) de certificat ne peut être attribué à un autre porteur.

A noter que l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC, mais que ce numéro est propre au certificat et non pas au porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné.

L'AE assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique du champ SN attribué à un porteur (se reporter au § 3.1.1.2).

En cas de différent au sujet de l'utilisation d'un nom pour un certificat, la PMA a la responsabilité de résoudre le différent en question.

3.1.6 Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n° 92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par la communauté d'utilisateur et les Clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par le porteur est réalisée par les procédures de génération de la clé privée (se reporter au § 6.1.1 ci-dessous) correspondant à la clé publique à certifier et par le mode de transmission de la clé publique (se reporter au § 6.1.3 ci-dessous).

3.2.2 Validation de l'identité d'un organisme

3.2.2.1 AE

L'authentification d'un revendeur, qui souhaite être AE, repose sur la vérification des informations fournies par le revendeur dans le cadre de l'établissement du contrat AE.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

3.2.2.2 AED

L'authentification d'un revendeur, qui souhaite être AED, repose sur la vérification des informations fournies par le revendeur dans le cadre de l'établissement du contrat AED.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

3.2.2.3 Mandataire de certification

L'AE qui procède à la vérification s'assure que le Client existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande MC aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité du Client comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.
Dans tous les cas, la vérification de l'appartenance d'un MC à l'organisation de « type » Administration et Entreprise dont il se réclame est effectuée.

3.2.2.4 Porteur

L'AE qui procède à la vérification s'assure que le Client existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande Porteur aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité du Client comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.
Dans tous les cas, la vérification de l'appartenance d'un Porteur à l'organisation de « type » Administration et Entreprise dont il se réclame est effectuée.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

3.2.3 Validation de l'identité d'un individu

3.2.3.1 AE non OPENTRUST

Les Opérateurs de références de l'AE sont identifiés et authentifié lors d'un face à face avec l'AE de DocuSign France. L'identification et l'authentification s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

L'AE est ensuite responsable de l'authentification de l'ensemble des Opérateurs d'AE. L'AE tient à jour une liste de l'ensemble des Opérateurs d'AE. Cette liste est communiquée à OPENTRUST.

3.2.3.2 AED

Les Opérateurs d'AED centrale de l'AED sont identifiés et authentifié lors d'un face à face avec l'AE avec laquelle le contrat est établit. L'identification et l'authentification s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

Le revendeur est ensuite responsable de l'authentification de l'ensemble des Opérateurs d'AED. L'AED tient à jour une liste de l'ensemble des Opérateurs d'AED. Cette liste est communiquée à OPENTRUST et aux AE avec lesquels l'AED a établi un contrat.

3.2.3.3 Mandataire de certification : RGS **, RGS *** et OID 1.3.6.1.4.1.22234.2.9.3.15

Les MC sont identifiés et authentifié lors d'un face à face avec l'AE ou une AED de l'AE. L'identification et l'authentification s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.4 Mandataire de certification : RGS *

L'identification et l'authentification du MC, et des signataires de la demande de MC est effectuée par l'AED ou l'AE à partir des informations contenues dans le dossier de demande de certificat (Cf. § 4.1.2). L'identification et l'authentification du MC par l'AE ou l'AED s'effectue sur la base de la pièce d'identité officielle (carte nationale d'identité, passeport, …) contenue dans le dossier.

Le Représentant Habilité s'engage sur le contenu des informations portées dans la demande de certificat.

3.2.3.5 Porteur via AE : RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS ***

Le porteur est identifié et authentifié lors d'un face à face avec l'AE. L'identification et l'authentification du porteur par l'AE s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.6 Porteur via AED : RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS ***

Le porteur est identifié et authentifié lors d'un face à face avec l'AED. L'identification et l'authentification du porteur par l'AE s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.7 Porteur via AED et MC : RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS ***

Le porteur est identifié et authentifié lors d'un face à face avec le MC. L'identification et l'authentification du porteur par le MC s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.8 Porteur via AE : RGS *

L'identification et l'authentification du porteur par le Représentant Habilité s'effectue sur la base d'une pièce d'identité officielle (carte nationale d'identité, passeport, …). Le Représentant Habilité s'engage sur le contenu des informations portées dans la demande de certificat.

L'identification et l'authentification du Porteur, et des signataires de la demande de certificat est effectuée par l'AE à a partir des informations contenues dans le dossier de demande de certificat (Cf. § 4.1.2).

3.2.3.9 Porteur via AED : RGS *

L'identification et l'authentification du Porteur, et des signataires de la demande de certificat est effectuée par l'AED à partir des informations contenues dans le dossier de demande de certificat (Cf. § 4.1.2).

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

L'identification et l'authentification du porteur par l'AE s'effectue sur la base de la pièce d'identité officielle (carte nationale d'identité, passeport, …) contenue dans la demande.

Le Représentant Habilité ou le MC s'engage sur le contenu des informations portées dans la demande de certificat.

3.2.3.10 Porteur via AED et MC

Le Représentant Habilité s'engage sur le contenu des informations portées dans la demande de certificat et le mandat de MC.

L'identification et l'authentification du porteur par le MC s'effectue sur la base d'une pièce d'identité officielle (carte nationale d'identité, passeport, …).

L'identification et l'authentification du Porteur et du MC, et des signataires de la demande de certificat est effectuée par l'AED à partir des informations contenues dans le dossier de demande de certificat (Cf. § 4.1.2). L'identification et l'authentification du Porteur et du MC par l'AE s'effectue sur la base d''une pièce d'identité officielle (carte nationale d'identité, passeport, …) contenue dans la demande de certificat.

3.2.4 Informations non vérifiées du Porteur

Les informations non vérifiées ne sont pas introduites dans les certificats.

3.2.5 Validation de la capacité du demandeur

La validation de la capacité d'un porteur correspond à la validation de l'appartenance à une organisation (se reporter au § 3.2.2 ci-dessus) et son autorisation par un représentant légal de l'organisation.

3.2.6 Critère d'interopérabilité

Un porteur qui obtient un certificat émis par l'AC (« KEYNECTIS ICS Advanced Class 3 CA » et « KEYNECTIS ICS QUALIFIED CA ») à la garantie d'être authentifiable dans le domaine de confiance AATL d'Adobe et dans les outils de messagerie électroniques et de navigateurs internet en fonction des systèmes d'exploitation qu'ils utilisent.

Un Porteur de certificat issu de l'une des AC conformément à la présente PC à la garantie d'être reconnu pour le niveau de sécurité définit pour le Certificat par les Autorité Administrative, au sens du RGS, et les UC pour les certificats RGS et par les UC pour les certificats ETSI.

3.3 Identification et validation d'une demande de renouvellement des clés

3.3.1 Identification et validation pour un renouvellement courant

Lors du premier renouvellement, l'AC s'assure au minimum que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide et que le porteur est toujours autorisé à avoir un certificat.

De même l'AC vérifie que le MC et/ou le Représentant Habilité (ou la personne autorisée) est toujours habilité à être MC et/ou le Représentant Habilité (ou la personne autorisée). Si ce n'est pas le cas, l'AE requière les mêmes pièces justificatives pour le MC et/ou le Représentant Habilité (ou la personne autorisée) comme pour une première demande de certificat. Lors du premier renouvellement, le Porteur signe la demande de certificat et est authentifié par l'AE à l'aide des informations recueillies lors de la première demande.

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le porteur selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

3.3.2 Identification et validation pour un renouvellement après révocation

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2).

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

3.4 Identification et validation d’une demande de révocation

Les demandes de révocation sont authentifiées par l'AE, l’AED ou le MC. Lorsque le demandeur est une personne autre que le porteur, l’authentification est réalisée suivant des procédures définies dans la DPC.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Un certificat peut être demandé par un représentant légal de l'entité ou un MC dûment mandaté pour cette entité, avec dans tous les cas le consentement préalable du futur porteur.

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

Les informations suivantes doivent figurer dans la demande de certificat du porteur :

- Porteur au sein d'une Entreprise :
    - La demande de certificat est signée par le porteur et le représentant légal du Client et datée de moins de 3 mois. Cette demande de certificat sert de mandat désignant le futur porteur auquel le certificat doit être délivré ;
        - Si la demande de certificat ne peut pas être signée par un représentant légal du Client, alors une personne autorisée par un représentant légal du Client doit être désignée et signer la demande de certificat. En ce cas, un document, désignant la personne autorisée, doit être élaboré et signé par un représentant légal de l'entité et la personne autorisée ;
        - Pour les demandes de certificats établies par un MC, la demande de certificat est signée par le MC et le porteur seulement ;
    - Un document officiel d'identité du futur porteur (notamment carte nationale d'identité, passeport ou carte de séjour), en cours de validité, comportant une photographie d'identité, l'AE en conserve une copie ;
    - Les informations qui permettent de construire l'identité du porteur (se reporter aux § 3.1.1.2 et § 3.1.2) ;
    - La valeur du pseudonyme sir le Porteur doit avoir un pseudonyme (seulement pour l'OID 1.3.6.1.4.1.22234.2.9.3.12) ;
    - Les Informations permettant à l'AE de contacter le porteur (numéro de téléphone, courriel, …) ;
    - Toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat (uniquement si l'AE ou l'AED ne peut pas se le procurer elle-même) ;
    - Tout document attestant de la qualité du signataire de la demande de certificat. La qualité du signataire est portée dans la demande de certificat et est ainsi garantie par l'entité ;
    - Les conditions générales d'utilisation (CGU) signée par le porteur et le Représentant Habilité et le cas échéant le MC ;
- Porteur au sein d'une Administration :
    - La demande de certificat est signée par le porteur et le représentant légal de l'entité et datée de moins de 3 mois. Cette demande de certificat sert de mandat désignant le futur porteur auquel le certificat doit être délivré ;
        - Si la demande de certificat ne peut pas être signée par un représentant légal de l'entité, alors une personne autorisée par un représentant légal de l'entité doit être désignée et signer la demande de certificat. En ce cas, un document, désignant la

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

personne autorisée, doit être élaboré et signé par un représentant légal de l'entité et la personne autorisée ;

- Pour les demandes de certificats établies par un MC, la demande de certificat est signée par le MC et le porteur seulement ;

- Un document officiel d'identité du futur porteur (notamment carte nationale d'identité, passeport ou carte de séjour), en cours de validité, comportant une photographie d'identité, l'AE en conserve une copie ;
- Les informations qui permettent de construire l'identité du porteur (se reporter aux § 3.1.1.2 et § 3.1.2) ;
- Les Informations permettant à l'AE de contacter le porteur (numéro de téléphone, courriel, …) ;
- La valeur du pseudonyme sir le Porteur doit avoir un pseudonyme (seulement pour l'OID 1.3.6.1.4.1.22234.2.9.3.12) ;
- Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
- Les conditions générales d'utilisation (CGU) signée par le porteur et le Représentant Habilité et le cas échéant le MC.

La demande de certificat est signée en utilisant un mot de passe temporaire (code OTP) transmit à l'adresse de courrier électronique La demande de certificat est signée en utilisant un mot de passe temporaire (code OTP) transmis à l'adresse de courrier électronique contenue dans la demande de certificat décrite ci-dessus conformément à la politique de signature [Signature de Formulaire]. Ceci permet de vérifier l'adresse de courrier électronique du Porteur, du Mandataire et Représentant habilité. Les adresses électroniques étant contenues dans les formulaires de demande de certificat, elles font parties des données garanties par les personnes qui font l'objet d'une vérification conforme à l'ETSI et au RGS.

L'ensemble du dossier d'enregistrement peut être fournit soit sous forme papier soit sous forme électronique mais seulement en utilisant la procédure de dématérialisation prévue à cet effet par DocuSign France. Les informations sur l'utilisation de cette procédure sont données par l'AE ou par l'AED. Lorsqu'une AED est utilisée alors l'AED doit signer la demande afin d'en garantir l'origine.

4.2 Traitement d'une demande de certificat

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

La demande est authentifiée (se reporter aux § 3.2.2 et le 3.2.5 en fonction du type de certificat et du niveau RGS) et validée soit par l'AED ou l'AE.

L'AE ou l'AED authentifie et identifie le MC (Cf. § 3.2.2 et le 3.2.5 en fonction du type de certificat et du niveau RGS). L'AE tient à disposition des AED une liste des MC autorisé par Client. Ceci évite de redemander le mandat au MC pour chaque dossier de porteur d'un même Client.

L'AE, l'AED ou le MC s'assure que le porteur a pris connaissance des conditions générales d'utilisation.

L'AE s'assure également que lorsqu'une adresse de courrier électronique est déclarée par le Porteur, alors le Porteur maîtrise cette adresse de courrier électronique.

L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.

4.2.2 Acceptation ou rejet de la demande

En cas d'approbation de la demande, l'AE (service de demande de certificat) transmet la demande à l'AC (service de génération de certificat).

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

En cas de rejet de la demande, l'AE en informe le porteur, le MC ou l'AED (en fonction de l'origine de la demande) en justifiant le rejet. Si le MC ou le porteur ne sont pas directement informé par l'AE, alors c'est à l'AED d'informer le MC ou le porteur.

4.2.3 Durée d'établissement du certificat

La demande de certificat est traitée dès la réception de la demande par l'AE dans les meilleurs délais.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

4.3.1.1 RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS ***

L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC génère le certificat du porteur.

L'AC transmet le certificat au service de retrait de certificat de l'AE.

Si c'est l'AE qui gère le porteur, alors c'est l'AE qui remet le certificat au porteur dans son support matériel protégé par code d'activation après authentification (se reporter aux § 3.2.3 et § 6.1.2).

Si c'est l'AED qui gère le porteur, alors le porteur récupère le certificat, dans son support matériel protégé par le code d'activation, grâce au service de retrait de l'AED après authentification (se reporter aux § 3.2.3 et § 6.1.2).

Si c'est le MC qui gère le porteur, alors le porteur qui récupère le certificat, dans son support matériel protégé par code d'activation, auprès du MC (se reporter aux § 3.2.3). Le MC aura préalablement récupéré le certificat, dans le support matériel protégé par code d'activation, auprès du service de retrait de l'AE ou de l'AED (en fonction du choix initiale de dépôt de la demande effectué par le MC, se reporter aux § 3.2.3 et § 6.1.2).

Les communications, entre les différentes composantes de l'IGC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

4.3.1.2 RGS *

L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC génère le certificat du porteur.

L'AC transmet le certificat au service de retrait de certificat de l'AE.

Si c'est l'AE ou l'AED qui gère le porteur, alors c'est l'AE qui transmet le certificat au porteur dans son support protégé par code d'activation (se reporter au § 6.1.2).

Les communications, entre les différentes composantes de l'IGC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

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

4.3.2.1 RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS ***

La remise du certificat au porteur (service de remise au porteur) s'effectue lors d'un face à face entre l'AE, l'AED ou le MC et le porteur.

4.3.2.2 RGS *

La remise du certificat au Porteur s'effectue lors de la réception du support par le Porteur.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Le porteur utilise son code d'activation et le support afin de vérifier le contenu de son certificat. Si le porteur ne souhaite pas accepter son certificat, alors il dispose d'un délai de 15 jours pour manifester son non consentement en utilisant le formulaire dédié à cet effet et mise à disposition par l'AE ou l'AED. Passé ce délai, le certificat est considéré comme accepté.

Pour les niveaux RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS *** l'AED ou l'AE, en fonction de qui remet le support, et le MC ou le Porteur, en fonction de qui reçoit le support, signe tous deux un bordereau de remise de support et de certificat. Ce bordereau doit être ensuite retourné à l'AE suivant des conditions et un délai indiqué par l'AE.

4.4.2 Publication du certificat

Le certificat de l'AC est publié par le SP.

Les certificats des porteurs ne sont pas publiés par le SP.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation des bi-clés et des certificats est définie au § 1.4 ci-dessus. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (se reporter au § 6.1.7). La clé privée du porteur ne peut être utilisée que pour une opération de signature de données et/ou de contrôle d'accès type session SSL comme indiqué au § 1.4 en fonction du type de certificat.

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

L'utilisation des certificats par les UC est décrites dans les paragraphes 1.4 et 3.1.4 ci-dessus.

4.6 Renouvellement d'un certificat

Cette section concerne le processus de renouvellement du certificat porteur, sans que les clés publiques ou toute autre information incluse dans les certificats soient modifiées. Seule la période de validité et le numéro de série changent.

Ce type d'opération n'est pas autorisé au titre de la présente PC.

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Cette section concerne la génération d'un nouveau certificat avec changement de la clé publique associée.

Le changement de la clé publique d'un certificat implique la création d'un nouveau certificat. Dans ce cas la procédure à appliquer pour renouveler un certificat porteur est identique à celles décrites pour la délivrance du premier certificat porteur (se reporter au § 3.3, § 4.2 ; § 4.3 et § 4.1 ci-dessus).

Le déclenchement de la fourniture d'un nouveau certificat du porteur peut être automatique est à l'initiative du porteur. L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.

Le premier renouvellement de certificat peut être simplifié à condition que les informations contenues dans la demande précédente n'aient été modifiées.

4.8 Modification du certificat

Cette section concerne la génération d'un nouveau certificat porteur avec conservation de la même clé. Cette opération est rendue possible uniquement si la clé publique réutilisée dans le certificat est toujours conforme aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Ce type d'opération n'est pas autorisé au titre de la présente PC.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat Composante IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.1.2 Certificat Porteur

Un certificat de porteur est révoqué quand l'association la clé publique et le porteur qu'il certifie n'est plus considérée comme étant valide. Les motifs qui invalident cette association sont :

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du porteur d'un certificat Entreprise ou Administration), ceci avant l'expiration normale du certificat ;
- Le porteur, le MC ou le revendeur (AE ou AED) n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement du porteur ;
- Le décès du porteur ou la cessation d'activité de l'entité au sein laquelle le porteur agit (pour un certificat Entreprise ou Administration) ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La révocation de l'AC ;
- La fin de vie de l'AC ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Quand l'une de ces occurrences se produit, le certificat du porteur en question doit être révoqué.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat composante IGC

La PMA ou une autorité judiciaire via une décision de justice est à l'origine de la demande de révocation des certificats d'AC. La cessation d'activité de l'AC est une cause de révocation.

L'AC est à l'origine de la demande de révocation des certificats de composantes d'IGC.

4.9.2.2 Certificat porteur

Le porteur peut faire une demande de révocation dans les cas suivants :

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du porteur d'un certificat Entreprise ou Administration), ceci avant l'expiration normale du certificat ;
- Le porteur, le MC ou le revendeur n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement du porteur ;
- La perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'organisation d'appartenance (se reporter au § 3.2.2) du porteur, pour les Entreprise et les Administration, peut demander la révocation d'un certificat de porteur dans les cas suivants :

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du porteur d'un certificat Entreprise ou Administration), ceci avant l'expiration normale du certificat ;
- Le porteur, le MC ou le revendeur n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement du porteur ;
- Le décès du porteur ou la cessation d'activité de l'entité du porteur (pour un certificat Entreprise ou Administration) ;
- La perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AC peut demander la révocation d'un certificat de porteur dans les cas suivants :

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du porteur d'un certificat Entreprise ou Administration), ceci avant l'expiration normale du certificat ;
- Le porteur, le MC ou le revendeur n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement du porteur ;
- La perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé ;
- La révocation de l'AC ;
- la fin de vie de l'AC ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AE et l'AED peuvent demander la révocation d'un certificat porteur dans les cas suivants :

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du porteur d'un certificat Entreprise ou Administration), ceci avant l'expiration normale du certificat ;
- Le porteur ou le MC n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement du porteur ;
- La perte de la clé privée, perte de contrôle de sa clé privée, suspicion ou compromission de clé ;

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat composante IGC

La DPC précise les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux AED. Ces derniers devront informer les porteurs de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le point de contact identifié sur le site : www.ssi.gouv.fr doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. L'ANSSI se réservent le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

4.9.3.2 Certificat porteur

Une demande de révocation contient les informations suivantes :

- L'identité du porteur du certificat utilisée dans le certificat (nom, prénom, ...) ;
- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série du certificat, ...).

La demande de révocation est conservée par l'AE dans ses journaux.

La demande de révocation est authentifiée conformément au § 3.4.

L'AE transmet la demande de révocation à l'AC.

L'AC (service de révocation) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC (service de révocation) révoque le certificat du porteur en incluant le numéro de série du certificat dans la prochaine LCR qui sera émise par l'AC.

Le demandeur de la révocation est informé de la révocation effective du certificat porteur. De plus, si le porteur du certificat n'est pas le demandeur, le porteur est également informé de la révocation effective du certificat.

Dans le cas d'un porteur au sein d'une Entreprise ou d'une Administration, l'organisation d'appartenance (se reporter § 3.2.2) est informée de la révocation des certificats des porteurs qui lui sont rattachés.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le demandeur a connaissance qu'une des causes possibles de révocation de son ressort, est effective, il formule sa demande de révocation sans délai.

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

4.9.5.1 Certificat Composantes IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR/LAR et/ou de réponses OCSP) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

4.9.5.2 Certificat Porteur

Le service de révocation est disponible 24 heures sur 24 et 7 jours sur 7 pour les demandes en ligne.

Une demande de révocation, authentifié et dûment établie par l'AE, de certificat porteur est traitée dans un délai inférieur à 24 heures.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1h.

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois de 4h.

4.9.6 Exigences de vérification de révocation pour les utilisateurs de certificats

Il appartient aux UC de vérifier l'état de validité d'un certificat à l'aide de l'ensemble des LCR émises et/ou du service OCSP mise en œuvre par l'AC.

La CRL émise par l'AC « KEYNECTIS ICS QUALIFIED CA » contient les certificats expirés et révoqués et contient l'extension « expiredCertsOnCRL ».

Il est à noter qu'un certificat non expiré avec un statu révoqué donné par le service OCSP peut avoir un statu valide dans la CRL car l'OCSP est sur base de données l'AC alors que la CRL est émise toutes les 24 heures. Cette différence d'état ne peut durer qu'au maximum 24 heure (la différence n'existe plus avec la prochaine CRL). Par contre un certificat expiré, non qualifié et révoqué ne sera plus dans la CRL mais aura un statu révoqué donné par l'OCSP.

4.9.7 Fréquences d'établissement des LCR

La LCR est émise toute les 24 Heures. La CRL est valide 6 jours.

La dernière LCR émise par les AC « KEYNECTIS ICS QUALIFIED CA » est publiée avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« 99991231235959Z »).

Les informations de révocation seront toujours disponibles auprès de l'AC qui publie une CRL. En cas de fin de vie de l'AC ou d'arrêt du Service avec cette AC ou y compris en cas de compromission de clé d'AC, une dernière CRL est générée et archivée chez DocuSign France. Cette dernière CRL est publiée sur le site internet de DocuSign France jusqu'à expiration du TSP et sur l'URL de distribution de la CRL, contenue dans le Certificat, jusqu'à expiration du dernier Certificat émis par l'AC.

4.9.8 Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LCR suite à sa génération est de 30 minutes.

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

Les AC mettent en œuvre un serveur OCSP sauf l'AC « Keynectis CA for Enterprise signature » (Cf. § 11).

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

La réponse OCSP contient les informations suivantes :

Field	Requirements
Version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Subscriber's certificate status made in the CRL.
Next Update	Date of the next CRL.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Field	Requirements
CertStatus	"Good", "Revoked" or "unknown"
Nonce	Used if and only if the user Application provides a value for this field and reused in full.
extensions	No extension referenced

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC la révocation suite à une compromission de sa clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.). En cas de révocation de l'AC, l'ensemble des certificats porteurs sont révoqués.

Les conditions générales d'utilisation du certificat mentionnent clairement qu'en cas de compromission de la clé privée du porteur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13 Causes possibles d'une suspension

Sans objet.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

Le service OCSP est mis à jour à partir de la base de données de l'AC. Cependant le mécanisme principal de communication du statut des certificats est la LCR publiée par l'AC. Dans tous les cas, les utilisateurs de certificats peuvent utiliser un mécanisme de consultation libre de LCR.

Pour les ACs qui continuent à émettre des certificats, les réponses OCSP ont une date d'expiration comme suit :

- 24 heures pour un certificat valide.
- 72 heures pour un certificat révoqué.
- 15 minutes pour un certificat inconnu.

4.10.2 Disponibilité de la fonction

Le service OCSP est mis à jour à partir des informations de l'AC. Le service est disponible 24 heures sur 24 et 7 jours sur 7. Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue est fixé à un maximum de 10 seconde.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme au tableau suivant de 2h.

Cette fonction doit avoir une durée maximale totale d'indisponibilité par de 8h.

Le service OCSP est coupé après la fin de vie de l'AC et seule la dernière LCR est la seule information disponible cf. 4.9.7.

4.11 Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat de porteur est révoqué.

4.12 Séquestre de clé et recouvrement

Les bi-clés et les certificats des porteurs et d’AC émis conformément à la PC ne font pas l'objet de séquestre ni de recouvrement.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physiques

5.1.1 Situation géographique et construction des sites

Le site d'exploitation de l'AC respecte les règlements et normes en vigueur et son installation tient compte des résultats de l'analyse de risques, du métier d'opérateur de certification selon la méthode EBIOS, par exemple certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...) réalisées par l'OSC.

5.1.2 Accès physique

Afin de limiter l'accès aux applications et aux informations de l'IGC et afin d'assurer la disponibilité du système d'exploitation de l'AC, l'OSC met en place un périmètre de sécurité opéré pour ses besoins. La mise en œuvre de ce périmètre permet de respecter les principes de séparation des rôles de confiance telle que prévus dans cette PC.

Les accès au site de l'OSC, qui met en œuvre les services d'IGC, sont limités aux seules personnes nécessaires à la réalisation des services et selon leur besoin d'en connaître. Les accès sont nominatifs et leur traçabilité est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion passifs et actifs. Tout évènement de sécurité fait l'objet d'un enregistrement et d'un traitement.

5.1.3 Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre par l'OSC afin d'assurer la continuité des services délivrés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs.

5.1.4 Vulnérabilité aux dégâts des eaux

Les systèmes de l'OSC sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions.

5.1.6 Mise hors service des supports

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation.

5.1.7 Sauvegardes hors site

L'OSC réalise des sauvegardes hors site permettant une reprise rapide des services d'IGC suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services.

Les précisions quant aux modalités des sauvegardes des informations sont fournies dans la DPC.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance de l'AC sont conformes et similaires aux rôles définis par l'ETSI et le RGS.

5.2.2 Nombre de personnes requises par tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Le nombre de personnes requises par tâche est précisé dans la DPC.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5.2.3 Identification et authentification pour chaque rôles

L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel qui est amené à mettre en œuvre les services de l'IGC avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

Ces contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de l'AC. Chaque attribution d'un rôle à un membre du personnel de l'IGC lui est notifiée par écrit ou équivalent.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et les exigences de non cumuls décrits dans al DPC doivent être respectées. La séparation des rôles définis par le RGS *** est appliquée.

Les attributions associées à chaque rôle doivent être décrites dans la DPC.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'AC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de certification de l'IGC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

L'AC met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

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

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

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

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5.3.5 Fréquence et séquence de rotation entres différentes attributions

Des précisions sont fournies dans la DPC.

5.3.6 Sanctions en cas d'actions non autorisées

Des précisions sont fournies dans la DPC.

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

Des précisions sont fournies dans la DPC.

5.3.8 Documentation fournie au personnel

Des précisions sont fournies dans la DPC.

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier et / ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'événements à enregistrer

L'IGC journalise les évènements concernant les systèmes liés aux fonctions qu'elles mettent en œuvre dans le cadre de l'IGC :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres évènements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ayant des rôles de confiance ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'GC sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Evènements liés aux clés d'AC et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction,...) ;
- Génération des certificats de porteurs ;
- Génération des bi-clés de porteurs ;
- Transmission des certificats aux porteurs et selon les cas, acceptations / rejets par les Porteurs ;

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- Publication et mise à jour des informations liées à l'AC ;
- Génération d'information de statut d'un certificat (porteur).

Chaque enregistrement d'un évènement dans un journal contient les champs suivants :

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement ;
- Résultat de l'évènement (échec ou réussite).

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

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés:

- Destinataire de l'opération ;
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

5.4.2 Fréquence de traitement des journaux d'événements

Les opérations de journalisation sont effectuées au cours du processus considéré. En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement. Des précisions sont fournies dans la DPC.

5.4.3 Période de conservation des journaux d'événements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.4 Procédures de sauvegarde des journaux d'événements

L'IGC mettent en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risques de l'AC.

5.4.5 Système de collecte des journaux d'événements

Des précisions sont fournies dans la DPC.

5.4.6 Evaluation des vulnérabilités

Les composantes de l'IGC doivent être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Pour l'analyse, les règles suivantes s'appliquent :

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- Mettre en œuvre des contrôles de détection et de prévention sous le contrôle de l'OSC pour protéger les systèmes IGC contre les virus et logiciels malveillant ;
- Documenter et suivre un processus de correction de la vulnérabilité qui traite de l'identification, l'examen, la réponse, et la résolution des vulnérabilités ;
- Effectuer une analyse de vulnérabilité (i) après tout changement de système ou réseau suivant la décision de la PMA qui décide si les changements sont importants pour les AC et le Client pour l'AE, et (ii) au moins une fois par semaine, sur les adresses IP publics et privés identifiés par l'OSC les systèmes de l'IGC (pour l'AC) ;
- Effectuer un test de pénétration sur les systèmes de l'IGC sur au moins une base annuelle et suite à une modification de l'infrastructure ou des applications qui sont jugées important par la PMA pour l'AC et le Client pour l'AE ;
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration ;
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration ; par des personnes qualifiées, avec des outils adéquates, et suivant une démarche indépendante afin de garantir la qualité et la pertinence des analyses et des tests ;
- Procéder à une veille sur les vulnérabilités et les résoudre en fonction de la politique de sécurité de l'OSC et de l'analyse de risque de l'OSC.

Les journaux sont analysés suivant la fréquence requise par le RGS.

5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

5.5.1 Type de données à archiver

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- La politique de certification ;
- La déclaration des pratiques de certification ;
- Les certificats tels qu'émis ou publiés ;
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement (pour les entreprises et les administrations) ;
- Les dossiers complets de demandes de certificats ;
- Les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Certificats et LCR émis par l'AC

Les certificats de porteur et d'AC sont archivés 7 ans après leur expiration.

Journaux d'événements

Les journaux techniques d'évènements traités au chapitre 5.4 sont archivés pendant 7 ans après leur génération.

Dossier de demande de certificat

Les dossiers d'enregistrement (papier ou électronique comme définit au § 4.1) ne sont conservés que 7 ans après l'expiration du certificat associé.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- Seront protégées en intégrité ;
- seront accessibles aux seules personnes autorisées ;
- pourront être consultées et exploitées.

5.5.4 Exigences d'horodatage des données

Si un service d'horodatage est utilisé pour dater les enregistrements, il doit répondre aux exigences formulées à l'article 6.8.

5.5.5 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (Se reporter au 5.5.3).

5.5.6 Procédures de récupération et de vérification des archives

Les archives papier sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées. Les sauvegardes électroniques archivées sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées.

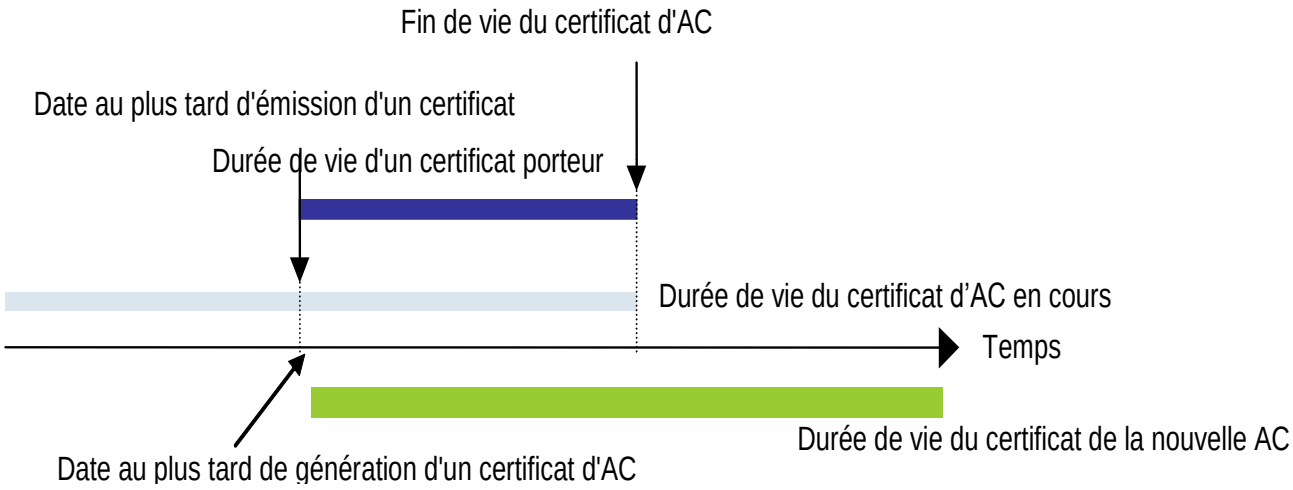
5.6 Changement de clé d'AC

5.6.1 Certificat d'AC

La durée de vie d'un certificat d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière.

Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats de porteurs. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats porteurs émis à l'aide de cette bi-clé.



Par ailleurs, l'AC change sa bi-clé et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5.6.2 Certificat de Porteur

La durée de validité d'un certificat est de 3 ans maximum.

5.7 Reprise suite à compromission et sinistre

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

L'AC a établi un plan de continuité de service qui met en évidence les différentes étapes à exécuter dans l'éventualité de la corruption ou de la perte des ressources système, des logiciels et ou des données et qui pourraient perturber ou compromettre le bon déroulement des services d'AC.

L'AC a conduit une analyse de risque pour évaluer les risques métier et déterminer les exigences de sécurité et procédures opérationnelles afin de rédiger un plan de reprise d'activité. Les risques pris en compte sont régulièrement revus et le plan est révisé en conséquence. Le plan de continuité de l'AC fait partie du périmètre audité, selon le paragraphe 8 ci-dessous.

Les personnels de l'AC dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas ou l'AC détecte une tentative de piratage ou une autre forme de compromission, elle mène une analyse afin de déterminer la nature des conséquences et leur niveau. Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

- Informe tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou à d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats ;
- Révoque tous les certificats concernés.

Si nécessaire, l'ampleur des conséquences est évalué par l'AC afin de déterminer si les services de l'AC doivent être rétablis, quels certificats porteurs doivent être révoqués, l'AC doit être déclarée compromise, certains services peuvent être maintenus (en priorité les services de révocation et de publication d'état des certificats porteurs) et comment, selon le plan de reprise d'activité.

L'AC doit également prévenir directement et sans délai le point de contact identifié sur le site : http://www.ssi.gouv.fr. Les vulnérabilités découvertes (AC, AE, …) sont traitées sous 48 heures dès leurs connaissances par la PMA et l'ANSSI et Adobe est alertée par la PMA en 24H00 dès connaissance de l'incident majeure portant atteinte à la sécurité du service ou des données personnelles.

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

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des service de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

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

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- La PMA, après enquête sur l'évènement décide de révoquer le certificat de l'AC ;
- Tous les Clients dont les certificats ont été émis par l'AC compromise, sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué ;
- La PMA décide ou non de générer un nouveau certificat d'AC ;
- Une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis ;
- Les porteurs sont informés de la capacité retrouvée de l'AC de générer des certificats.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 5.7.1. Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

5.8 Fin de vie d'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

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

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC :

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats) ;
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire ;
- L'AC doit communiquer au point de contact identifié sur le site http://www.ssi.gouv.fr , les principes du plan d'action mettant en oeuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats ;
- L'AC doit tenir informées le SGMAP et l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC procède aux actions suivantes :

- La notification des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- Révoque son certificat ;
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Informe (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Bi-clés d'AC

Suite à l'accord de la PMA pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle (Cf. 6.2.11).

Pour les AC émettant des Certificats RGS ***, les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins deux sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Il est obligatoire qu'il y ait parmi les témoins un officier public (huissier ou notaire). L'ensemble de la cérémonie des clés est enregistré sous vidéo

Pour les autres AC, les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. L'ensemble de la cérémonie des clés est enregistré sous vidéo.

Suite à leur génération, les parts de secrets (données d'activation) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

6.1.1.2 Bi-clés de Porteurs : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (1.3.6.1.4.1.22234.2.9.3.12)

La génération de la bi-clé du porteur est réalisée directement dans le support matériel de la bi-clé par le porteur ou l'AE. Dans tous les cas, la génération a lieu directement dans le support matériel.

Lorsque c'est l'AE qui génère la bi-clé du porteur suite à une demande de certificat émise par une AED, alors la génération est effectuée dans un environnement sécurisé. La bi-clé ainsi générée est bloquée dans le support à l'aide du code d'activation associé. Ce processus peut aussi être utilisé par l'AE même lorsque le porteur se déplace directement auprès de l'AE et a été enregistré par l'AE.

Dans tous les cas, le processus de génération et la procédure de remise de la bi-clé et de son support au porteur permettent de garantir que seul le porteur peut en avoir l'utilisation. Dans tous les cas, aucune information permettant de retrouver tout ou partie de la clé du porteur n'est conservée par l'AC.

6.1.1.3 Bi-clés de Porteurs : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

C'est l'AE qui génère la bi-clé du porteur suite à une demande de certificat émise par une AED ou par l'AE. La génération est effectuée dans un environnement sécurisé en utilisant une ressource cryptographique qualifié renforcée par l'ANSSI. La bi-clé ainsi générée au format Pkcs#12 est protégée à l'aide d'un code P12 associé. Le code P12 est aussi généré par l'AE. Ce processus peut aussi être utilisé par l'AE même lorsque le porteur se déplace directement auprès de l'AE et a été enregistré par l'AE.

Le processus de génération et la procédure de remise de la bi-clé et de son support au porteur permettent de garantir que seul le porteur peut en avoir l'utilisation. Dans tous les cas, aucune information permettant de retrouver tout ou partie de la clé du porteur n'est conservée par l'AC.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

6.1.2 Transmission de la clé privée à son propriétaire

6.1.2.1 Bi-clés de Porteurs : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (1.3.6.1.4.1.22234.2.9.3.12)

Lorsque le porteur génère lui-même sa bi-clé sur demande de l'AE, il doit changer son code d'activation lors de cette opération. La clé reste donc constamment sous le control du porteur. La clé ne sort donc jamais du support matériel et donc l'AC ne conserve pas de copie de la clé privée.

Lorsque l'AE génère la bi-clé du porteur, cette opération est effectuée de manière sécurisée de sorte que l'AE ne puisse pas avoir connaissance du code d'activation ni de la bi-clé générée directement dans la carte et immédiatement protégée par le code d'activation du porteur. Lorsque l'AE génère la bi-clé du porteur, alors pour la remise du code d'activation et du support, les deux cas suivants se produisent :

- RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS *** : Porteur enregistré par AED : l'AE transmet le support protégé par le code d'activation à l'AED. L'AED remet ensuite le support ainsi protégé au porteur ou au MC (en fonction du type de demande) lors d'un face à face en authentifiant le Porteur ou le MC à l'aide de la pièce d'identité portée dans la demande de certificat ;
- RGS * : Porteur enregistré par AED ou AE : l'AE transmet le support protégé par le code d'activation au Porteur ;
- RGS **, OID 1.3.6.1.4.1.22234.2.9.3.15 et RGS *** : Porteur enregistré par l'AE : l'AE remet directement le code d'activation au porteur ou le transmet au Porteur (cf. 6.4), et son support protégé par code d'activation directement au porteur ou au MC (en fonction du type de demande) lors d'un face à face en authentifiant le Porteur ou le MC à l'aide de la pièce d'identité portée dans la demande de certificat.

6.1.2.2 Bi-clés de Porteurs : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

Cette opération est effectuée de manière sécurisée de sorte que l'AE ne puisse pas avoir connaissance du code P12 (transmit directement au Porteur) ni de la bi-clé générée et immédiatement protégée par le code P12 du porteur. Les deux cas suivants se produisent :

- Porteur enregistré par AED : l'AE transmet la bi-clé au format Pkcs#12 protégée par le code P12 à l'AED. L'AED remet ensuite la bi-clé ainsi protégé au porteur ;
- Porteur enregistré par l'AE : l'AE remet directement au porteur sa bi-clé protégée par code P12 directement au porteur.

6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise à l'AC lors de la génération de la bi-clé, sous un format PKCS#10, et lors d'une connexion sécurisée de manière à garantir l'intégrité et la confidentialité de la communication et l'authentification entre l'AC et l'AE.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

L'ensemble des certificats de la chaîne de confiance de l'AC est contenu dans le support qui est remis au porteur lors de la remise du certificat au porteur.

L'ensemble des certificats d'AC sont publiés par l'AC.

Le certificat de l'AC Racine dont dépend l'AC est contenu dans les logiciels d'Adobe.

Le certificat de l'ACR « Class 2 Primary CA », utilisé pour cross-certifié l'AC (Cf. 3.2.6), est diffusé dans la plus part des navigateurs internet.

6.1.5 Taille des clés

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

si les paramètres utilisés dans l'émission de certificats porteurs et AC doivent ou ne doivent pas être modifiés.

L'utilisation de l'algorithme RSA avec la fonction de hachage SHA-256 est utilisée pour l'AC. La taille de la bi-clé de l'AC est d'au moins 2048 bits.

La longueur des clés des certificats porteurs est de 2048 bits pour l'algorithme RSA avec la fonction de hachage SHA-256.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

6.1.6.1 Bi-clé AC

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles évaluées certifiées EAL 4+ et qualifié renforcé.

6.1.6.2 Bi-clés de Porteurs : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (1.3.6.1.4.1.22234.2.9.3.12)

Les bi-clés des porteurs sont générées par le porteur ou l'AE à l'aide d'un support matériel évalué certifié EAL 4+ (conformément au profil de protection SSCD définit par l'ETSI) et qualifié renforcé.

6.1.6.3 Bi-clés de Porteurs : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

Les bi-clés des porteurs sont générées par l'AE à l'aide d'une ressource cryptographique qualifiée renforcée par l'ANSSI.

Le Porteur a ensuite la responsabilité de protéger ses bi-clés conformément aux exigences du RGS.

6.1.7 Objectifs d'usage de la clé

L'utilisation de l'extension "key usage" dans le certificat « Porteur » (et aussi de l'extension « Extended Key Usage » quand elle est présente) et dans les certificats des AC est décrite au § 10 dans les profils de certificats et indique l'objectif d'usage de la clé.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

La ressource cryptographique matérielle de l'AC utilise des générateurs d'aléas qui devront être conformes à l'état de l'art, aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés devront être conformes aux standards en vigueurs ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

L'AC fournit le support matériel au porteur, directement, et s'assure que :

- La préparation des dispositifs de création de signature est contrôlée de façon sécurisée par le prestataire de service ;
- Les supports matériels sont stockés et distribués de façon sécurisée dans l'OSC.

6.2.2 Contrôle de la clé privée par plusieurs personnes

6.2.2.1 AC

L'activation de la clé privée d'AC est contrôlée par au moins 2 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée d'AC font l'objet d'une authentification forte. L'AC est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seul rôles de confiances qui peuvent émettre des certificats.

6.2.2.2 Porteur : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (sauf 1.3.6.1.4.1.22234.2.12.3.3)

Le porteur est responsable de la protection et du contrôle de la clé privée à l'aide de sa donnée d'activation.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

6.2.2.3 Porteur : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

Le porteur est responsable de la protection et du contrôle de la clé privée à l'aide de sa donnée d'activation. La première donnée d'activation est le code P12. Le Porteur a obligation de changer ce code 12 et d'en définir un nouveau qui respecte les exigences du RGS *.

6.2.3 Séquestre de clé privée

Les clés privées d'AC et des porteurs ne font jamais l'objet de séquestre.

6.2.4 Copie de secours de de clé privée

6.2.4.1 AC

La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC. Les sauvegardes de clés privées d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme de fichier chiffrée (AES ou 3DES).

6.2.4.2 Porteur : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (sauf 1.3.6.1.4.1.22234.2.12.3.3)

Le porteur ne peut pas procéder à une copie de sauvegarde de sa clé privée.

6.2.4.3 Porteur : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

Il n'est pas conseillé que le porteur procède à une copie de sauvegarde de sa clé privée.

Toutefois, si Porteur décide de faire une copie de secours de sa bi-clé, il en est alors le seul et unique responsable et doit définir et respecter les moyens et procédures permettant de réaliser l'opération de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS.

6.2.5 Archivage de la clé privée

Les clés privées d'AC ne font jamais l'objet d'archives.

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

Les clés d'AC sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC sont chiffrées au moyen de l'algorithme AES ou 3DES. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC stockées dans des ressources cryptographique matérielles sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 AC

Les clés privées d'AC ne peuvent être activées qu'avec un minimum de 2 personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

6.2.8.2 Porteur : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (sauf 1.3.6.1.4.1.22234.2.12.3.3)

La clé privée d'un porteur est activable à l'aide d'une donnée d'activation. L'activation est nécessaire à chaque utilisation de la clé privée à l'aide du support matériel de la bi-clé. Le porteur doit configurer son support de bi-clé de telle sorte qu'il requière la saisie de la donnée d'activation à chaque utilisation de sa clé privée correspondant au certificat que l'AC a émis.

6.2.8.3 RGS * (OID 1.3.6.1.4.1.22234.2.12.3.3)

La première donnée d'activation est le code P12 que le Porteur se doit de changer avant d'utiliser sa bi-clé dans le cadre d'une application.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

La clé privée d'un porteur est activable à l'aide d'une donnée d'activation. L'activation est nécessaire à chaque utilisation de la clé privée à l'aide du logiciel qui utilise la bi-clé. Le porteur doit configurer le logiciel, lorsque cela est possible, qui utilise la bi-clé de telle sorte qu'il requière la saisie de la donnée d'activation à chaque utilisation de sa clé privée correspondant au certificat que l'AC a émis.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 AC

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC ont été activées ne sont pas laissées sans surveillance ou accessible à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

Les ressources cryptographiques de signature de l'AC sont en ligne uniquement afin de signer des certificats porteurs et des LCR après avoir authentifié la demande de certificat et la demande de révocation.

6.2.9.2 Porteur : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (sauf 1.3.6.1.4.1.22234.2.12.3.3)

La désactivation de la clé privée du porteur est effectuée de façon à garantir que la clé privée, contenue dans le support matériel, est toujours sous le contrôle du porteur.

6.2.9.3 Porteur : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

La désactivation de la clé privée du porteur doit s'effectuer de façon à garantir que la clé privée est toujours sous le contrôle du porteur. Le Porteur est responsable de paramétrer les logiciels qui utilise la bi-clé de telle sorte à respecter les exigences du RGS *.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 AC

Les clés privées d'AC sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la retrouver.

6.2.10.2 Porteur : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (sauf 1.3.6.1.4.1.22234.2.12.3.3)

La destruction de la clé privée du porteur, est effectuée à l'aide du support matériel de la bi-clé en utilisant les fonctions logiques d'effacement pour le support matériel de la bi-clé et/ou en détruisant le support matériel de la bi-clé.

6.2.10.3 Porteur : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

Suite à la récupération de la bi-clé par le Porteur, l'AE et l'AED doivent détruire les bi-clés de manière à garantir qu'aucunes informations restantes ne permettent de retrouver tout ou partie de la clé privée du Porteur.

Dès que la clé est téléchargée par le Porteur, les opérations de destruction de la bi-clé relève de la seule responsabilité du Porteur. La destruction de la clé privée du porteur par le Porteur, et de ses sauvegardes le cas échéant, est effectuée par le Porteur en utilisant un logiciel d'effacement sûr. Le Porteur est le seul responsable du choix des logiciels et moyens de destruction qui permettent de réaliser les exigences du RGS *.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs d'authentification et de signature

Se reporter au § 6.1.6.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (se reporter au § 5.5.2 ci-dessus).

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

6.3.2 Durée de vie des bi-clés et des certificats

6.3.2.1 AC

Comme une AC ne peut émettre de certificats porteurs d'une durée de vie supérieure à celle de son propre certificat, la bi-clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats porteurs émis.

6.3.2.2 Porteur

La durée de vie opérationnelle d'un certificat est limitée par son expiration ou sa révocation. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 AC

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (Se reporter au § 6.1.1.1). Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs après génération pendant la cérémonie des clés. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Porteur : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (sauf 1.3.6.1.4.1.22234.2.12.3.3)

La donnée d'activation est soit générée par le porteur lui-même en présence de l'AE soit par l'AE sans que l'AE puisse avoir connaissance de cette donnée. L'AE transmet le code d'activation par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données par :

- courrier sécurisé au format papier, ou
- SMS ou courrier électronique si le Porteur est techniquement obligé par l'AC de changer son code d'activation).

Les envois du support (cf. § 6.1.2) et du code d'activation, sont séparés dans le temps d'au moins 24 heures. Pour les porteurs enregistrés par l'AE, c'est l'AE qui remet directement lors d'un face à face le code d'activation et le support protégé par code d'activation (Cf. § 6.1.2 et § 4.3).

Les données de déblocage sont générées par l'AE.

Le porteur a la responsabilité de faire en sorte que les clés privées qu'il détient soient protégées par ses données d'activation. Le porteur est obligé de saisir une donnée d'activation d'au moins 4 caractères alphanumériques. Lorsqu'il n'y est pas contraint, il est recommandé au porteur de changer son code d'activation lors de la première utilisation de son support.

6.4.1.3 Porteur : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

La donnée initiale d'activation est générée par l'AE sans que l'AE puisse avoir connaissance de cette donnée. L'AE transmet le code P12 directement au porteur. Les envois de la bi-clé (cf. § 6.1.3) et du code P12, sont séparés dans le temps et dans l'espace. Pour les porteurs enregistrés par l'AE, c'est l'AE qui remet directement la bi-clé protégée par code P12 (Cf. § 6.1.2 et § 4.3).

Le porteur a la responsabilité de faire en sorte que la clé privée qu'il gère soit protégée par une donnée d'activation. Le porteur est obligé de saisir une nouvelle donnée d'activation d'au moins 6 caractères alphanumériques. Il est exigé de la part du porteur de changer son code PIN lors de la première utilisation de sa bi-clé.

6.4.2 Protection des données d'activation

6.4.2.1 AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation sont responsables

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

de leur gestion et de leur protection. Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'une même AC à un même instant.

6.4.2.2 Porteur : RGS ***, OID 1.3.6.1.4.1.22234.2.9.3.15, RGS ** et RGS * (sauf 1.3.6.1.4.1.22234.2.12.3.3)

L'AC conserve les codes d'activation initiaux du porteur et les données de déblocage du support chiffrées.

Le porteur s'assure que la donnée d'activation de la clé privée est protégée en confidentialité de tel sort qu'il soit le seul à pouvoir activer la clé privée contenue sur son support matériel.

6.4.2.3 Porteur : RGS * (1.3.6.1.4.1.22234.2.12.3.3)

L'AE détruit le code P12 du Porteur qu'elle génère.

Le porteur s'assure que la donnée d'activation de la clé privée est protégée en confidentialité de tel sort qu'il soit le seul à pouvoir activer la clé privée.

6.4.3 Autres aspects liés aux données d'activation

Les données d'activation sont changées dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance. Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

Le Porteur a la possibilité de débloquer son support lors d'un face à face auprès de l'AE ou l'AED (uniquement pour l'OID 1.3.6.1.4.1.22234.2.9.3.10, 1.3.6.1.4.1.22234.2.9.3.12, 1.3.6.1.4.1.22234.2.9.3.15). L'authentification du Porteur est effectuée en face à face sur la base d'une pièce officielle d'identité. Toutes les opérations de déblocage de support d'un Porteur notifie automatiquement le Porteur sur son adresse de courrier électronique enregistré par l'AE lors de sa demande de certificat.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une IGC comprend les fonctions suivantes :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Eventuellement, gestion des reprises sur erreur.

Quand un composant d'IGC est hébergé sur une plate forme évaluée au regard d'exigences d'assurance de sécurité, il doit être utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'IGC sont

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

6.5.2 Niveau de qualification des systèmes informatiques

Les composants d'IGC utilisés pour supporter les services d'AC et qui sont hébergés par l'OSC ont été conçus en suivant les recommandations du document du CEN CWA 14167-1 "Security requirement for trustworthy system managing digital certificates for electronic signatures".

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développements des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;
- Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation ;
- Les matériels et logiciels sont dédiés aux activités d'IGC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'IGC ;
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'IGC. Seules les applications nécessaires à l'exécution des activités IGC sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite ;
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système d'AC, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'IGC. Lors de son premier chargement, on vérifie que le logiciel de l'IGC est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

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

En ce qui concerne les logiciels et matériels évalués, l'AC poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

6.7 Mesures de sécurité réseau

L'AC est en ligne accessible par des postes informatiques sous contrôle. Les composantes accessibles de l'IGC sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

Les autres composantes de l'IGC de l'AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système IGC est hébergé refuse tout service, hormis ceux qui sont nécessaires au système IGC, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP). Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

- Du début de validité d'un Certificat ;
- De la révocation d'un Certificat ;
- De l'affichage de mises à jour de LCR.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil de Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats porteurs et AC sont définis par le RFC 5280.

7.1.1 Extensions de Certificats

7.1.1.1 Certificat AC

Les informations principales contenues dans le certificat de l'AC sont les extensions suivantes :

- Authority Key Identifier ;
- Basic Constraint (critique) ;
- Key Usage (critique) ;
- CRL distribution point ;
- Subject Key Identifier.

7.1.1.2 Certificat Porteur

Cf. § 11.

7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est Sha-2WithRSAEncryption: 1.2.840.113549.1.1.11.

7.1.3 Formes de noms

Les formes de noms respectent les exigences du § 3.1.1.1 pour l'identité des porteurs et de l'AC qui est portée dans les certificats émis par l'AC.

7.1.4 Identifiant d'objet (OID) de la Politique de Certification

Les certificats émis par l'AC contiennent l'OID de la PC qui est donné au § 1.2.

7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies"

Pas d'exigence formulée.

7.2 Profil de LCR

7.2.1 LCR et champs d'extensions des LCR

Cf. § 11.

7.3 Profil OCSP

Cf. § 11.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et / ou circonstances des audits

L'ensemble des composantes de l'IGC (y compris les AE des Revendeurs) fait l'objet d'audit périodique de conformité, réalisé par DocuSign France, au moins une fois par an, pour permettre à la PMA d'autoriser l'AC d'émettre ou non (selon le résultat des audits) des certificats porteurs au titre de la présente PC. Cet audit est réalisé dans le cadre de la qualification RGS de l'AC.

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par le COFRAC en France (Se reporter au [PROG_ACCRED]) conformément à [QPSCe] et au [décretRGS] et le programme de l'ANSSI pour la qualification eIDAS.

A ce titre, des audits appelés « audit interne » quand ils sont réalisés par OPENTRUST et « audit externe » quand ils sont réalisés par un auditeur externe sont réalisés de manière régulière. De même, l'AE et l'AED sont informées que dans le cadre du schéma de qualification utilisé pour qualifier l'AC dans son ensemble, dont dépendent l'AE et l'AED, l'auditeur externe, qui audit les composante de l'IGC pour le service complet de gestion des certificats émis par l'AC, se réserve le droit de réaliser des audits dit « inopiné » de l'AED et des AE. La réalisation de ces audits (dit audit externe) n'est pas soumis à obligation de la part de OPENTRUST ni de l'auditeur d'avertissement spécifiques auprès de l'AED et de l'AE et peuvent se réaliser n'importe quand. Une AE qui est totalement autonome pour la gestion des certificats Porteurs, doit obligatoirement être auditée par un auditeur externe, vis-à-vis du RGS (dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par le COFRAC en France (Se reporter au [PROG_ACCRED]) conformément à [QPSCe] et au [décretRGS]) pour les certificats qu'elle gère, et ce de manière régulière.

La démarche et les exigences liées aux audits de qualification sont définies dans [PROG_ACCRED] et par l'ANSSI et ne sont donc pas reprises ici.

8.2 Identités / qualifications des évaluateurs

Les auditeurs doivent démontrer leurs compétences dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la PC. Les auditeurs en charge de l'audit de conformité doivent effectuer l'audit de conformité comme tâche principale. La PMA apporte une attention particulière quant à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit. La PMA effectue elle-même le choix des auditeurs.

8.3 Relation entre évaluateurs et entités évaluées

Les auditeurs en charge de l'audit de conformité sont soit une entreprise privée indépendante de la PMA, soit une entité de la PMA suffisamment séparée de l'AC afin d'effectuer une évaluation juste et indépendante.

La PMA détermine si un auditeur remplit cette condition.

8.4 Sujets couverts par les évaluations

L'objectif de l'audit de conformité est de vérifier qu'une composante de l'AC opère ses services en conformité avec la présente PC et sa DPC.

8.5 Actions prises suite aux conclusions des évaluations

La PMA peut décider que l'AC ou l'une de ses composantes n'agit pas en conformité avec les obligations définies dans la présente PC. Quand une telle décision est prise, la PMA peut suspendre les opérations de la composante non conforme de l'IGC, ou peut donner l'ordre de cesser toute relation avec la composante en question, ou peut décider que des actions correctives sont à prendre.

Quand l'auditeur en charge de l'audit de conformité trouve une divergence avec les exigences de la présente PC, les mesures suivantes doivent être prises :

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- L'auditeur note la divergence ;
- L'auditeur avise l'entité en question de la divergence. L'entité en avise rapidement la PMA ;
- La partie responsable de la correction de la divergence détermine quelles sont les mesures à prendre en fonction des exigences de la présente PC, et les effectue sans délai avec l'approbation de la PMA.

Suivant la nature et la gravité de la divergence, et la rapidité avec laquelle elle peut être corrigée, la PMA peut décider de suspendre temporairement le fonctionnement de l'AC, de révoquer le certificat émis par l'AC, ou de prendre toute autre mesure qu'il juge opportune.

Quand les actions correctives sont réalisées, l'AC en informe la PMA et lui fournit un rapport de mise à hauteur, pour évaluation.

8.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à la PMA comme prévu au § 8.1 ci-dessus. Ce rapport cite les versions des PC et DPC utilisées pour cette évaluation. Quand nécessaire, le rapport de contrôle peut être diffusé comme prévu au § 8.5 ci-dessus. Le Rapport de Contrôle de Conformité n'est rendu disponible à des tiers utilisateurs sur Internet.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Les conditions tarifaires sont communiquées au Client par OpenTrust ou le revendeur.

9.1.2 Tarifs pour accéder aux certificats

Les certificats de la chaîne de confiance sont accessibles par les utilisateurs de certificats gratuitement.

Les certificats Porteurs ne sont pas publiés.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Le service de publication de l'AC (qui contient la LCR pour les certificats Porteurs et d'AC) est accessible gratuitement sur Internet.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

La politique de remboursement applicable est définie dans les conditions générales d'utilisation à destination du Porteur.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

DocuSign France atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations décrite dans ce document.

9.2.2 Autres ressources

DocuSign France dispose de ressources financières suffisantes à son bon fonctionnement et à l'accomplissement de sa mission.

9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité utilisatrice du fait d'un manquement par l'AC à ses obligations, l'AC pourra être amené à dédommager l'entité utilisatrice dans la limite de la responsabilité de l'AC définie dans les conditions générales d'utilisation et les contrats établis avec les revendeurs.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- La partie non-publique de la DPC de l'AC ;
- Les clés privées de l'AC, des composantes et des Porteurs ;
- Les données d'activation associées aux clés privées d'AC et des Porteurs ;
- Tous les secrets de l'IGC ;
- Les journaux d'évènements des composantes de l'IGC ;
- Le dossier d'enregistrement du porteur ;
- Les causes de révocations, sauf accord explicite du porteur ;
- La politique de sécurité interne de l'AC ;
- Les parties de la DPC considérées comme confidentielles.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Par ailleurs, l'AC garantit que seuls ses personnels dans des rôles de confiance autorisés, les personnels contrôleurs dans la réalisation des audits de conformité, ou d'autres personnes détenant le besoin d'en connaître, ont accès et peuvent utiliser ces informations confidentielles.

9.3.2 Informations hors du périmètre des informations confidentielles

Les données figurant dans le certificat ne sont pas considérées comme confidentielles.

9.3.3 Responsabilité en termes de protection des informations confidentielles

L'AC a mis en place et respecte des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles au sens de l'article 9.3.1 ci-dessus.

A cet égard, l'AC respecte notamment la législation et la réglementation en vigueur sur le territoire français. En particulier, il est précisé qu'elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

La collecte et l'usage de données personnelles par les composantes de l'IG dans le cadre du traitement des demandes de certificats sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi CNIL.

9.4.2 Informations à caractère personnelles

L'AC considère que les informations suivantes sont des informations à caractère personnel :

- Données d'identification contenues dans les dossiers d'enregistrement ;
- Demande (renseignée) d'émission de certificat ;
- Demande (renseignée) de révocation de certificat ;
- Motif de révocation des certificats.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AC a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles au sens de l'article 9.4.1 ci-dessus dans le cadre de la délivrance et la gestion d'un certificat de porteur.

A cet égard, l'AC respecte notamment la législation et la réglementation en vigueur sur le territoire français, en particulier, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés révisée 2006.

En application de l'article 34 de la loi Informatique et Libertés du 6 janvier 1978, les porteurs disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent comme convenu et décrit dans la demande de certificat et les CGU associés. Pour l'exercer, les porteurs doivent s'adresser à DocuSign France suivant les moyens de contact indiqués dans les CGU.

Pour toute autre information relative à l'exercice de leurs droits en matière de données à caractère personnel, les signataires peuvent s'adresser au Correspondant Informatique et Libertés de DocuSign France suivant les moyens de contact indiqués dans les CGU.

Lorsqu'un revendeur est utilisé alors, il doit se conformer aux exigences de la CNIL et de la présente PC pour la gestion des données personnelles. DocuSign France reporte ce type d'exigence dans le contrat avec le Revendeur.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

9.4.5 Notification et consentement d'utilisation de données personnelles

Aucune des données à caractère personnel communiquées lors de l'enregistrement ne peut être utilisée par l'IGC, pour une autre utilisation autre que celle définie dans le cadre de la PC, sans consentement exprès et préalable de la part du porteur, du MC le cas échéant et du Représentant Habilité ou une personne autorisée par le Représentant Habilité. Les consentements du porteur, du MC et du Représentant Habilité pour l'utilisation desdites données pour celle définie dans le cadre de la PC sont considérés comme obtenus lors de la soumission de la demande de certificat signée et du fait de l'acceptation par le porteur du certificat émis par l'AC.

Le Porteur, MC et Représentant habilité ou la personne désignée par le Représentant Habilité acceptent que les données personnelles les concernant recueillies lors de la demande de certificats fassent l'objet d'un traitement informatique aux seules fins : d'être authentifié par l'AE et le cas échéant l'AED, de permettre les vérifications nécessaires à la personnalisation et la gestion des support, des données d'activation et la délivrance des certificats, à leur renouvellement et à leur révocation, de permettre la construction de l'identité portée dans les certificats et d'apporter les preuves nécessaires à la gestion des certificats.

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

L'AC agit conformément aux réglementations européenne et française et dispose de procédures sécurisées pour permettre l'accès aux autorités judiciaires sur décision judiciaire ou autre autorisation légale aux données à caractère personnel.

9.4.7 Autres circonstances de divulgation d'informations personnelles

L'AC obtient l'accord des signataires d'une demande de certificat (se reporter au § 9.4.5) de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, …) est sanctionnée par le Code de la propriété intellectuelle.

L'AC détient tous les droits de propriété intellectuelle et elle est propriétaire de la PC et de la DPC associée, des certificats émis par l'AC.

Le porteur détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats porteurs émis par l'AC et dont il est propriétaire.

L'entité légale détient tous les droits de propriété intellectuelle sur les informations de l'entité légales contenues dans les certificats Porteurs et dont elle est propriétaires.

9.6 Interprétations contractuelles et garanties

Les composantes de l'IGC, les Clients et la communauté d'utilisateurs de certificats sont responsables pour tous dommages occasionnés en suite d'un manquement de leurs obligations respectives telles que définies aux termes de la PC, des CGU et des contrats.

9.6.1 Obligations communes

Les obligations communes des différentes composantes de l'IGC sont :

- Assurer l'intégrité et la confidentialité des clés privées dont elles sont dépositaires, ainsi que des données d'activation desdites clés privées, le cas échéant ;
- N'utiliser les clés publiques et privées dont elles sont dépositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- Mettre en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent ;

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- Documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'IGC ;
- Respecter et appliquer les termes de la présente PC qu'elles reconnaissent ;
- Accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées ;
- Respecter les conventions qui les lient aux autres entités composantes de l'IGC.

9.6.2 Obligations et garanties de la PMA

Les obligations de la PMA sont les suivantes :

- L'élaboration de la PC et de la DPC ;
- L'audit de l'AC ;
- Le contrôle de la relation contractuelle avec le porteur agissant en tant qu'AE ;
- Documente les schémas de certification qu'elle entretient avec des AC tierces.

9.6.3 Obligations et garanties de l'AC

L'AC s'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de certificats porteurs.

L'AC est responsable du maintien de la conformité aux procédures prescrites dans la présente PC. L'AC fournit tous les services de certification en accord avec sa DPC. Les obligations communes aux composantes de l'AC sont :

- Protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;
- N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC ;
- Respecter et appliquer les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC doit être transmise à la composante concernée) ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC ;
- Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- Met à la disposition de l'AE l'ensemble des moyens techniques nécessaires à la réalisation de ses obligations ;
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

L'AC est responsable de la conformité de sa PC, avec les exigences émises dans les PC Types du RGS pour le niveau de sécurité mis en œuvre par la présente PC. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences des PC Types, par elle-même ou l'une de ses composantes. Elle prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture,

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

l'altération ou le détournement des données personnelles des porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée.

9.6.4 Obligations de l'AE

Les obligations de l'AE sont les suivantes :

- L'authentification du porteur ;
- L'authentification de la demande de certificat ;
- L'authentification de la demande de révocation ;
- La personnalisation des supports des porteurs ;
- La transmission des supports protégés par code PIN aux AED ou directement aux Porteurs ;
- Générer les bi-clés et les codes P12 ;
- Détruire les bi-clés une fois transmises à l'AED ou au Porteur ;
- La transmission des bi-clés protégées par code P12 aux AED ou leurs remises directe aux Porteurs ;
- L'envoi des codes P12 aux porteurs ;
- L'authentification des demandes de déblocage de support ;
- L'envoi sécurisé des codes PIN aux porteurs ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC ;
- Respecter la PC et la DPC de l'AC ;
- En cas de délégation complète de l'AE, respecter les modalités du contrat établit avec DOCUSIGN FRANCE.

9.6.4.1 Obligations et garanties de l'AED

Les obligations de l'AED sont :

- L'authentification du porteur ;
- L'authentification de la demande de certificat ;
- L'authentification de la demande de révocation ;
- L'authentification des demandes de déblocage de support ;
- La vérification de la complétude des dossiers d'enregistrement des porteurs avant leur remise à l'AE ;
- Remettre aux porteurs leur support ou au MC ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC ;
- Respecter la PC et la DPC de l'AC ;
- Respecter les obligations qui le lient à l'AE.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

9.6.5 Obligations et garanties du porteur

Les obligations du porteur sont :

- Protéger en confidentialité et intégrité les informations confidentielles qu'il détient (clé privée et donnée d'activation) ;
- Transmettre la clé publique, correspondante à la clé privée, à l'AE ;
- Se conformer à toutes les exigences de la PC et de la DPC associée ;
- Changer son code d'activation avant d'utiliser pour la première fois son support ;
- Garantir que les informations qu'il fournit à l'AE sont complètes et correctes ;
- Prendre toutes les mesures raisonnables pour éviter l'utilisation non autorisée de sa clé privée et en protéger la confidentialité ;
- Aviser immédiatement l'AE en cas de besoin de révocation de son certificat.

9.6.6 Obligations et garanties du SP

Les obligations du SP sont :

- De publier les LCR ;
- De publier les certificats d'AC ;
- De publier la PC et les CGU associées ;
- De garantir les taux de disponibilités des informations publiées ;
- De protéger les accès au SP.

9.6.7 Obligations et garanties des autres participants

9.6.7.1 Obligations et garanties de l'UC

Les obligations de l'UC sont de valider un certificat SSL à l'aide de la LCR ou du service OCSP fournit par DOCUSIGN FRANCE.

9.6.7.2 Obligations et garanties du MC

Les obligations du MC sont :

- L'authentification du porteur ;
- L'authentification de la demande de certificat ;
- L'authentification de la demande de révocation ;
- La vérification de la complétude des dossiers d'enregistrement des porteurs avant leur remise à l'AE ou à une AED ;
- Remettre aux porteurs leur support ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC ;
- Respecter la PC et la DPC de l'AC ;
- Respecter les obligations qui le lient au Client.

9.7 Limite de garantie

L'AC garantit au travers de ses services d'IGC :

- L'identification et l'authentification de l'AC avec son certificat auto signé ;
- L'identification et l'authentification des porteurs avec les certificats générés par l'AC ;

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Ces garanties sont exclusives de toute autre garantie de l'AC.

L'émission de Certificats, conformément à la PC, ne fait pas de l'une des composantes de l'IGC, un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du porteur et du Client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

En conséquence de quoi, les porteurs, les Clients et les utilisateurs de Certificat sont des personnes juridiquement et financièrement indépendantes de l'AC et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'AC ou de l'une des composantes de l'IGC. Les services de certification (Se reporter au § 1.3) ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre.

Le fait que le nom d'une organisation soit dans un certificat et utilisé à des fins de signature électronique ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur du porteur.

9.8 Limite de responsabilité

DocuSign France n'est pas responsable quant à la forme, la suffisance, l'exactitude, l'authenticité la falsification ou l'effet juridique des documents et informations remis lors de la demande d'émission, de renouvellement ou de révocation d'un Certificat.

DocuSign France ne garantit pas l'exactitude des informations fournies par le Porteur et le Client à l'utilisateur de certificat, ni les conséquences d'une négligence ou d'un manque de précaution ou de sécurité imputable au Porteur.

En outre, le Porteur demeure responsable à l'égard de DocuSign France de toute utilisation non autorisée :

- du Certificat et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée ;
- du Certificat et des dommages qui pourraient en résulter.

En outre, le Porteur demeure responsable à l'égard de DocuSign France de toute utilisation non autorisée du Certificat et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée.

DocuSign France n'assume aucun engagement ni responsabilité quant aux conséquences dues à tout retards, perte, altération, destruction, utilisation frauduleuse des données, transmission accidentelle de virus ou tout autre élément nuisible via toute télécommunication telle que Internet. En outre, DocuSign France n'est pas responsable de la qualité de la liaison internet du Client.

Dans le cas où la responsabilité de DocuSign France serait retenue au titre des présentes Conditions Générales d'Utilisation, il est expressément convenu que DocuSign France serait tenue à réparation des dommages directs certains et immédiats, dont le Client apportera la preuve, dans les limites maximums fixées par DocuSign France.

DocuSign France exclut toute responsabilité en cas de non-respect par le Client de ses obligations définies dans les présentes et dans la PC.

DocuSign France ne sera pas responsable des préjudices indirects ou imprévisibles subis par le Client, tels que notamment les pertes de bénéfices, de vente, de contrats, de chiffre d'affaires, de revenus ou d'économies anticipées, perte de clientèle, préjudice d'exploitation, atteinte à l'image de marque, perte de données ou usage de celles-ci, inexactitude ou corruption de fichiers, en relation ou provenant de l'inexécution ou exécution fautive des présentes ou inhérents à l'utilisation des Certificats émis par DocuSign France.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure au sens de l'article 9.15.5 ci-après.

9.9 Indemnités

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'AC vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés lors de la procédure prévue à l'article 9.3 des présentes.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La PC devient effective une fois approuvée par la PMA. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

Selon l'importance des modifications apportées à la PC, la PMA décidera soit de faire procéder à un audit de la PC/DPC des AC concernées, soit de donner instruction à l'AC de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

9.10.3 Effets de la fin de validité et clauses restant applicables

La fin de validité de la PC entraîne la cessation de toutes les obligations et responsabilités de l'AC pour les certificats émis conformément à la PC.

9.11 Amendements à la PC

9.11.1 Procédures d'amendements

La PMA révise sa PC et sa DPC au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de la PMA. Les corrections de fautes d'orthographe ou de frappe qui ne modifient pas le sens de la PC sont autorisées sans avoir à être notifiées.

9.11.2 Mécanisme et période d'information sur les amendements

La PMA donne un préavis d'1 mois au moins aux composantes de l'IGC de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, …) et non sur la forme de la PC et de la DPC.

9.11.3 Circonstances selon lesquelles l'OID doit être changé

Si la PMA estime qu'une modification de la PC modifie le niveau de confiance assuré par les exigences de la PC ou par le contenu de la DPC, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).

9.12 Dispositions concernant la résolution de conflits

La PMA s'assure que tous les accords qu'elle conclut prévoient des procédures adéquates pour le règlement des différends.

Entre autre, l'AC définit sa politique de nommage et propose, et s'autorise dans certains cas, de régler les différends concernant l'identité à inscrire dans un certificat et dans le cas où les parties ne parviendraient pas à un accord amiable, le différend sera réglé par un tribunal français.

Lorsque le différend porte sur une identité, alors il est du ressort de l'AE de gérer et de résoudre le litige.

9.13 Juridictions compétentes

Les dispositions de la politique de certification sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.

9.14 Conformité aux législations et réglementations

La PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux, d'état, locaux et étrangers concernant les, mais non limités aux, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.15 Disposition diverses

9.15.1 Accord global

Le cas échéant, la DPC précisera les exigences spécifiques.

9.15.2 Transfert d'activités

Sauf si spécifié dans d'autres contrats, seule la PMA a le droit d'affecter et de déléguer la PC à une partie de son choix.

9.15.3 Conséquence d'une clause non valide

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention de ladite Politique de Certification.

Les intitulés portés en tête de chaque Article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

9.15.4 Application et renonciation

Les exigences définies dans la PC/DPC doivent être appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

9.15.5 Force majeure

L'AC ne saurait être tenue pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs aux porteurs ou aux UC.

9.16 Autres dispositions

Le cas échéant, la DPC en fournira les détails.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

10 REFERENCES

Les documents référencés sont les suivants :

- [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 ;
- [DIRSIG] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques ;
- [ORDONNANCE] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives ;
- [DécretRGS] Décret relatif à l'Ordonnance n° 2005-1516 du 8 décembre 2005 ;
- [RGS] Référentiel Général de Sécurité – Arrêté ou version de travail publiée. ;
- [PROG_ACCRED] : COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf www.cofrac.fr.

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

11 PROFIL DE CERTIFICAT, CRL AND OCSP

11.1 “KEYNECTIS ICS QUALIFIED CA” CA

11.1.1 Signature (Entreprise et administration) : RGS *** (sans déblocage) : 1.3.6.1.4.1.22234.2.9.3.1

Base Certificate	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C= FR O =KEYNECTIS OU =ICS OU=0002 478217318 CN =KEYNECTIS ICS QUALIFIED CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String1**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	OU	Identification de l’entité légale Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d’espace. Ceci est cohérent avec la formalisation XML proposée par l’INSEE. Pour les entités de droit non français, plusieurs possibilités existent : • soit il n’y a pas d’instance de l’attribut organizationalUnitName conforme à la norme	UTF8String

[1] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

		ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.	
	T	Qualité du porteur au sein de son entité de rattachement	UTF8String
	SN	Numéro pour distinguer les porteurs au CN identique	PrintableString
	CN	Prénom et Nom du porteur	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		54 97 45 c1 ea 00 c5 45 a8 cd db 82 f8 7d cb f5 90 41 a0 78
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Non Repudiation		Set
1.2.840.113583.1.1.9.2	**FALSE**	
1.2.840.113583.1.1.9.2		1
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.1
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Extensions	Criticality (True/False)	Value
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_QUALIFIED_CA.crl URL=ldap://ldap.keynectis.com/cn=KEYNECTIS%20ICS%20QUALIFIED%20CA,o=KEYNECTIS?certificateRevocationList;binary?base?objectclass=crlDistributionPoint
Authority Information Access	**FALSE**	
Ocsp		http://kvalid.keynectis.com/ics_qualified_ca
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>
Qualified Certificate Statements	**FALSE**	
Statement 1		QC compliance
Statement 2		Secure Signature Creation Device
Time stamping	**FALSE**	
1.2.840.113583.1.1.9.1		URI = http://kstamp.keynectis.com/KSign/

11.1.2 Signature (Entreprise et administration) : EN 319 411 – 2 (Qualified with SSCD) : 1.3.6.1.4.1.22234.2.9.3.15

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS QUALIFIED CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String2**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Au choix : • « VATEU-XXNNNNNN » avec	UTF8String

[2] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

		XX=code pays EU et NNNNNN=numéro de TVA intracommunautaire • « NTRXX-YYNNNNNN » avec XX=code pays, YY=sous-division si nécessaire (par exemple code de l'état pour les USA), et NNNNNN=numéro d'enregistrement de l'entreprise	
	T	Qualité du porteur au sein de son entité de rattachement	UTF8String
	serialNumber	Numéro pour distinguer les porteurs au CN identique	PrintableString
	givenName	Prénom du Porteur	UTF8String
	surName	Nom du porteur	UTF8String
	CN	Prénom et Nom du porteur tel qu'indiqué sur sa pièce d'identité	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		54 97 45 c1 ea 00 c5 45 a8 cd db 82 f8 7d cb f5 90 41 a0 78
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Non Repudiation		Set
Digital Signature		Set
1.2.840.113583.1.1.9.2	**FALSE**	
1.2.840.113583.1.1.9.2		1
Extended Key Usage	**FALSE**	
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Service)		Set
1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.15
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_QUALIFIED

Extensions	Criticality (True/False)	Value
		_CA.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp-id.dsf.docusign.net/ics_qualified_ca
caIssuers		http://crt.dsf.docusign.net/keynectisicsqualifiedca.p7c
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>
Qualified Certificate Statements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal
esi4-qcStatement-4		*No value (SSCD)*
esi4-qcStatement-6		QcType=id-etsi-qct-esign
esi4-qcStatement-5		EN: https://pds.dsf.docusign.net/keynectisicsqualifiedca.pdf
1.2.840.113583.1.1.9.1	**FALSE**	
1.2.840.113583.1.1.9.1		http://tss.dsf.docusign.net/certid

11.1.3 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS QUALIFIED CA
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

CRL Extensions	Criticality (True/False)	Value
Expired Certs On CRL	**FALSE**	
expiredCertsOnCRL		2017/03/08 11:35:50 Z

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

11.2 AC : KEYNECTIS ICS ADVANCED Class 3 CA

11.2.1 Authentification (Entreprise et administration) : RGS ** : 1.3.6.1.4.1.22234.2.9.3.13

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	O =KEYNECTIS OU =ICS OU=0002 478217318 CN =KEYNECTIS ICS ADVANCED Class 3 CA C= FR		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String3**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	OU	Identification de l'entité légale Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette	UTF8String

[3] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

		identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent : • soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.	
	T	Qualité du porteur au sein de son entité de rattachement	UTF8String
	SN	Numéro pour distinguer les porteurs au CN identique	PrintableString
	CN	Prénom et Nom du porteur	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		6a 09 14 a8 9a 3b 9f 1e c3 cd 1f 2f 01 3d 54 76 65 0f de fd
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	

Extensions	Criticality (True/False)	Value
Digital Signature		Set
1.2.840.113583.1.1.9.2	**FALSE**	
1.2.840.113583.1.1.9.2		1
Extended Key Usage	**FALSE**	
Id-kp-clientAuth		Yes
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.13
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_ADVANCED_Class_3_CA.crl URL=ldap://ldap.keynectis.com/cn=KEYNECTIS%20ICS%20ADVANCED%20Class%203%20CA,o=KEYNECTIS?certificateRevocationList;binary?base?objectclass=crlDistributionPoint
Authority Information Access	**FALSE**	
Ocsp		http://kvalid.keynectis.com/ics_advanced_class_3_ca
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>
Time stamping	**FALSE**	
1.2.840.113583.1.1.9.1		URI = http://kstamp.keynectis.com/KSign/

11.2.2 Signature et authentification (Entreprise et administration) : RGS ** et EN 319 411 – 1 NCP+ : 1.3.6.1.4.1.22234.2.9.3.10

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS ADVANCED Class 3 CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String4**
	C	Code pays ISO 3166-1 sur 2 caractères.	PrintableString

[4] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

		Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Au choix : • « VATEU-XXNNNNNN » avec XX=code pays EU et NNNNNN=numéro de TVA intracommunautaire • « NTRXX-YYNNNNNN » avec XX=code pays, YY=sous-division si nécessaire (par exemple code de l'état pour les USA), et NNNNNN=numéro d'enregistrement de l'entreprise	UTF8String
	OU	Identification de l'entité légale Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent : • soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.	UTF8String
	T	Qualité du porteur au sein de son entité de rattachement	UTF8String
	serialNumber	Numéro pour distinguer les porteurs au CN identique	PrintableString
	givenName	Prénom du porteur	UTF8String
	surName	Nom du porteur	UTF8String
	CN	Prénom et Nom du porteur tel qu'indiqué sur sa pièce d'identité	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm &	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

OID)	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		6a 09 14 a8 9a 3b 9f 1e c3 cd 1f 2f 01 3d 54 76 65 0f de fd
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Non Repudiation		Set
1.2.840.113583.1.1.9.2	**FALSE**	
1.2.840.113583.1.1.9.2		1
Extended Key Usage	**FALSE**	
Id-kp-clientAuth		Yes
Id-kp-emailProtection		Yes
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Service)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.10
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_ADVANCED_Class_3_CA.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp-id.dsf.docusign.net/ics_advanced_class_3_ca
caIssuers		http://crt.dsf.docusign.net/keynectisicsadvancedclass3ca.p7c
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>
1.2.840.113583.1.1.9.1	**FALSE**	
1.2.840.113583.1.1.9.1		http://tss.dsf.docusign.net/certid
QCStatements	**FALSE**	
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

11.2.3 Signature et authentification (Offre SPM) (Entreprise et administration) : RGS * et EN 319 411 – 1 LCP : 1.3.6.1.4.1.22234.2.9.3.12

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS ADVANCED Class 3 CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String5**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Au choix : • « VATEU-XXNNNNNN » avec XX=code pays EU et NNNNNN=numéro de TVA intracommunautaire • « NTRXX-YYNNNNNN » avec XX=code pays, YY=sous-division si nécessaire (par exemple code de l'état pour les USA), et NNNNNN=numéro d'enregistrement de l'entreprise	UTF8String
	OU	Identification de l'entité légale Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent : • soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002	UTF8String

[5] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

		• soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.	
	T	Qualité du porteur au sein de son entité de rattachement	UTF8String
	serialNumber	Numéro pour distinguer les porteurs au CN identique	PrintableString
	givenName	Prénom du porteur si pas de pseudo et vide si pseudo	UTF8String
	surName	Nom du porteur si pas de pseudo et vide si pseudo	UTF8String
	pseudonym	Pseudonyme si choisi par le porteur et vide si pas de pseudo	UTF8String
	CN	Prénom et Nom du porteur tel qu'indiqué sur sa pièce d'identité si pas pseudo, si pseudo = valeur du pseudo	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		6a 09 14 a8 9a 3b 9f 1e c3 cd 1f 2f 01 3d 54 76 65 0f de fd
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Non Repudiation		Set
1.2.840.113583.1.1.9.2	**FALSE**	
1.2.840.113583.1.1.9.2		1
Extended Key Usage	**FALSE**	
Id-kp-clientAuth		Yes
Id-kp-emailProtection		Yes
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Signing)		Set
Certificate Policies	**FALSE**	

Extensions	Criticality (True/False)	Value
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.12
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_ADVANCED_Class_3_CA.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp-id.dsf.docusign.net/ics_advanced_class_3_ca
caIssuers		http://crt.dsf.docusign.net/keynectisicsadvancedclass3ca.p7c
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>
1.2.840.113583.1.1.9.1	**FALSE**	
1.2.840.113583.1.1.9.1		http://tss.dsf.docusign.net/certid
QCStatements	**FALSE**	
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal

11.2.4 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS ADVANCED Class 3 CA
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number (plus one each time)

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

11.3 AC « Keynectis CA for Enterprise signature »

11.3.1 Offre Cert ID : Classic : 1.3.6.1.4.1.22234.2.12.3.3

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	CN = Keynectis CA for Enterprise signature OU = 0002 478217318 O = Keynectis C = FR		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String6**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	OU	Identification de l'entité légale Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent :	UTF8String

[6] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

		• soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.	
	T	Qualité du porteur au sein de son entité de rattachement	UTF8String
	SN	Numéro pour distinguer les porteurs au CN identique	PrintableString
	CN	Prénom et Nom du porteur	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		b2 0c 12 34 a4 7b 79 96 a9 7a ef f3 bf dc 0d 0e 34 08 5b ec
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Non Repudiation		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.12.3.3
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False

Extensions	Criticality (True/False)	Value
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/Keynectis_CA_for_Enterprise_signature.crl URL=ldap://ldap.keynectis.com/CN=Keynectis%20CA%20for%20Enterprise%20signature,OU=0002%20478217318,O=KEYNECTIS,C=FR?certificateRevocationList;binary?base?objectclass=pkiCA
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>

11.3.2 CRL

CRL Fields	Value
Version	1 (=version 2)
Issuer	CN = Keynectis CA for Enterprise signature OU = 0002 478217318 O = Keynectis C = FR
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number (plus one each time)

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

11.4 OCSP

Field	Requirements
version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature

Docusign Envelope ID: 7D112C55-B559-440E-A020-67FA5F588687

Field	Requirements
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Subscriber's certificate status made in the CRL.
Next Update	Date of the next CRL.
CertStatus	"Good", "Revoked" or "unknown"
nonce	Used if and only if the user Application provides a value for this field and reused in full.
extensions	No extension referenced