

Référentiel :	Sous-Référentiel :	Référence :	Statut :
Sécurité	PKI	PPKIG034 1.2.250.1.16.12.5.41.1.4.1.1.1	validé
Validé par :	Fonction :	Date :	Signature :
MMI	Responsable Sécurité	13/03/2013	
Approuvé par :	Fonction :	Date° :	Signature :
JMT	Autorité de Gouvernance IGC	13/03/2013	
Diffusion auprès de :	Publique		
En accès pour :	Public. Mise à disposition sur site web (http://pki.almerys.com)		
Localisation :			
Sommaire	<p>AVERTISSEMENT</p> <p>1. INTRODUCTION</p> <p>2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES.....</p> <p>3. IDENTIFICATION ET AUTHENTIFICATION</p> <p>4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS</p> <p>5. MESURES DE SECURITE NON TECHNIQUES</p> <p>6. MESURES DE SECURITE TECHNIQUES</p> <p>7. PROFILS DES CERTIFICATS, OCSP ET DES LCR.....</p> <p>8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS.....</p> <p>9. AUTRES PROBLEMATIQUES METIERS ET LEGALES.....</p> <p>10. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE</p>		
Date de péremption	N/A	Responsable de l'actualisation	Autorité de Gouvernance IGC
Version	Date	Modifications	Auteur
v1.1	16/10/2012	Version validée pour publication	MMI
V1.2	13/03/2013	Version après modification mineurs	MMI

• **Date d'entrée en vigueur**

Le présent document contient des informations qui sont la propriété d'Almerys. L'acceptation de ce document par son destinataire, implique de la part de ce dernier, la reconnaissance du caractère confidentiel de son contenu et l'engagement de n'en faire aucune reproduction, aucune transmission à des tiers, aucune divulgation et aucune utilisation commerciale sans l'accord préalable d'Almerys.

Sommaire détaillé

AVERTISSEMENT	8
1. INTRODUCTION	9
1.1 Présentation générale	9
1.1.1 Signature électronique Almerys	9
1.2 Identification du document	11
1.3 Entités intervenant dans l'IGC.....	11
1.3.1 Autorité de certification (AC).....	12
1.3.2 Autorité de Gouvernance (AG).....	13
1.3.3 Service de stockage sécurisé des Bi-clés des Utilisateurs	13
1.3.4 Autorité d'Enregistrement (AE).....	13
1.3.5 Module client <i>ebeeSignClient</i> ou Service d'enregistrement en ligne <i>ebeeSignWeb</i>	13
1.3.6 Utilisateur, Porteur de certificat.....	14
1.3.7 Applications utilisatrices des certificats	14
1.3.8 Autres participants	14
1.4 Usage des certificats	14
1.4.1 Domaines d'utilisation applicables.....	14
1.4.2 Domaines d'utilisation interdits	15
1.5 Gestion de la PC	15
1.5.1 Entité gérant la PC	15
1.5.2 Point de contact.....	15
1.5.3 Entité déterminant la conformité d'une DPC avec cette PC	15
1.5.4 Procédure d'approbation de la conformité de la DPC	16
1.6 Acronymes et définitions	16
1.6.1 Acronymes.....	16
1.6.2 Définitions.....	17
2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	21
2.1 Entités chargées de la mise à disposition des informations	21
2.2 Informations devant être publiées.....	21
2.3 Délais et fréquences de publication.....	21
2.4 Contrôle d'accès aux informations publiées	21
3. IDENTIFICATION ET AUTHENTIFICATION	23
3.1 Nommage.....	23
3.1.1 Type de noms	23
3.1.2 Nécessité d'utilisation de noms explicites.....	23
3.1.3 Anonymisation ou pseudonymisation des Utilisateurs.....	23
3.1.4 Règles d'interprétation des différentes formes de nom	23
3.1.5 Unicité des noms	23
3.1.6 Identification, authentification et rôle des marques déposées	24
3.2 Validation initiale de l'identité	24
3.2.1 Méthode pour prouver la possession de la clé privée	24
3.2.2 Validation de l'identité d'un organisme	24
3.2.3 Validation de l'identité d'un individu	24
3.2.4 Informations non vérifiées de l'Utilisateur.....	24
3.2.5 Validation de l'autorité du demandeur	24

3.2.6.	Critères d'interopérabilité	24
3.3	Identification et validation d'une demande de renouvellement des clés	24
3.3.1.	Identification et validation pour un renouvellement courant	25
3.3.2.	Identification et validation pour un renouvellement des clés après révocation	25
3.4	Identification et validation d'une demande de révocation	25
3.4.1.	Demande faite via les moyens informatiques	25
3.4.2.	Demande faite via Service support.....	25
4.	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS.....	26
4.1	Demande de certificat.....	26
4.1.1.	Origine d'une demande de certificat.....	26
4.1.2.	Processus et responsabilités pour l'établissement d'une demande de certificat	26
4.2	Traitement d'une demande de certificat	26
4.2.1.	Exécution des processus d'identification et de validation de la demande	26
4.2.2.	Acceptation ou rejet de la demande	27
4.2.3.	Durée d'établissement du certificat	27
4.3	Délivrance du certificat	27
4.3.1.	Actions de l'AC concernant la délivrance du certificat	27
4.3.2.	Notification par l'AC de la délivrance du certificat.....	27
4.4	Acceptation du certificat.....	28
4.4.1.	Démarche d'acceptation du certificat	28
4.4.2.	Publication du certificat.....	28
4.4.3.	Notification par l'AC aux autres entités de la délivrance du certificat	28
4.5	Usages de la bi-clé et du certificat	28
4.5.1.	Utilisation de la clé privée et du certificat par le porteur	28
4.5.2.	Utilisation de la clé publique et du certificat par l'Application utilisatrice du certificat.....	29
4.6	Renouvellement d'un certificat.....	29
4.7	Délivrance d'un nouveau certificat suite à changement de la bi-clé	29
4.7.1.	Causes possibles de changement d'une bi-clé	29
4.7.2.	Origine d'une demande d'un nouveau certificat.....	29
4.7.3.	Procédure de traitement d'une demande d'un nouveau certificat	29
4.7.4.	Notification de l'établissement du nouveau certificat	29
4.7.5.	Démarche d'acceptation du nouveau certificat	29
4.7.6.	Publication du nouveau certificat.....	29
4.7.7.	Notification par l'AC aux autres entités de la délivrance du nouveau certificat	30
4.8	Modification du certificat.....	30
4.9	Révocation et suspension des certificats	30
4.9.1.	Causes possibles d'une révocation.....	30
4.9.2.	Origine d'une demande de révocation.....	30
4.9.3.	Procédure de traitement d'une demande de révocation	31
4.9.4.	Délai accordé pour formuler la demande de révocation	32
4.9.5.	Délai de traitement par l'AC d'une demande de révocation.....	32
4.9.6.	Exigences de vérification de la révocation par les Applications utilisatrices de certificats....	32
4.9.7.	Fréquence d'établissement des LCR.....	32
4.9.8.	Délai maximum de publication d'une LCR.....	32
4.9.9.	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats 32	
4.9.10.	Exigences de vérification en ligne de la révocation des certificats par les applications utilisatrices de certificats.....	33
4.9.11.	Autres moyens disponibles d'information sur les révocations	33

4.9.12.	Exigences spécifiques en cas de compromission de la clé privée	33
4.9.13.	Causes possibles d'une suspension	33
4.9.14.	Origine d'une demande de suspension	33
4.9.15.	Procédure de traitement d'une demande de suspension.....	33
4.9.16.	Limites de la période de suspension d'un certificat	33
4.10	Fonction d'information sur l'état des certificats.....	33
4.10.1.	Caractéristiques opérationnelles.....	33
4.10.2.	Disponibilité de la fonction.....	33
4.10.3.	Dispositifs optionnels	34
4.11	Fin de la relation entre le porteur et l'AC	34
4.12	Séquestre de clé et recouvrement.....	34
4.12.1.	Politique et pratiques de recouvrement par séquestre des clés	34
4.12.2.	Politique et pratiques de recouvrement par encapsulation des clés de session	34
5.	MESURES DE SECURITE NON TECHNIQUES	35
5.1	Mesures de sécurité physique	35
5.1.1.	Situation géographique et construction des sites	35
5.1.2.	Accès physique	35
5.1.3.	Alimentation électrique et climatisation.....	35
5.1.4.	Vulnérabilité aux dégâts des eaux.....	36
5.1.5.	Prévention et protection incendie.....	36
5.1.6.	Conservation des supports	36
5.1.7.	Mise hors service des supports	36
5.1.8.	Sauvegardes hors site	36
5.2	Mesures de sécurité procédurales.....	36
5.2.1.	Rôles de confiance.....	36
5.2.2.	Nombre de personnes requises par tâches.....	37
5.2.3.	Identification et authentification pour chaque rôle.....	37
5.2.4.	Rôles exigeant une séparation des attributions.....	37
5.3	Mesures de sécurité vis-à-vis du personnel.....	37
5.3.1.	Qualifications, compétences et habilitations requises.....	37
5.3.2.	Procédures de vérification des antécédents	38
5.3.3.	Exigences en matière de formation initiale.....	38
5.3.4.	Exigences et fréquence en matière de formation continue.....	38
5.3.5.	Fréquence et séquence de rotation entre différentes attributions.....	38
5.3.6.	Sanctions en cas d'actions non autorisées	38
5.3.7.	Exigences vis-à-vis du personnel des prestataires externes.....	38
5.3.8.	Documentation fournie au personnel.....	38
5.4	Procédures de constitution des données d'audit	38
5.4.1.	Type d'événements à enregistrer.....	39
5.4.2.	Fréquence de traitement des journaux d'événements.....	40
5.4.3.	Période de conservation des journaux d'événements	40
5.4.4.	Protection des journaux d'événements	40
5.4.5.	Procédure de sauvegarde des journaux d'événements	40
5.4.6.	Système de collecte des journaux d'événements	40
5.4.7.	Notification de l'enregistrement d'un événement au responsable de l'événement	40
5.4.8.	Evaluation des vulnérabilités.....	40
5.5	Archivage des données	41
5.5.1.	Types de données à archiver	41
5.5.2.	Période de conservation des archives.....	41
5.5.3.	Protection des archives	41

5.5.4.	Procédure de sauvegarde des archives	42
5.5.5.	Exigences d'horodatage des données	42
5.5.6.	Système de collecte des archives	42
5.5.7.	Procédures de récupération et de vérification des archives.....	42
5.6	Changement de clé d'AC	42
5.7	Reprise suite à compromission et sinistre	43
5.7.1.	Procédures de remontée et de traitement des incidents et des compromissions	43
5.7.2.	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)	43
5.7.3.	Procédures de reprise en cas de compromission de la clé privée d'une composante.....	43
5.7.4.	Capacités de continuité d'activités suite à un sinistre	43
5.8	Fin de vie de l'IGC.....	43
6.	MESURES DE SECURITE TECHNIQUES	46
6.1	Génération et installation de bi-clés	46
6.1.1.	Génération des bi-clés.....	46
6.1.2.	Transmission de la clé privée à son propriétaire.....	47
6.1.3.	Transmission de la clé publique à l'AC	47
6.1.4.	Transmission de la clé publique de l'AC aux applications utilisatrices de certificats	47
6.1.5.	Tailles des clés	47
6.1.6.	Vérification de la génération des paramètres des bi-clés et de leur qualité	47
6.1.7.	Objectifs d'usage de la clé	47
6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques.....	48
6.2.1.	Standards et mesures de sécurité pour les modules cryptographiques	48
6.2.2.	Contrôle de la clé privée de l'AC par plusieurs personnes	48
6.2.3.	Séquestre de la clé privée.....	48
6.2.4.	Copie de secours de la clé privée	48
6.2.5.	Archivage de la clé privée	49
6.2.6.	Transfert de la clé privée vers / depuis le module cryptographique	49
6.2.7.	Stockage de la clé privée dans un module cryptographique.....	49
6.2.8.	Méthode d'activation de la clé privée.....	49
6.2.9.	Méthode de désactivation de la clé privée	49
6.2.10.	Méthode de destruction des clés privées	49
6.2.11.	Niveau d'évaluation sécurité du module cryptographique	50
6.3	Autres aspects de la gestion des bi-clés.....	50
6.3.1.	Archivage des clés publiques.....	50
6.3.2.	Durées de vie des bi-clés et des certificats.....	50
6.4	Données d'activation	50
6.4.1.	Génération et installation des données d'activation	50
6.4.2.	Protection des données d'activation.....	51
6.5	Mesures de sécurité des systèmes informatiques.....	51
6.5.1.	Exigences de sécurité technique spécifiques aux systèmes informatiques	51
6.6	Mesures de sécurité des systèmes durant leur cycle de vie.....	52
6.6.1.	Mesures de sécurité liées au développement des systèmes	52
6.6.2.	Mesures liées à la gestion de la sécurité	52
6.7	Mesures de sécurité réseau	52
6.8	Horodatage / Système de datation.....	53
7.	PROFILS DES CERTIFICATS, OCSP ET DES LCR	54

7.1	Profil du certificat de l'AC « Almerys User Signing CA NA ».....	54
7.2	Profil du certificat User Signing.....	56
7.3	Profil de LCR	58
8.	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS.....	59
8.1	Fréquences et / ou circonstances des évaluations	59
8.2	Identités / qualifications des évaluateurs.....	59
8.3	Relations entre évaluateurs et entités évaluées.....	59
8.4	Sujets couverts par les évaluations.....	59
8.5	Actions prises suite aux conclusions des évaluations	59
8.6	Communication des résultats	60
9.	AUTRES PROBLEMATIQUES METIERS ET LEGALES.....	61
9.1	Tarifs.....	61
9.2	Responsabilité financière	61
9.3	Confidentialité des données professionnelles	61
9.3.1.	Périmètre des informations confidentielles.....	61
9.3.2.	Informations hors du périmètre des informations confidentielles.....	61
9.3.3.	Responsabilités en terme de protection des informations confidentielles	62
9.4	Protection des données à caractère personnel	62
9.4.1.	Politique de protection des données à caractère personnel	62
9.4.2.	Informations à caractère personnel	62
9.4.3.	Responsabilité en termes de protection des données à caractère personnel.....	62
9.4.4.	Notification et consentement d'utilisation des données à caractère personnel	62
9.4.5.	Conditions de divulgation d'informations à caractère personnel aux autorités judiciaires ou administratives.....	62
9.4.6.	Autres circonstances de divulgation d'informations personnelles	62
9.5	Droits sur la propriété intellectuelle et industrielle.....	62
9.6	Interprétations contractuelles et garanties	63
9.6.1.	Autorité de Certification.....	63
9.6.2.	Autorité de Gouvernance	63
9.6.3.	Autorité d'enregistrement.....	64
9.6.4.	Porteurs de certificats	64
9.6.5.	Applications utilisatrices de certificats	64
9.6.6.	Autres participants	64
9.7	Limite de garantie	64
9.8	Limite de responsabilité.....	64
9.9	Indemnités	65
9.10	Durée et fin anticipée de validité de la PC.....	65
9.10.1.	Durée de validité	65
9.10.2.	Fin anticipée de validité.....	65
9.10.3.	Effets de la fin de validité et clauses restant applicables.....	65
9.11	Notifications individuelles et communications entre les participants.....	65
9.12	Amendements à la PC.....	65
9.12.1.	Procédures d'amendements	65
9.12.2.	Circonstances selon lesquelles l'OID doit être changé.....	66
9.13	Dispositions concernant la résolution de conflits.....	66

9.14	Juridictions compétentes	66
9.15	Conformité aux législations et réglementations.....	66
10.	ANNEXE 1 : DOCUMENTS CITES EN REFERENCE.....	67
10.1	Réglementation.....	67
10.2	Documents techniques	67

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1^{er} 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 d'Almerys.

La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par Almerys 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.

1. INTRODUCTION

1.1 PRESENTATION GENERALE

Dans le cadre de ses offres de services de dématérialisation et de confiance, Almerys met à disposition des Clients de son Service de signature électronique pour le compte de leurs Utilisateurs une Autorité de Certification spécifique, Almerys User Signing CA NA.

Dans ce cadre, le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification (AC) « Almerys User Signing CA NA ». Cette AC est habilitée à délivrer des Certificats de signature pour les Utilisateurs du Service de signature électronique d'Almerys mis à leur disposition par les Clients.

L'objectif de la présente PC est de définir les exigences concernant les Certificats de signature dans toutes les phases de leur cycle de vie. Le Porteur d'un tel Certificat pourra signer des messages, des documents ou formulaires électroniques, assurant ainsi leur non-répudiation et leur intégrité.

Cette Politique de Certification est conforme à la norme ETSI TS 102 042 au niveau LCP.

Les Certificats produits respectent la norme X.509v3 et leur utilisation est dédiée au mécanisme de signature. L'AC « Almerys User Signing CA NA » émet 2 types de certificats : les certificats à usage unique et les certificats réutilisables.

La présente PC traite spécifiquement du cycle de vie des certificats de signature à usage unique.

A un certificat de signature est associé de manière univoque une session de signature électronique établie dans le cadre du Service de signature électronique.

La structure de la présente politique de certification s'appuie sur 2 documents de référence :

- le RFC 3647 de l'IETF « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework »
- et la Politique de Certification Type « Signature » du Référentiel Général de Sécurité (RGS) émis par la l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), réf. 1.2.250.1.137.2.2.1.2.2.2

La section suivante permet d'illustrer l'intérêt de ces Certificats dans le cas du Service de signature électronique proposé par Almerys.

1.1.1. Signature électronique Almerys

Almerys propose une solution de signature électronique multicanale qui permet de dématérialiser les échanges de documents et d'informations, et de créer de la valeur probante dans les phases d'engagement, entre les différentes parties concernées, et d'enregistrement d'informations.

Le schéma suivant permet d'illustrer ces principes dans le cas particulier d'un processus de contractualisation multicanal proposée par une entreprise cliente du Service de signature électronique à ses Utilisateurs :

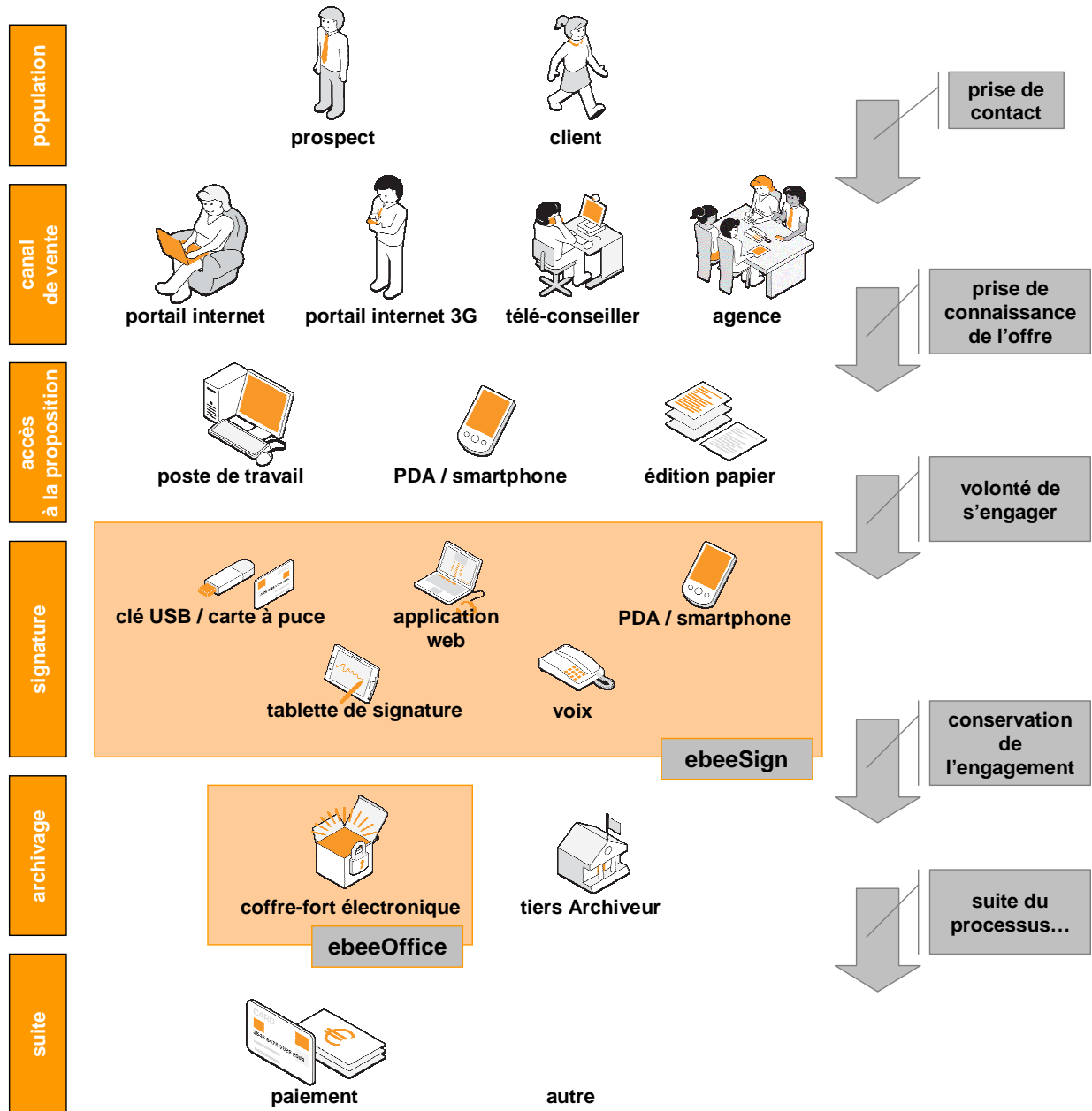


Illustration du principe de contractualisation multicanal

Les services de signature électronique sont appelés par des *Offreurs de Services* (entreprises, institutions, administrations, associations, etc.) afin de mettre à disposition des *Bénéficiaires de Services* (clients, prospects, professionnels, grand public, etc.) les fonctionnalités de signature électronique.

Les Offreurs de Services sont les *Clients* de la plate-forme de signature électronique et les Bénéficiaires de Services en sont les *Utilisateurs*, tel qu'illustré dans la figure suivante :



Les Clients et les Utilisateurs du Service de signature électronique d'Almerys

Dans le cadre de ce Service, l'Utilisateur dispose d'un certificat de signature électronique (identifié par l'OID 1.2.250.1.16.12.5.41.1.4.1.1.1 et objet de la présente PC) qui sera utilisé par les composants du service de signature électronique pour apposer une signature numérique sur les documents présentés par le Client à l'Utilisateur dans le cadre de transactions de contractualisation et de signature.

1.2 IDENTIFICATION DU DOCUMENT

Ce document est la PC de l'AC « Almerys User Signing CA NA » de l'Infrastructure de Gestion de Clés (IGC) d'Almerys – Orange Business Services, pour les certificats de signature à usage unique.

Son identifiant d'objet (OID) est le suivant : 1.2.250.1.16.12.5.41.1.4.1.1.1

Cette référence figure dans les Certificats de signature émis par l'AC « Almerys User Signing CA NA » (cf. section 9.12.2).

La référence du document au sein d'Almerys est la suivante : PPKIG034.

1.3 ENTITES INTERVENANT DANS L'IGC

La décomposition fonctionnelle de l'IGC Almerys qui est retenue dans la présente PC est la suivante :

- **Fonction d'enregistrement** - Cette fonction vérifie les informations d'identification du futur Porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. Elle a également en charge, lorsque cela est nécessaire, la revérification des informations du Porteur lors du renouvellement du Certificat de celui-ci. Cette fonction est divisée en deux phases : phase d'identification du demandeur de Certificat effectuée par le Client en tant qu'Autorité d'enregistrement (cf. §1.3.4 « Autorité d'Enregistrement (AE) ») et phase de collecte des informations

du demandeur par le Service de signature électronique d'Almerys via le module client *ebeeSignClient* ou le service d'enregistrement en ligne *ebeeSignWeb* mis à disposition du Client, qui transmet alors la demande à la fonction adéquate de l'IGC Almerys.

- **Fonction de génération des certificats** – Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les Certificats à partir des informations transmises par la composante chargée de la fonction d'enregistrement et de la clé publique de l'Utilisateur du service provenant de la fonction de génération des éléments secrets de l'Utilisateur chargée en particulier de générer le Bi-clé de l'Utilisateur.
- **Fonction de génération des éléments secrets de l'Utilisateur** – Cette fonction génère les éléments secrets à destination de l'Utilisateur et les prépare en vue de leur stockage sécurisé au niveau des Modules cryptographiques matériels du Service de stockage sécurisé de Bi-clé d'Almerys et de la mise à disposition de la fonction d'activation par l'Utilisateur. Il s'agit en particulier de la bi-clé de l'Utilisateur et des informations d'activation de la clé privée de l'Utilisateur. Cette fonction est déléguée au Service de stockage sécurisé de Bi-clés de l'IGC Almerys (cf. 1.3.5 « Module client *ebeeSignClient* ou Service d'enregistrement en ligne *ebeeSignWeb* »).
- **Fonction de remise à l'Utilisateur** – Cette fonction remet à l'Utilisateur les moyens de contrôle de sa clé privée et de son certificat.
- **Fonction de publication** – Cette fonction met à disposition des différentes parties concernées, les politiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux Porteurs et/ou aux Applications utilisatrices de certificats, hors informations d'état des Certificats. La liste complète des Certificats valides des Porteurs n'est pas fournie publiquement.
La publication des conditions générales de fourniture et d'utilisation des Certificats User Signing, dans le cadre d'un processus métier, sont à la charge des Clients du service de signature électronique.
- **Fonction de gestion des révocations** – Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des Certificats.
Cette fonction ne concerne que les Certificats de signature réutilisables.
- **Fonction d'information sur l'état des certificats** – Cette fonction fournit aux Applications utilisatrices de certificats des informations sur l'état des Certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

La mise en œuvre opérationnelle de ces fonctions peut être effectuée par une ou plusieurs composante(s) de l'IGC (opérateurs techniques et/ou autorités tel que AC, AG, OC, AE, SP, AH, AA ...).

1.3.1. Autorité de certification (AC)

L'**Autorité de Certification (AC)** « Almerys User Signing CA NA » a en charge la fourniture des prestations de gestion des Certificats de signature tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation) et est, à ce titre, identifiée dans ces Certificats en tant qu'émetteur.

L'AC « Almerys User Signing CA NA » appartient à la hiérarchie de confiance d'Almerys (ensemble des AC d'Almerys regroupées au sein de son Infrastructure de Gestion de Clés). A ce titre, la gestion de l'AC « Almerys User Signing CA NA » ainsi que de l'AC Racine est assurée par Almerys.

Les prestations de l'AC « Almerys User Signing CA NA » sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des Bi-clés et des Certificats.

1.3.2. Autorité de Gouvernance (AG)

L'**Autorité de Gouvernance (AG)** est l'autorité responsable de l'ensemble des services de l'IGC Almerys, elle a un pouvoir décisionnaire au sein de l'IGC. Elle définit et fait appliquer les PC et DPC.

Concrètement, il s'agit d'un ou plusieurs représentants d'Almerys ayant un mandat spécifique pour assurer cette fonction.

1.3.3. Service de stockage sécurisé des Bi-clés des Utilisateurs

Almerys met en œuvre un service sécurisé de stockage des Bi-clés des Utilisateurs.

Ce service est hébergé dans les locaux d'Almerys et met en œuvre des Modules cryptographiques matériels répondant au minimum aux exigences du standard FIPS 140-2 level 2.

Seule l'application de signature électronique peut communiquer avec le Module cryptographique matériel pour une création du Bi-clé de signature de l'Utilisateur. A aucun moment, la clé privée de signature de l'Utilisateur ne peut être exportée du Module.

La création et l'activation du Bi-clé d'un Utilisateur n'intervient que si 2 conditions sont remplies :

- le Client a identifié le futur Porteur de Certificat,
- le Porteur s'est doublement identifié pour accéder au Service de signature électronique en ligne d'Almerys et a validé les informations qui lui sont présentées à la signature.

Seul le Porteur a la capacité à utiliser son certificat de signature.

1.3.4. Autorité d'Enregistrement (AE)

L'**Autorité d'enregistrement (AE)** est un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC et les Utilisateurs, Porteurs de certificats *User Signing*. Dans le cas du Service de signature électronique, ce sont les Clients du service qui sont chargés de la relation avec les Utilisateurs, et de leur identification et authentification.

A ce titre, le Client agissant en tant qu'AE assure :

- l'établissement et la transmission de la demande de Certificat de signature à la fonction adéquate de l'AC « Almerys User Signing CA NA » grâce au module client *ebeeSignClient* ou au service d'enregistrement en ligne *ebeeSignWeb* mis à sa disposition ;

C'est le Client en tant qu'AE qui détermine le niveau d'assurance attendu dans le processus d'identification de ses Utilisateurs. Elle établit en conséquence les procédures nécessaires pour assurer ce niveau d'assurance et s'assure de leur mise en œuvre opérationnelle.

L'AE s'engage également au maintien opérationnel des moyens lui permettant d'utiliser le module client *ebeeSignClient* ou le service d'enregistrement en ligne *ebeeSignWeb* mis à sa disposition afin que ce dernier puisse transmettre les demandes de Certificats *User Signing*, et au respect des règles communes d'authentification et de contrôle des flux établies entre l'AE et l'AC « Almerys User Signing CA NA ».

1.3.5. Module client *ebeeSignClient* ou Service d'enregistrement en ligne *ebeeSignWeb*

Almerys met à disposition du Client un module *ebeeSignClient* ou un Service d'enregistrement en ligne, lequel a la charge de transmettre la demande de génération de Bi-clé et de Certificat

La demande de génération du Bi-clé et du Certificat de l'Utilisateur est effectuée automatiquement auprès des fonctions adéquates de l'IGC. Almerys est responsable du bon fonctionnement de son module ebeeSignClient et de son Service d'enregistrement en ligne ainsi que de leur disponibilité et de l'intégrité des informations transmises par le Client, conformément aux accords contractuels passés avec le Client.

1.3.6. Utilisateur, Porteur de certificat

L'Utilisateur, Porteur de certificat, ne peut être qu'une personne physique, à laquelle est remis un Certificat individuel (avec l'identité de l'Utilisateur inscrite dans le Certificat) après contrôle de son identité par l'AE et validation de ses informations par l'AE dans le module ebeeSignClient ou sur le Service d'enregistrement en ligne.

Le Porteur utilise son Certificat pour signer des informations présentées par le Client qui a fait la demande de Certificat User Signing via le module ebeeSignClient ou le Service d'enregistrement en ligne.

L'application de signature électronique supporte plusieurs types de format de présentation des informations du Client, et notamment le format PDF (norme ISO 32000).

1.3.7. Applications utilisatrices des certificats

La présente PC traitant de Certificats de signature, une Application utilisatrice de certificat est un processus qui met en place la vérification d'une signature. C'est donc une application informatique qui est sous la responsabilité d'une personne physique ou morale, et qui utilise un dispositif de vérification de signature afin d'assurer l'Intégrité et la Non-répudiation du document ou du message signé.

Les applications peuvent être notamment :

- le Service de signature électronique d'Almerys qui permet de présenter les informations devant être signées par l'Utilisateur, ainsi que les informations sur la signature associée ;
- le service de vérification de signature Almerys qui permet à partir d'une information ou d'un document signé à l'aide d'un certificat User Signing, de vérifier et d'afficher un statut sur l'état du Certificat utilisé et de la signature ;
- l'application Acrobat Reader™ d'Adobe™ qui permet d'afficher un document au format PDF signé par un Certificat User Signing ainsi que le cartouche d'information sur les signatures associées au document. Cette application doit être correctement configurée pour accepter les Certificats User Signing, notamment la chaîne de certification de l'AC « Almerys User Signing CA NA » doit être reconnue dans le logiciel.

1.3.8. Autres participants

Sans objet pour la présente PC.

1.4 USAGE DES CERTIFICATS

1.4.1. Domaines d'utilisation applicables

1.4.1.1. Bi-clés et certificats des porteurs

Le seul domaine d'utilisation applicable de la présente PC pour les Bi-clés et les Certificats User Signing est le Service de signature électronique Almerys, grâce auquel l'Utilisateur peut signer les formulaires ou documents présentés par le Client.

Remarque : la présentation des documents ou des informations à signer peut être à la charge du Client ou être déléguée à Almerys par le Client.

Par contre, les processus de génération de Certificat et de Bi-clé de signature sont à l'entière charge d'Almerys, quel que soit le contexte du Client. Les processus de vérification de l'identité des Utilisateurs et de gestion des demandes de Certificats et de signatures via le module ebeeSignClient ou le Service d'enregistrement en ligne sont à l'entière charge du Client.

1.4.1.2. Bi-clés et certificats d'AC

Les Bi-clés et Certificats de l'AC « Almerys User Signing CA NA » ne peuvent être utilisés que pour la signature de Certificats User Signing et de LCR.

1.4.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des Bi-clés et des Certificats sont définies au chapitre 4.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par ses Porteurs et ses Applications utilisatrices de certificats.

A cette fin, elle communique à tous les Porteurs et Applications utilisatrices de certificat potentiels les termes et conditions relatives à l'utilisation du Certificat.

1.5 GESTION DE LA PC

1.5.1. Entité gérant la PC

L'entité en charge de l'administration et de la gestion de la politique de certification est l'AG. Elle est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.

A cette fin, elle met en œuvre et coordonne une organisation dédiée, qui statue à échéance régulière, sur la nécessité d'apporter des modifications à la PC.

1.5.2. Point de contact

L'AG est l'entité à contacter pour toutes questions concernant la présente PC.

Autorité de gouvernance IGC

Téléphone : 04 73 74 58 90

Almerys – 46 rue du Ressort – 63967 CLERMONT-FERRAND CEDEX 9

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

Afin de déterminer la conformité de la DPC avec la présente PC, l'AG s'appuie sur les ressources d'Almerys spécialisées dans l'audit et l'évaluation de la sécurité des services et des produits.

Un document interne précise, au sein de l'organisation Almerys, l'entité qui assure cette responsabilité.

Pour les exigences portant sur l'AE, ce sont les Clients qui sont chargés de mesurer l'adéquation de la conformité de la DPC avec la PC, sous réserve que les parties de la DPC la concernant et la présente PC lui soient bien communiquées. L'AG peut également demander à auditer l'AE pour mesurer cette conformité ou obtenir auprès des Clients les documents permettant de s'en assurer.

1.5.4. Procédure d'approbation de la conformité de la DPC

L'approbation de conformité de la DPC par rapport à cette PC fait l'objet d'une procédure interne. L'AG est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place.

1.6 ACRONYMES ET DEFINITIONS

1.6.1. Acronymes

Les acronymes utilisés dans le référentiel de l'IGC Almerys sont les suivants :

AC	Autorité de Certification [Certification Authority (CA)]
AE	Autorité d'Enregistrement [Registration Authority (RA)]
AH	Autorité d'Horodatage [Time-stamping Authority (TA)]
AG	Autorité de Gouvernance [Governance Authority (GA)]
ANSSI	Agence nationale de la sécurité des systèmes d'information
CC	Critères Communs [Common Criteria (CC)]
CEN	Comité Européen de Normalisation
CSP	Cryptographic Service Provider
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification [Certification Practice Statement (CPS)]
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés [Public Key Infrastructure (PKI)]
KC	Cérémonie des clés (Key Ceremony)
LAR	Liste des certificats d'AC Révoqués [Authority Revocation List]
LCR	Liste des Certificats Révoqués [Certificate Revocation List (CRL)]
OC	Opérateur de Certification [Certification Operator (CO)]
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification [Certification Policy (CP)]
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure – X.509
PP	Profil de Protection [Protection Profile (PP)]
PSCE	Prestataire de Services de Certification Electronique
RAE	Responsable d'Autorité d'Enregistrement
RSA	Rivest Shamir Adelman
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

1.6.2. Définitions

Les termes utilisés dans le référentiel de l'IGC Almerys sont les suivants :

Applications utilisatrices :

Services applicatifs exploitant les Certificats émis par l'AC « Almerys User Signing CA NA », par exemple, pour des besoins de vérification de signature de l'Utilisateur.

Authentification :

Action de s'assurer de l'identité d'une personne physique ou morale ou de l'origine d'une communication.

Autorité de Certification (AC) :

Entité qui délivre et est responsable des Certificats électroniques émis et signés en son nom conformément aux règles définies dans la PC et dans la DPC associée.

Dans le cadre de la présente PC, il s'agit de l'AC « Almerys User Signing CA NA » d'Almerys.

Remarque :

L'AC peut assurer elle-même l'exploitation ou la faire gérer par un Opérateur de Services de Certification (OSC ou OC) disposant de locaux sécurisés, du personnel et de l'infrastructure technique qui lui permettront de réaliser l'ensemble des tâches de gestion des certificats pour le compte de l'AC.

Autorité de Certification Racine (ACR) :

Entité qui dispose d'une IGC lui permettant d'enregistrer, de générer, d'émettre et de révoquer des Certificats d'AC (dont l'AC « Almerys User Signing CA NA »), conformément à la PC et à la DPC définies par son AG. L'ACR d'Almerys est auto-certifiée, c'est-à-dire que son certificat est auto-signé.

L'ACR d'Almerys est l'AC « Almerys Root CA1 ».

Autorité d'Enregistrement (AE) :

Entité disposant d'un ensemble de ressources (informatiques et humaines) ayant pour rôle de gérer les relations entre l'AC et les Porteurs de certificat conformément au paragraphe 1.3.4 de la présente PC.

L'AE a pour rôle de vérifier l'identité du futur Porteur de certificat.

Dans le cadre de la présente PC, l'AE est le Client du service de signature électronique d'Almerys. Pour assurer les demandes de génération de Bi-Clés et de Certificats pour ses Utilisateurs, elle s'authentifie et communique les informations nécessaires aux fonctions adéquates de l'IGC via le module ebeeSignClient ou le Service d'enregistrement en ligne mis à sa disposition par Almerys dans le cadre de la fourniture de son Service de signature électronique.

Voir également Client.

Autorité de Gouvernance (AG) :

Entité responsable de l'ensemble des fonctions de l'IGC avec pouvoir décisionnaire.

Bi-clé [Key Pair] :

Couple clé publique/clé privée.

Cérémonie des Clés ou Key Ceremony (KC) :

Réunion spéciale des personnes autorisées pour générer le **Certificat** d'une **AC**. Le Bi-clé de ce Certificat doit être généré avec toutes les précautions nécessaires (voir la DPC) pour éviter sa compromission.

Certificat électronique :

Fichier électronique attestant qu'un Bi-clé appartient à la personne physique ou morale ou à l'élément matériel identifié, directement ou indirectement (pseudonyme), dans le Certificat. Il est délivré par une AC. En signant le Certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel et le Bi-clé. Le Certificat est valide pendant une durée donnée précisée dans celui-ci.

Dans le cadre de la présente PC, le Certificat désigne un Certificat de signature électronique à usage unique.

Chiffrement :

Transformation cryptographique d'un ensemble de données (clair) en vue de produire un ensemble chiffré (dit cryptogramme).

Client :

Entité cliente ayant décidé de souscrire au Service Almerys, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des Utilisateurs. Dans le cadre de la présente PC, le Client joue le rôle de l'AE et gère les demandes de Certificats User Signing des Utilisateurs qu'il transmet aux fonctions adéquates de l'IGC via le module ebeeSignClient ou le Service d'enregistrement en ligne mis à sa disposition par Almerys.

Voir également Autorité d'enregistrement.

Composante de l'IGC

Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.

Confidentialité :

Propriété d'une *information* ou d'une *ressource* de n'être accessible qu'aux utilisateurs autorisés (création, diffusion, sauvegarde, archivage, destruction).

Déchiffrement :

Transformation d'un cryptogramme en vue de retrouver les données originelles en clair.

Déclaration des Pratiques de Certification (DPC) :

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

Horodatage :

Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.

Infrastructure de Gestion de Clés (IGC) [Public Key Infrastructure (PKI)] :

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

Intégrité :

Propriété d'exactitude, de complétude et d'inaltérabilité dans le temps des *informations* et des *fonctions* de l'information traitée.

Liste des certificats d'AC Révoqués (LAR) :

Liste de certificats d'AC ayant fait l'objet d'une révocation avant la fin de leur période de validité.

Liste de Révocations de Certificats (LRC) [Certificate Revocation List (CRL)] :

Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.

Module cryptographique matériel :

Matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques.

Online Certificate Status Protocol (OSCP) :

Protocole permettant à une personne de vérifier la validité d'un certificat, en particulier s'il a été révoqué.

Non-répudiation :

Impossibilité pour un Porteur ou un Utilisateur de nier sa participation à un échange d'information ; cette participation porte tant sur l'origine de l'information (*imputabilité*) que sur son contenu (*intégrité*).

PKI (Public Key Infrastructure) :

Cf. Infrastructure de Gestion de Clés (IGC).

PKIX (Public Key Infrastructure – X509) :

Groupe de travail de l'IETF (Internet Engineering Task Force) visant à faciliter la genèse d'IGC basées sur la norme X.509 pour des applications Internet. PKIX a produit des normes telles que les extensions de X.509 pour l'Internet, OCSP, etc.

Politique de Certification (PC) :

Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Porteurs et les Applications utilisatrices de certificats.

Politique de Gestion de Preuve (PGP) :

Ensemble de règles portant un nom (OID) qui indiquent l'applicabilité d'un ou plusieurs types de preuves à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes.

Porteur de certificat :

Un Porteur de certificats ne peut être qu'une personne physique.

Il s'agit de l'Utilisateur qui doit respecter les conditions qui lui incombent définies dans la présente PC.

Produit de sécurité :

Dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de Signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Promoteur d'application :

Fournisseur d'une offre de service sécurisé (échanges dématérialisés).

Responsable d'Autorité d'Enregistrement (RAE) :

Personne physique en charge de l'AE.

Service Almerys :

Un des services de la gamme d'offres de services de dématérialisation et de confiance d'Almerys, déployé en tout ou partie.

Signature électronique:

« Usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache », conformément au Code civil.

Transaction de signature :

Période de courte durée (une quinzaine de minutes) pendant laquelle un Utilisateur dûment identifié peut signer électroniquement les documents qui lui sont présentés par le Service de signature électronique.

Utilisateur :

Personne physique, utilisatrice d'un service mis à disposition par un Client et notamment du Certificat à usage unique.

L'identification et l'authentification de l'Utilisateur sont à la charge du Client (rôle d'AE).

Voir également Porteur de certificat.

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

2.1 ENTITES CHARGES DE LA MISE A DISPOSITION DES INFORMATIONS

Pour la mise à disposition des informations devant être publiées à destination des Porteurs et des Applications utilisatrices de certificats, l'AC « Almerys User Signing CA NA » met en œuvre une fonction de publication et une fonction d'information sur l'état des Certificats.

La mise à disposition des informations sur l'état des Certificats se base sur un mécanisme de LCR (Liste de Certificats Révoqués) accessible via plusieurs liens HTTP. Les adresses de publication sont fournies dans la section 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ».

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

L'AC « Almerys User Signing CA NA » diffuse les informations suivantes :

- la présente PC, qui contient en particulier les profils de certificat et de LCR, les délais et fréquences de publication, le glossaire qui contient les acronymes et les définitions applicables, les adresses principales de diffusion) ;
- les Certificats en cours de validité des AC de la hiérarchie de rattachement de l'AC User Signing, les différentes PC correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'ACR ;
- la liste des Certificats de signature des Porteurs et des AC révoqués ;
- les formulaires nécessaires pour la gestion des Certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.) ;
- les conditions générales d'utilisation des Certificats.

Ces informations sont disponibles sur le site web dédié à l'infrastructure de confiance: <http://pki.almerys.com/>

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Pour la PC, la publication est effective dès que nécessaire afin d'assurer, à tout moment, la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

Pour les certificats d'AC, ils sont diffusés préalablement à toute émission de Certificats et/ou de LCR correspondants sous un délai de 72 heures après la génération du certificat.

Pour les informations d'état des Certificats, les LCR sont mises à jour dans un délai maximum de 24 heures. Une fois la mise à jour effectuée, la LCR est publiée dans un délai maximum de 60 minutes.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées est du niveau de confidentialité « diffusion libre » pour les Applications utilisatrices de certificats.

La fonction de publication et la fonction d'information sur l'état des Certificats doivent assurer à tout moment l'intégrité des informations qu'elles publient.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'AC « Almerys User Signing CA NA », et aux personnes dûment autorisées.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1. Type de noms

Les noms utilisés dans les Certificats de signature émis par l'AC « Almerys User Signing CA NA » sont conformes aux spécifications de la norme X.500.

Dans chaque Certificat X.509v3, l'AC émettrice (issuer) et le Porteur (subject) sont identifiés par un « Distinguish Name » DN dont le format est précisé dans la section 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ».

3.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les Utilisateurs, Porteurs de certificats de signature, sont explicites :

- l'attribut CN du champ subject DN de l'Utilisateur est construit à partir des nom et prénom de l'Utilisateur et d'une référence unique propre à une Transaction de signature. Ces éléments sont présentés dans la demande de Certificat effectuée par le Client via le module ebeeSignClient ou le Service d'enregistrement en ligne ;
- les attributs O et OU du champ subject DN identifie le Client ainsi que le service pour lequel le Certificat sera utilisé.

Le format exact du subject DN des Certificats de signature est précisé dans la section 7 décrivant le profil des Certificats et des LCR.

3.1.3. Anonymisation ou pseudonymisation des Utilisateurs

Les Certificats des Utilisateurs ne peuvent pas être anonymes. L'utilisation d'un pseudonyme est interdite.

3.1.4. Règles d'interprétation des différentes formes de nom

Les règles d'interprétation des différentes formes de nom sont explicitées dans la section 7 décrivant le profil des Certificats et des LCR.

3.1.5. Unicité des noms

Afin d'assurer la continuité d'une identification unique de l'Utilisateur au sein du domaine de l'AC « Almerys User Signing CA NA » et pour éviter toute ambiguïté, le DN du champ « subject » de chaque Certificat d'Utilisateur permet d'identifier de façon unique l'Utilisateur correspondant au sein du domaine de l'AC grâce à la référence unique inscrite dans l'attribut CN du champ subject DN en plus des prénom et nom de l'Utilisateur. Cette référence est le numéro de Transaction de signature calculé par le Service de signature électronique, il est unique et aléatoire. A chaque Transaction de signature est associé un ensemble de données de l'Utilisateur permettant son identification.

Durant toute la durée de vie de l'AC, un DN attribué à un Porteur de certificats ne peut être attribué à un autre Porteur. Des précisions seront fournies, dans la DPC associée à cette PC, répondant à cette exigence en respectant les spécifications sur le DN définies dans les profils de Certificats (cf. section 7).

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

3.1.6. Identification, authentification et rôle des marques déposées

Les nom et prénom sont présentés par l'Utilisateur lors de son enregistrement auprès de l'AE (i.e. le Client). En cas de litige sur l'interprétation de ces paramètres, une résolution amiable des conflits est privilégiée.

De la même manière, les éventuelles étapes d'authentification permettant au Client de rapprocher des éléments d'authentification ou de surauthentification à des éléments d'identification sont à la charge du Client.

3.2 VALIDATION INITIALE DE L'IDENTITE

L'enregistrement d'un Utilisateur se fait directement auprès de l'AE.

Les modalités pratiques de validation de l'identité de l'Utilisateur sont déterminées par le Client. Les seuls éléments d'identité qui doivent être transmis à l'AC dans la requête de Certificat via le module ebeeSignClient ou le Service d'enregistrement en ligne sont les nom et prénom de l'Utilisateur.

3.2.1. Méthode pour prouver la possession de la clé privée

La clé privée de signature de l'Utilisateur est stockée de manière sécurisée par le Service de stockage sécurisé des Bi-clés des Utilisateurs d'Almerys (cf. §1.3.3 « Service de stockage sécurisé des Bi-clés des Utilisateurs »). Les modalités de vérification de la possession de la clé privée par l'Utilisateur dépendent des méthodes d'enregistrement et d'activation de la clé privée par l'Utilisateur. Ces modalités sont explicitées, pour chaque Client, dans les conditions particulières d'utilisation du Service de signature électronique acceptées par les parties. En effet, les moyens mis en œuvre pour effectuer cette vérification peuvent varier en fonction du contexte Client, et un choix est effectué parmi les modalités proposées par le Service de signature électronique d'Almerys.

3.2.2. Validation de l'identité d'un organisme

Sans objet dans le cadre de la présente PC.

3.2.3. Validation de l'identité d'un individu

La validation de l'identité d'un Utilisateur est à la charge du Client.

3.2.4. Informations non vérifiées de l'Utilisateur

Le choix de la vérification ou non des informations fournies par l'Utilisateur est à la discrétion du Client.

3.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée par le Client dans le cadre de ses processus métier.

3.2.6. Critères d'interopérabilité

Les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient est de la responsabilité de l'AG de l'ACR « Almerys Root CA ».

3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

Le contenu de cette section est sans objet pour les Certificats à usage unique car ces Certificats ne sont pas renouvelables étant donné leur objet.

3.3.1. Identification et validation pour un renouvellement courant

Sans objet dans le cadre de la présente PC.

3.3.2. Identification et validation pour un renouvellement des clés après révocation

Sans objet dans le cadre de la présente PC.

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

3.4.1. Demande faite via les moyens informatiques

3.4.1.1. Par le Porteur

Le Porteur peut demander la révocation de son Certificat lors de l'étape d'acceptation de son Certificat. Cette étape a lieu en ligne au cours de la Transaction de signature électronique : s'il ne valide pas les informations contenues dans son certificat (cf. §4.4.1 « Démarche d'acceptation du certificat »), cela implique la fin de la Transaction de signature et la révocation de son Certificat.

3.4.1.2. Par le responsable du service de signature électronique

Sans objet dans le cadre de la présente PC.

3.4.2. Demande faite via Service support

Sans objet dans le cadre de la présente PC.

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 ne peut être demandé que par un Client (AE) au nom d'un Utilisateur dans le cadre d'un service ou processus métier qu'il propose à ses Utilisateurs.

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

L'établissement de la demande de Certificat est effectué par le Client (AE) via le module client ebeeSignClient ou le Service d'enregistrement en ligne mis à sa disposition par Almerys, lequel transmet automatiquement la demande, si elle est correcte, à la fonction adéquate de l'IGC.

La connexion établie entre le système d'information du Client et celui d'Almerys est sécurisée grâce à un système d'authentification mutuelle, basée sur l'utilisation de Certificats électroniques, qui permet d'identifier les parties, de chiffrer le canal de communication, et de faire des vérifications d'intégrité des flux échangés.

Alternativement, le Client, ou l'un quelconque de ses représentants, peut, si cette option a été choisie, utiliser l'interface d'administration client de type web pour déposer une requête de Certificat et de signature pour un Utilisateur donné. Les conditions d'accès et d'authentification permettent de s'assurer de l'identité des acteurs accédant à ce service.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

La vérification de l'identité de l'Utilisateur est un pré-requis indispensable à toute demande de Certificat ; les modalités de cette vérification étant laissées à la discrétion du Client, en fonction de son contexte métier.

Une fois le processus d'identification validé, le Client peut procéder à une demande de Certificat et de Signature via le module ebeeSignClient ou le Service d'enregistrement en ligne qui comprend, au minimum les informations suivantes :

- les nom et prénom de l'Utilisateur,
- une référence unique et associée à la Transaction de signature,
- les données d'identification du Client
 - o complétées par la validation du profil de Certificat d'authentification du module de signature client mis à sa disposition pour se connecter à la plate-forme de signature électronique, et qui comprend lui-même des éléments d'identification du Client, ou par la validation de la requête reçue du portail de gestion du Service de signature électronique ;
 - o d'autre part, il est indispensable de fournir des données d'identification qui permettront de mettre en œuvre une identification à 2 facteurs
- les informations ou documents qui devront être signés par l'Utilisateur,

- des informations de contexte et de configuration propres à l'interface de programmation utilisée et aux options choisies par le Client.

4.2.2. Acceptation ou rejet de la demande

A réception du flux de demande de Certificat et de signature, l'AC « Almerys User Signing CA NA » :

- vérifie que le Client est enregistré et habilité à émettre des demandes,
- les éléments fournis sont complets et intègres, et en cas de succès, transmet la demande de Certificat proprement dite à la fonction de l'AC chargée de la génération des clés et des Certificats des Utilisateurs.

4.2.3. Durée d'établissement du certificat

La durée d'établissement des Certificats est maîtrisée, et compte tenu de la spécificité des processus synchrones de signature mis en œuvre par la plupart des Clients, l'AC vise une durée d'établissement la plus courte possible.

A titre d'information, l'AC fournit les temps moyens constatés d'établissement de Certificats.

4.3 DELIVRANCE DU CERTIFICAT

4.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE via le module ebeeSignClient ou le Service d'enregistrement en ligne, l'AC déclenche le processus de génération de la Bi-clé et du Certificat de signature de l'Utilisateur.

Le Certificat est à usage unique (durée de vie limitée à 1 jour). Le chapitre 7.17.2 « Profil du certificat User Signing » détaille le format utilisé par l'AC pour ce type de Certificats.

Le Bi-clé et le Certificat sont alors stockés par le Service de stockage sécurisé d'Almerys. La section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques » précise les caractéristiques des modules utilisés pour générer et stocker la Bi-clé de signature.

Suivant les options de signature retenues par le Client, le Certificat pourra être présenté ou non à l'Utilisateur lors de la présentation des informations ou des documents signés grâce à son Certificat.

4.3.2. Notification par l'AC de la délivrance du certificat

L'AC « Almerys User Signing CA NA » renvoie au Client un statut sur l'opération de certification. La DPC associée à la présente PC précise les différents codes qui sont retournés par l'application.

En cas de succès, le Certificat peut être remis au Client de manière indépendante, via le flux établi entre le Client et le service de signature, ou mis à disposition en tant qu'élément de preuve dans le dossier de preuve associé à la transaction de certification et de signature initiée par le Client et constitué par Almerys.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1. Démarche d'acceptation du certificat

L'acceptation du Certificat par l'Utilisateur est explicite : les informations du Certificat lui sont présentées en ligne après consultation des documents ou informations à signer et acceptation des Conditions générales d'utilisation du Service :

- En cas d'acceptation, le Certificat et le Bi-clé de signature de l'Utilisateur sont utilisés pour signer les documents ou informations présentés par le Client ;
- En cas de refus, la Transaction de signature est annulée et le Certificat de l'Utilisateur est révoqué.

Les informations minimales du Certificat présentées à l'Utilisateur sont les données à caractère personnel contenues dans le certificat, i.e. ses prénom et nom contenus dans le champ CN, ainsi que les dates de début et de fin de validité du certificat.

4.4.2. Publication du certificat

Les Certificats de signature ne sont pas publiés.

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

L'AC « Almerys User Signing CA NA » informe l'AE de la délivrance du Certificat. Cf. section 4.3.2 « Notification par l'AC de la délivrance du certificat ».

4.5 USAGES DE LA BI-CLE ET DU CERTIFICAT

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

L'utilisation de la clé privée de l'Utilisateur et du Certificat associé est strictement limitée au Service de signature (cf. section 1.4 « Usage des certificats »).

L'usage autorisé de la Bi-clé de l'Utilisateur et du Certificat associé est précisé dans le Certificat lui-même, via les extensions concernant les usages des clés (cf. section 7.2 «

Profil du certificat User Signing »)

Les Utilisateurs doivent respecter strictement les usages autorisés des Bi-clés et des Certificats. Dans le cas contraire, leur responsabilité serait engagée.

D'une manière générale, tout usage non autorisé explicitement est interdit.

4.5.2. Utilisation de la clé publique et du certificat par l'Application utilisatrice du certificat

Cf. chapitre précédent et sections 1.4 « Usage des certificats » et 1.3.7 « Applications utilisatrices des certificats »

Les Applications utilisatrices de certificats doivent respecter strictement les usages autorisés des Certificats. Dans le cas contraire, leur responsabilité peut être engagée.

4.6 RENOUELEMENT D'UN CERTIFICAT

Le renouvellement d'un Certificat – i.e. la délivrance d'un nouveau Certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations restant identiques au Certificat précédent (y compris la clé publique du Porteur), cf. [RFC3647] – n'est pas autorisé dans le cadre de la présente PC.

4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

Le contenu de cette section est sans objet pour les Certificats à usage unique car ces Certificats ne sont pas renouvelables étant donné leur objet.

4.7.1. Causes possibles de changement d'une bi-clé

Sans objet pour la présente PC.

4.7.2. Origine d'une demande d'un nouveau certificat

Sans objet pour la présente PC.

4.7.3. Procédure de traitement d'une demande d'un nouveau certificat

Sans objet pour la présente PC.

4.7.4. Notification de l'établissement du nouveau certificat

Sans objet pour la présente PC.

4.7.5. Démarche d'acceptation du nouveau certificat

Sans objet pour la présente PC.

4.7.6. Publication du nouveau certificat

Sans objet pour la présente PC.

4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet pour la présente PC.

4.8 MODIFICATION DU CERTIFICAT

La modification d'un Certificat – i.e. des modifications d'informations du Certificat sans changement de la clé publique, et autres qu'uniquement la modification des dates de validité, cf. [RFC3647] – n'est pas autorisée dans le cadre de la présente PC.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats de Porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du Certificat de signature du Porteur :

- les informations du Porteur figurant dans son certificat ne sont pas en conformité avec son identité,
- le Certificat de signature de l'AC « Almerys User Signing CA NA » est révoqué (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante).

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC « Almerys User Signing CA NA » en a connaissance, les Certificats concernés sont révoqués.

4.9.1.2. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un Certificat d'une composante de l'IGC (y compris un certificat de l'AC « Almerys User Signing CA NA » pour la génération de Certificats, de LCR et/ou de réponses OCSP) :

- 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 ;
- révocation du certificat de l'ACR.

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats de Porteurs

Les personnes / entités qui peuvent demander la révocation d'un Certificat Porteur sont les suivantes :

- le Porteur, s'il constate que les données de son Certificat ne sont pas conformes à son identité,
- l'AC « Almerys User Signing CA NA », émettrice du Certificat.

4.9.2.2. Certificat d'une composante de l'IGC

La révocation d'un Certificat d'AC ne peut être décidée que par l'AG de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres Certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat de Porteur

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre 3.4 « Identification et validation d'une demande de révocation ».

A l'initiative du Porteur (cf. §4.9.2 « Origine d'une demande de révocation »), le Service de Signature électronique transmet la demande de révocation à la fonction de gestion des révocations de l'AC User Signing. La demande de révocation de Certificat comprend au minimum :

- l'identification du Certificat concerné via au minimum :
 - o son numéro de série,
 - o l'identification de l'émetteur (champ DN de l'émetteur du certificat),
 - o la raison de révocation.

Une fois la demande contrôlée, la fonction de gestion des révocations de l'AC « Almerys User Signing CA NA » révoque le Certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via le mécanisme de Liste de Certificats Révoqués (LCR) mis en œuvre par l'AC « Almerys User Signing CA NA ».

Le processus de révocation d'un Certificat de signature Porteur est décrit dans la DPC.

Le Porteur, demandeur de la révocation, est informé en ligne du bon déroulement de l'opération et de la révocation effective du Certificat. Cette révocation met fin à la Transaction de signature, et il est redirigé vers la page d'accueil du Service de signature en ligne.

L'opération est enregistrée dans les journaux d'événements.
Les causes de révocation des Certificats ne sont pas publiées.

4.9.3.2. Révocation d'un certificat d'une composante de l'IGC

La DPC de l'AC « Almerys User Signing CA NA » 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 doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des Porteurs concernés que leur Certificat n'est plus valide.

4.9.4. Délai accordé pour formuler la demande de révocation

Dès qu'une entité autorisée (cf 4.9.2 « Origine d'une demande de révocation ») a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

4.9.5.1. Révocation d'un certificat de Porteur

Dans le cas du Service de signature électronique, la demande de révocation émise par le Porteur est traitée immédiatement dans un flux de communication synchrone entre le Service de signature et la fonction de révocation de l'AC « Almerys User Signing CA NA ».

La demande de révocation est donc traitée en quelques secondes. La fonction de révocation doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme aux engagements contractuels établis entre Almerys et le Client.

4.9.5.2. Révocation d'un certificat d'une composante de l'IGC

La révocation d'un Certificat d'une composante de l'IGC doit être effectuée dès la détection d'un événement 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, et que cette liste est accessible au téléchargement. La révocation d'un Certificat de signature de l'AC (signature de certificats, de LCR / LAR et/ou de réponses OCSP) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.6. Exigences de vérification de la révocation par les Applications utilisatrices de certificats

L'application utilisatrice d'un Certificat de Porteur est tenue de vérifier, avant son utilisation, l'état des Certificats de l'ensemble de la chaîne de certification correspondante, y compris le Certificat du Porteur lui-même.

4.9.7. Fréquence d'établissement des LCR

La fréquence d'établissement des LCR est au maximum de 24 heures (durée maximale pendant laquelle aucune révocation naturelle n'a eu lieu). La durée de validité est de 72 heures.

4.9.8. Délai maximum de publication d'une LCR

Suite à sa génération, une LCR doit être publiée dans le délai maximum de 60 minutes.

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

Aucun service OSCP n'est adjoint au mécanisme de LCR.

4.9.10. Exigences de vérification en ligne de la révocation des certificats par les applications utilisatrices de certificats

Cf. section 4.9.6 « Exigences de vérification de la révocation par les Applications utilisatrices de certificats » ci-dessus.

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 d'AC, outre les exigences du chapitre 4.9.3.2, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC.

4.9.13. Causes possibles d'une suspension

Sans objet pour la présente PC.

4.9.14. Origine d'une demande de suspension

Sans objet pour la présente PC.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet pour la présente PC.

4.9.16. Limites de la période de suspension d'un certificat

Sans objet pour la présente PC.

4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.10.1. Caractéristiques opérationnelles

L'AC fournit aux Applications utilisatrices de certificats de signature les moyens de vérifier et valider préalablement à son utilisation, le statut d'un Certificat et de sa chaîne de certification, c'est-à-dire de vérifier également les signatures des Certificats de la chaîne et les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état des Certificats de l'ACR.

La fonction d'information sur l'état des Certificats met à la disposition des Applications utilisatrices de certificats un mécanisme de consultation libre de LCR/LAR. Ces LCR/LAR sont des LCR/LAR respectant le format X.509v2 [RFC3280], publiées en mode HTTP directement accessibles via l'Internet.

Le chapitre 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR » fournit les informations de format sur les LCR, ainsi que les URL de publication des LCR/LAR.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des Certificats est disponible 24h/24 7j/7.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme aux engagements contractuels établis entre Almerys et le Client.

4.10.3. Dispositifs optionnels

Sans objet pour la présente PC.

4.11 FIN DE LA RELATION ENTRE LE PORTEUR ET L'AC

Compte tenu de la durée de vie des certificats, cette section est sans objet dans le cadre présente PC.

4.12 SEQUESTRE DE CLÉ ET RECOUVREMENT

Le séquestre de clé et le recouvrement sont interdits dans le cadre de la présente PC.

4.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet pour la présente PC.

4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet pour la présente PC.

5. MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

Le Responsable de l'AC « Almerys User Signing CA NA » s'engage à mettre en œuvre et maintenir le niveau de sécurité physique exigé pour les locaux d'exploitation des composantes de l'IGC.

5.1.1. Situation géographique et construction des sites

En fonction de la sensibilité des composants de l'IGC interne d'Almerys, les sites sont définis au niveau 1 de la politique de sécurité Almerys : impact vital (majeur pour l'entreprise).

A ce titre, la mise en sécurité du site du bâtiment respecte les mesures de sécurité physique de niveau 1 pour la protection périphérique, périmétrique et intérieure et notamment les mesures relatives à :

- l'alimentation électrique et climatisation ;
- la vulnérabilité aux dégâts des eaux ;
- la prévention et protection incendie.

Les mesures permettent également de respecter les engagements pris dans la PC ou dans les engagements contractuels avec les Clients du service de signature électronique, en matière de disponibilité des services.

5.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'AC « Almerys User Signing CA NA », les accès aux locaux sont contrôlés conformément au niveau de zonage des locaux de niveau 1 : « accès très restreint ».

Pour les fonctions de génération des Certificats, de génération des éléments secrets de l'Utilisateur, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. De plus, le contrôle en entrée et en sortie est permanent en heures non ouvrées (HNO).

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC définissent un périmètre de sécurité physique où sont installées ces machines. Tout local utilisé en commun entre la composante concernée et une autre composante (de ou hors de l'IGC) est en dehors de ce périmètre de sécurité.

L'ouverture de la porte est commandée par un système de contrôle d'accès.

5.1.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'AC « Almerys User Signing CA NA » telles que fixées par leurs fournisseurs.

Elles respectent également les exigences du cahier des charges fourni par le prestataire des services, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des Certificats.

5.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection mis en place par l'AC Almerys User Signing CA NA permettent de protéger son infrastructure contre les dégâts des eaux.

5.1.5. Prévention et protection incendie

l'AC Almerys User Signing CA NA met en places des moyens de protection et de lutte contre les incendies..

5.1.6. Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) utilisés au sein de l'AC « Almerys User Signing CA NA » sont traités et conservés conformément aux besoins de sécurité définis pour les actifs sensibles (en confidentialité, intégrité et disponibilité).

5.1.7. Mise hors service des supports

En fin de vie, les supports seront, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation sont conformes à la Politique de Sécurité d'Almerys.

5.1.8. Sauvegardes hors site

En complément de sauvegardes sur sites, les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des services après incident la plus rapide possible.

5.2 MESURES DE SECURITE PROCEDURALES

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé de l'AC « Almerys User Signing CA NA ».

5.2.1. Rôles de confiance

Les rôles de confiance définis ci-dessous sont ceux requis pour les composantes de l'IGC, indépendamment des rôles de confiance définis dans le cadre de la cérémonie des clés.

- Officier de Sécurité de l'IGC (PKI Security Officer) – L'Officier de Sécurité est chargé de la mise en œuvre de la politique de sécurité de l'AC « Almerys User Signing CA NA ». Il gère les contrôles d'accès physiques aux équipements des systèmes de l'entité. Il est habilité à prendre connaissance des documents conservés au niveau de l'OC, et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- Responsable d'application – Le responsable d'application est chargé, au sein de la composante de l'IGC concernée, de la mise en œuvre des différentes PC et DPC de l'AC « Almerys User Signing CA NA ». Sa responsabilité couvre l'ensemble des fonctions rendues par les applications et des performances correspondantes.
- Ingénieur système – Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'entité. Il assure l'administration technique des systèmes et des réseaux de l'entité.
- Opérateur – Un opérateur au sein de la composante de l'IGC concernée réalise, dans le cadre de ses attributions, l'exploitation des applications pour les services délivrés par la composante de l'IGC.

- Auditeur – Personne désignée par le responsable de la composante de l'IGC et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des services fournis par la composante de l'IGC par rapport aux PC, aux DPC de l'AC « Almerys User Signing CA NA ».

5.2.2. Nombre de personnes requises par tâches

La DPC de l'AC « Almerys User Signing CA NA » précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.), en particulier, les personnes requises pour la cérémonie des clés.

5.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC fait vérifier l'identité et les autorisations de tout membre de son personnel 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 les systèmes concernés par le rôle,
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes,
- qu'un compte soit ouvert à son nom dans ces systèmes,
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.
- Ces contrôles sont décrits dans la DPC de l'AC « Almerys User Signing CA NA » et sont conformes à la Politique de Sécurité d'Almerys.

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 services offerts.

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC « Almerys User Signing CA NA » et sont conformes à la Politique de Sécurité d'Almerys.

Pour les différents rôles de confiance, il est recommandé qu'une même personne ne détienne pas plusieurs rôles et les cumuls suivants sont interdits :

- officier de sécurité et ingénieur système / opérateur,
- ingénieur système et opérateur.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé de l'AC « Almerys User Signing CA NA ».

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité.

Le responsable de l'AC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de l'IGC, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC « Almerys User Signing CA NA » doit informer toute personne intervenant dans des rôles de confiance de l'IGC :

- de ses responsabilités relatives aux services de l'IGC,
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

Les qualifications, compétences et habilitations requises pour la cérémonie des clés sont définies dans une procédure spécifique.

5.3.2. Procédures de vérification des antécédents

Les personnels amenés à travailler au sein d'une composante de l'IGC, et en fonction du contexte applicable, sont amenés à remettre une attestation sur l'honneur de non-condamnation, un extrait de casier judiciaire, ou un engagement de confidentialité.

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

5.3.3. Exigences en matière de formation initiale

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

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4. Exigences et fréquence en matière de formation continue

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

5.3.5. Fréquence et séquence de rotation entre différentes attributions

La présente PC ne prévoit pas d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la DPC de l'AC « Almerys User Signing CA NA ».

5.3.6. Sanctions en cas d'actions non autorisées

La présente PC ne prévoit d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la DPC de l'AC « Almerys User Signing CA NA ».

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

Le personnel des prestataires externes intervenant dans les locaux d'Almerys et/ou sur les composantes de l'IGC respecte également les exigences du présent chapitre 5.3.

Ceci doit être traduit en clauses adéquates dans les contrats concernés avec les prestataires.

5.3.8. Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille, plus spécifiquement de la Politique de Sécurité l'impactant.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'événements consiste à enregistrer des événements sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

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

5.4.1. Type d'événements à enregistrer

Chaque entité opérant une composante de l'IGC journalise au minimum les événements suivants, automatiquement dès le démarrage d'un système et sous forme électronique :

- création / modification / suppression des données d'authentification correspondantes (mots de passe, certificats, etc.),
- démarrage et arrêt des systèmes informatiques et des applications,
- événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation,
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres événements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques,
- les actions de maintenance et de changements de la configuration des systèmes,
- les changements apportés au personnel,
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs...).

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

- réception d'une demande de Certificat,
- validation / rejet d'une demande de Certificat,
- événements liés aux clés de signature et aux Certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...),
- publication et mise à jour des informations liées à l'AC (PC, Certificats d'AC, conditions générales d'utilisation, etc.),
- génération des Certificats des Porteurs,
- transmission des Certificats aux Porteurs et aux Clients,
- génération puis publication des LCR.

Chaque enregistrement d'un événement dans un journal contient lorsque cela est applicable les champs suivants :

- type de l'événement,
- nom de l'exécutant ou référence du système déclenchant l'événement,
- date et heure de l'événement,
- résultat de l'événement (échec ou réussite).

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

De plus, en fonction du type de l'événement, chaque enregistrement contient également contenir les champs suivants :

- dans la mesure du possible : demandeur et destinataire de l'opération,
- 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'événement,
- toute information caractérisant l'événement (par exemple, pour la génération d'un Certificat, le numéro de série de ce Certificat).

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement.

5.4.2. Fréquence de traitement des journaux d'événements

Cf. chapitre 5.4.8 ci-dessous.

5.4.3. Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins un mois.

5.4.4. Protection des journaux d'événements

L'AC met en œuvre une protection des journaux d'événements adaptée au niveau de sensibilité des informations contenues dans ces journaux. Ce niveau de sensibilité est issu d'une analyse de risque.

5.4.5. Procédure de sauvegarde des journaux d'événements

L'AC met en œuvre un processus de sauvegarde des journaux d'événements adapté au niveau de sensibilité des informations contenues dans ces journaux. Ce niveau de sensibilité est issu d'une analyse de risque.

5.4.6. Système de collecte des journaux d'événements

L'AC met en œuvre un système de journalisation des événements qui intègre une datation conforme aux exigences du paragraphe 6.8.

5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

La présente PC ne prévoit pas d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la DPC de l'AC « Almerys User Signing CA NA ».

5.4.8. Evaluation des vulnérabilités

L'AC met en œuvre une gestion des vulnérabilités de systèmes de l'AC « Almerys User Signing CA NA » en conformité avec la Politique de Sécurité d'Almerys.

Les journaux d'événements sont contrôlés régulièrement selon des modalités définies dans la DPC, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins à une fréquence mensuelle et dès la détection d'une anomalie. 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.

5.5 ARCHIVAGE DES DONNEES

5.5.1. Types de données à archiver

Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les agréments contractuels avec d'autres AC ;
- les LCR tels qu'émisses ou publiées ;
- les récépissés ou notifications (à titre informatif).

5.5.2. Période de conservation des archives

En l'état de la législation et de la réglementation en vigueur (dite « Informatique et Libertés »), toute information de type :

- personnel,
- trafic,
- connexion,
- facturation,

et issue d'un processus automatique de traitement de données, n'est pas archivée pendant plus d'un an.

Les durées d'archivage sont les suivantes :

- PC : durée de vie de l'AC,
- documents organisationnels de cérémonies des clés : durée de vie de l'AC,
- DPC : durée de vie de l'AC,
- dossiers de demande de certificat : au moins 5 ans,
- certificats émis par l'AC après expiration : au moins 5 ans,
- dernière LCR émis par l'AC après expiration : au moins 5 ans,
- journaux d'événements après leur génération : au moins 5 ans.

5.5.3. Protection des archives

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

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

5.5.4. Procédure de sauvegarde des archives

La procédure est précisée dans la DPC.

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

5.5.5. Exigences d'horodatage des données

Les certificats sont datés au moment de leur génération et cette information est archivée avec le certificat correspondant.

Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6. Système de collecte des archives

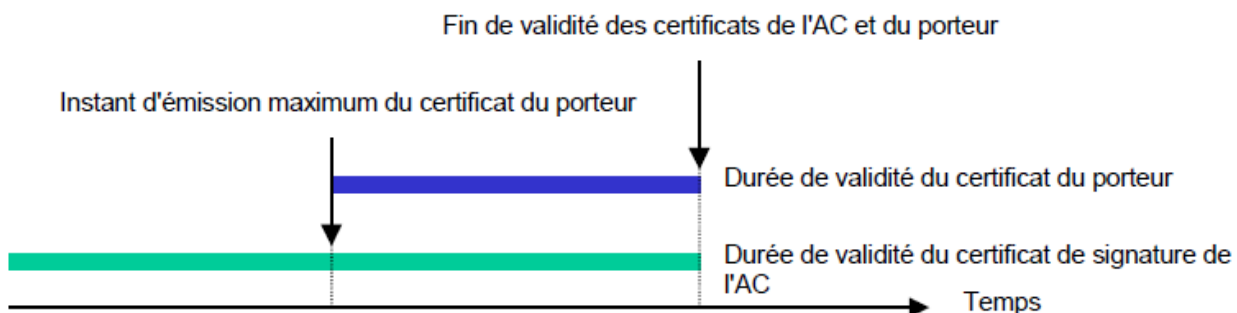
La DPC précise les moyens mis en œuvre pour collecter les archives en toute sécurité.

5.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérables dans un délai inférieur à 2 jours ouvrés, étant noté que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de Certificat dont la date de fin serait postérieure à la date d'expiration du Certificat correspondant de l'AC. Pour cela, la période de validité de ce Certificat de l'AC doit être supérieure à celle des Certificats qu'elle signe.



Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle Bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des Certificats.

Le Certificat précédent reste utilisable pour valider les Certificats émis sous cette clé et ce, au moins jusqu'à ce que tous les Certificats signés avec la clé privée correspondante aient expiré.

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

Chaque composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents conformément aux exigences de la Politique de Sécurité d'Almerys.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC « Almerys User Signing CA NA », l'événement déclencheur est la constatation de cet incident. L'AG de l'IGC Almerys est immédiatement informée. Le cas de l'incident majeur doit être impérativement traité dès la détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible.

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

Conformément à la Politique de Sécurité d'Almerys, l'AC « Almerys User Signing CA NA » dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité de ses différentes fonctions, et découlant :

- de la présente PC,
- des engagements en termes de qualité de service des différentes composantes de l'IGC,

notamment pour ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des Certificats. Ce plan est testé au minimum une fois tous les 3 ans.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante de l'IGC Almerys est traité conformément au chapitre 5.7.2 « Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) ».

5.7.4. Capacités de continuité d'activités suite à un sinistre

Les différentes composantes de l'IGC Almerys disposent des moyens raisonnablement nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. section 5.7.2 « Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) »).

5.8 FIN DE VIE DE L'IGC

Une ou plusieurs composantes de l'IGC Almerys peut être amenée à cesser son activité en tout ou partie, ou à la transférer à une autre entité.

La compromission de la Bi-clé de l'AC « Almerys User Signing CA NA » entraîne immédiatement sa cessation d'activité et la révocation de tous les Certificats émis en cours de validité. Pour retrouver le niveau de service, la création d'une nouvelle AC et de nouveaux Certificats sont obligatoires.

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

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC « Almerys User Signing CA NA » s'engage, entre autres obligations :

- 1) à mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des Certificats des Utilisateurs et des informations relatives aux Certificats) ;
- 2) à assurer 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 présente PC.

L'AC « Almerys User Signing CA NA » s'engage à respecter les points suivants :

- 1) dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des Porteurs ou des Applications utilisatrices de certificats, l'AC « Almerys User Signing CA NA » doit les en aviser aussitôt que nécessaire et, au moins, sous le délai d'un mois.
- 2) L'AC « Almerys User Signing CA NA » doit communiquer aux Clients les principes du plan d'action mettant en œuvre 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 « Almerys User Signing CA NA » devra communiquer aux Clients les modalités des changements survenus. L'AC « Almerys User Signing CA NA » mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les Porteurs et les Applications utilisatrices de certificats.
- 3) L'AC « Almerys User Signing CA NA » doit tenir informés les Porteurs de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

Cessation d'activité affectant l'AC « Almerys User Signing CA NA »

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 doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC « Almerys User Signing CA NA », ou une entité tierce qui reprend les activités, lors de l'expiration du dernier Certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC « Almerys User Signing CA NA » 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, assure la révocation des Certificats et la publication des LCR conformément aux engagements pris dans sa PC.

Lors de l'arrêt du service, l'AC « Almerys User Signing CA NA » :

- 1) détruit la clé privée lui ayant permis d'émettre des Certificats ;
- 2) prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- 3) révoque son Certificat ;
- 4) révoque tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;

- 5) informe (par exemple par récépissé) tous les Porteurs des certificats révoqués ou à révoquer, et/ou le Client des services de signature électronique qui a demandé l'émission de ces Certificats en leur nom.

6. MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI-CLES

6.1.1. Génération des bi-clés

6.1.1.1. Clés d'AC

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

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique certifié Fips 140-2 Niveau 3(cf. également la section 6.2.1« Standards et mesures de sécurité pour les modules cryptographiques »).

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre d'une « Cérémonies des Clés » (ou encore Key Ceremony – KC). Cette cérémonie se déroule suivant des scripts, organisationnels et techniques, préalablement définis.

La génération des clés d'AC s'accompagne de la génération de différents secrets et éléments sensibles. Ces secrets sont des données permettant de gérer de manière sécurisée (personne ne peut posséder l'intégralité du secret), et ultérieurement à la Cérémonie des Clés, les opérations sur le HSM cryptographique, notamment, de pouvoir redémarrer, sauvegarder, et restaurer la sauvegarde de la partition HSM.

Suite à leur génération, les secrets sont remis à des Détenteurs de secrets désignés au préalable et habilités à ce rôle de confiance.

Le renouvellement du Certificat et des clés de l'AC suit les mêmes principes que ceux de la première génération des clés d'AC.

6.1.1.2. Clés porteurs générées par l'AC

La réception de la requête de Certificat et de signature de la part d'un Client au nom d'un Utilisateur déclenche le processus de création du Bi-clé.

Le Service de stockage sécurisé de Bi-clé de l'AC « Almerys User Signing CA NA » est en charge de la génération des Bi-clés de signature des Porteurs.

La génération et le stockage de la Bi-clé de signature se fait au sein d'un module cryptographique matériel certifié FIPS 140-2 niveau 3. Ce module est hébergé dans les locaux à accès très restreint Almerys.

Les clés à usage unique sont détruites dans un laps de temps très court, une fois que la Transaction de signature est achevée.

6.1.1.3. Clés porteurs générées par le porteur

Les Utilisateurs, Porteurs des Bi-clés de signature, ne génèrent pas leurs Bi-clés.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée de signature n'est pas transmise à son propriétaire, elle est stockée par le Service de signature électronique Almerys.

6.1.3. Transmission de la clé publique à l'AC

La clé publique est transmise à l'AC « Almerys User Signing CA NA » dans la demande de génération de Certificat. La clé est protégée en intégrité et l'origine est authentifiée grâce à l'utilisation d'une enveloppe au format PKCS#10 qui est signée par la clé privée associée à la clé publique.

6.1.4. Transmission de la clé publique de l'AC aux applications utilisatrices de certificats

Plus d'informations sur le sujet sont fournies dans la PC de l'ACR d'Almerys.

6.1.5. Tailles des clés

Les tailles de clés sont les suivantes :

- Certificat de l'AC « Almerys User Signing CA NA » : 4096 bits (algorithme RSA)
- Certificats des Utilisateurs: 2048 bits (algorithme RSA)

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

L'équipement de génération de Bi-clé utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant au Bi-clé. Ces paramètres sont rappelés dans le chapitre 7 « PROFILS DES CERTIFICATS, OCSP ET DES LCR ». De plus, cet équipement est configuré pour respecter au minimum une configuration FIPS 140-2 niveau 2 qui interdit les algorithmes et paramètres considérés comme faibles, ainsi que l'exportation en clair de la clé privée de Signature du Porteur.

6.1.7. Objectifs d'usage de la clé

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

L'usage de la clé privée de l'Utilisateur et du Certificat associé est strictement limité au Service de signature Almerys (cf. sections 1.4 « Usage des certificats » et 7.2 «

Profil du certificat User Signing » pour les restrictions dans le format de Certificat User Signing).

6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature sont certifiés Fips 140-2 niveau 3.

6.2.1.2. Dispositifs de création de signature des porteurs

Le dispositif de création de signature des Porteurs est un Module cryptographique matériel certifié FIPS 140-2 niveau 3.

Sa configuration opérationnelle minimale est conforme au standard FIPS 140-2 niveau 2.

Le Service de stockage sécurisé des Bi-clés de l'AC est chargé du maintien opérationnel et de la sécurité de ces Modules.

6.2.2. Contrôle de la clé privée de l'AC par plusieurs personnes

Le contrôle de la clé privée de l'AC est assuré pour les actions suivantes :

- pour l'exportation / l'importation hors / dans un module cryptographique : les systèmes sont configurés pour interdire l'exportation en clair de la clé privée, assurant ainsi sa non compromission ;
- pour la génération du Bi-clé (cf. 6.1.1.1) : utilisation d'un module cryptographique matériel sécurisé pour la génération et le stockage de la clé privée, et le partage des secrets assure qu'aucun acteur ne puisse accéder ou interpréter un des secrets ;
- pour l'activation de la clé privée (cf. section 6.2.8) : les flux de requêtes de Certificats et de révocation (mise à jour de la LCR) sont maîtrisés pour s'assurer que seuls les services autorisés puissent être enregistrés ; l'action d'autorisation et de configuration de ces flux nécessite la présence d'au minimum 2 acteurs ayant des fonctions différentes ;
- pour la destruction (cf. section 6.2.10) : les procédures de destruction permettent de s'assurer que personne ne pourra utiliser la clé privée.

6.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des Utilisateurs ne sont séquestrées.

6.2.4. Copie de secours de la clé privée

Les clés privées des Porteurs ne doivent faire l'objet d'aucune copie de secours par l'AC.

La clé privée d'AC fait l'objet de copies de secours hors des modules cryptographiques sous forme chiffrée et répartie (principe du partage de secrets) et avec un mécanisme de contrôle d'intégrité.

6.2.5. Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivées.

Les clés privées des Porteurs ne sont pas archivées, ni par l'AC, ni par aucune des composantes de l'IGC.

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

Pour les clés privées d'AC, tout transfert se fait sous forme chiffrée, conformément aux indications de la section 6.2.4.

Les clés privées de signature d'Utilisateur générés par un module cryptographique matériel ne sont jamais exportées.

6.2.7. Stockage de la clé privée dans un module cryptographique

cf. section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques ».

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clé privée d'AC

cf. 6.2.2 « Contrôle de la clé privée de l'AC par plusieurs personnes »

6.2.8.2. Clés privées des porteurs

L'activation de la clé privée de l'Utilisateur est contrôlée via des données ou des actions d'activation (cf. section 6.4 « Données d'activation ») propres à l'Utilisateur.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clé privée d'AC

La désactivation de la clé privée d'AC dans les modules cryptographiques est automatique dès que l'environnement du module évolue de manière sensible : choc, déconnexion, etc.

Les modalités de désactivation sont propres à la technologie du module ; elles sont détaillées dans la documentation constructeur.

6.2.9.2. Clés privées des porteurs

L'Utilisateur ne pourra pas activer la clé privée s'il n'est pas capable de fournir les informations ou de mener à bien les actions qui autorisent l'activation.

La désactivation de la clé a lieu à l'issue de la Transaction de signature par le biais de la destruction du Bi-clé de signature qui est stockée dans le Module cryptographique matériel. Cette destruction a lieu quel que soit l'état final de la transaction.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Clés privées d'AC

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

6.2.10.2. Clés privées des porteurs

La clé privée de signature d'un Utilisateur est détruite au sein du Module cryptographique qui est en charge de la stocker pour la durée de la Transaction de signature pour laquelle l'Utilisateur a accepté la création d'un Certificat de signature. Cette destruction a lieu à l'issue de la transaction, quel que soit l'état final de la transaction.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

cf. section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques ».

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des Utilisateurs sont archivées dans le cadre de l'archivage des Certificats correspondants.

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

Les Certificats des Utilisateurs couverts par la présente PC ont une durée de vie de 24 heures. Les Bi-clés associés ont une durée de vie effective de quelques minutes au maximum, durée qui correspond à la durée de vie des Transactions de signature électronique.

6.4 DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

6.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se fait lors de la phase d'initialisation et de personnalisation de ce module.

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du porteur

L'activation de la clé privée de l'Utilisateur est contrôlée via des données ou des actions d'activation propres à l'Utilisateur.

Un Porteur peut obtenir un Certificat de signature User Signing et activer sa clé privée de signature dans le cadre du processus de souscription en ligne mis en œuvre par le Client sous réserve du respect de 2 conditions préalables :

1. La validation de la session (ou Transaction) de signature, établie à l'issue d'une phase d'identification à 2 facteurs. Cette identification se base par défaut sur :
 - o La fourniture par mail d'une URL personnalisée de signature au Porteur ;

- L'envoi d'un code à usage unique (OTP) par SMS sur le numéro de téléphone portable du Porteur.

Note : il est obligatoire de mettre en œuvre 2 facteurs d'identification offrant un niveau de sécurité au moins équivalent à celui du processus décrit ci-dessus, mais les modalités d'implémentation peuvent être différentes en fonction du contexte Client.

2. L'action de cliquer sur le bouton « Je signe » lors de la présentation des documents à valider :
 - Permet de générer le Bi-clé de signature du Porteur uniquement pour cette Transaction de signature. Ce Bi-clé est protégé matériellement dans le Module cryptographique matériel conforme au minimum au standard FIPS 140-2 level 2.

Les données d'identification (par défaut, l'adresse mail et le numéro de téléphone du Porteur) sont transmis au service de signature par le Client qui les a collectés lors de la phase d'enregistrement du Porteur.

L'authentification réussie de la session permet l'activation de la clé privée pour l'action de Signature.

Les méthodes d'enregistrement et d'activation de la clé privée par l'Utilisateur sont explicitées, pour chaque Client, dans les conditions particulières d'utilisation du Service de signature électronique.

6.4.2. Protection des données d'activation

6.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

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

6.4.2.2. Protection des données d'activation correspondant aux clés privées des porteurs

Les modalités de protection des données d'activation des clés privées des porteurs dépendent de la méthode choisie. Le détail de ces modalités est fourni dans les conditions particulières d'utilisation du service de signature électronique. Dans tous les cas, une identification à 2 facteurs est requise pour activer le processus de génération du Bi-clé et du Certificat de Signature.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC de l'AC « Almerys User Signing CA NA ». Il répond en particulier aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, 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) ;
- éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle doit être cohérente avec la Politique de Sécurité d'Almerys.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramètres du système sont mis en place.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.6.1. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre une fonction de l'IGC Almerys est documentée.

La configuration du système des composantes de l'IGC Almerys ainsi que toute modification et mise à niveau sont documentées.

Tout développement doit être cohérent avec la Politique de Sécurité d'Almerys et avec les exigences contenues dans la présente PC ainsi que dans la PC de l'ACR.

6.6.2. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC Almerys doit être signalée à l'AG pour validation. Elle doit être documentée.

6.7 MESURES DE SECURITE RESEAU

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'IGC Almerys font l'objet de la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés notamment).

6.8 HORODATAGE / SYSTEME DE DATATION

Les systèmes de datation sont synchronisés par rapport à une source fiable du temps universel (UTC) et un système de synchronisation temporelle (NTP) avec une précision au moins égale à une minute.

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 PROFIL DU CERTIFICAT DE L'AC « ALMERYS USER SIGNING CA NA »

Le tableau suivant fournit les valeurs des attributs du Certificat de l'AC « Almerys User Signing CA NA » émis par l'AC racine « Almerys Root CA ».

Le format de ce Certificat ainsi que ses attributs respectent le profil X.509v3 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		3
signature		
▶ algorithm		Sha2withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ALMERYS ROOT CA OU = 0002 432701639 O = ALMERYS C = FR
validity		
▶ notBefore		Date de création (référentiel temporel de l'AC)
▶ notAfter		notBefore + 10ans
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ALMERYS USER SIGNING CA NA OU = ADVANCED SERVICES OU = 0002 432701639 O = ALMERYS C = FR
subjectPublicKeyInfo		
▶ algorithm		
↳ algorithm		rsaEncryption (OID = 1.2.840.113549.1.1.1)
↳ parameters		RSAParams : NULL
▶ subjectPublicKey		DER encoded RSAPublicKey (4096 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶ authorityKeyIdentifier	Non	160 bits du haché SHA-1 de la clé publique de l'issuer
▶ subjectKeyIdentifier	Non	160 bits du haché SHA-1 de la clé publique de l'issuer
▶ keyUsage	Oui	keyCertSign (5), cRLSign (6)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies		Stratégie du certificat :

		Identificateur de stratégie = 1.2.250.1.16.12.5.41.1.4.2.1
▶ basicConstraints ↳ cA ↳ pathLenConstraint	Non	false None
▶ cRLDistributionPoints	Non	[1]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almerysrootca.cr
Private extensions		
▶ authorityInfoAccess		[1] : accessMethod : id-ad-calssuers accessLocation : URL=http://pki.almerys.com/almerysrootca.cer
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha2withRSAEncryption, clé de 4096 bits
parameters		NULL

7.2 PROFIL DU CERTIFICAT USER SIGNING

Le tableau suivant fournit les valeurs par défaut des attributs d'un Certificat User Signing émis par l'AC « Almerys User Signing CA NA ».

Le format de ce Certificat ainsi que ses attributs respectent le profil X.509v3 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

tbsCertList		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe.
signature		
▶ algorithm		Sha2withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ALMERY'S USER SIGNING CA NA OU = ADVANCED SERVICES OU = 0002 432701639 O = ALMERY'S C = FR
Validity		
▶ notBefore		Date de création (référentiel temporel de l'AC)
▶ notAfter		notBefore + durée ¹
subject GN=givenName SN=surName CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = \${Prénom usuel} \${Nom usuel} \${ID} ² GN = \${Prénom usuel} ³ SN = \${Nom usuel} ³ OU = \${Service} ³ OU = 0002 \${SIREN} ³ O = \${Client} ³ C = FR
subjectPublicKeyInfo		
▶ algorithm		
↳ algorithm		rsaEncryption (OID = 1.2.840.113549.1.1.1)
↳ parameters		RSAParams : NULL
▶ subjectPublicKey		DER encoded RSAPublicKey (2048 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé
Standard extensions	Critique :	
▶ authorityKeyIdentifier	Non	160 bits du haché SHA-1 de la clé publique de l'issuer
▶ subjectKeyIdentifier	Non	160 bits du haché SHA-1 de la clé publique de l'issuer
▶ keyUsage	Oui	nonRepudiation (1)
▶ privateKeyUsagePeriod		Extension non utilisée
▶ certificatePolicies		Stratégie du certificat : Identificateur de stratégie =

		1.2.250.1.16.12.5.41.1.4.1.1.1
▶ basicConstraints ↳ cA ↳ pathLenConstraint	Non	false None
▶ cRLDistributionPoints	Non	[1]Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : URL=http://pki.almerys.com/almerysusersigningcana.crl
Private extensions		
▶ authorityInfoAccess	Non	[1] : accessMethod : id-ad-calssuers accessLocation : URL=http://pki.almerys.com/almerysusersigningcana.cer
▶ subjectInfoAccess		Extension non utilisée
signatureAlgorithm		
algorithm		Sha2withRSAEncryption clé de 4096 bits
parameters		NULL

¹ La durée de vie du certificat est déterminée de la manière suivante :
24 heures pour un Certificat à usage unique

² Variables de l'attribut subject DN :

- \${Nom usuel} \${Prénom usuel} = nom et prénom de l'Utilisateur
- \${ID} = identifiant unique et aléatoire de Transaction de signature. Des contraintes sur le format de cet identifiant peuvent être imposées par l'AC.
- \${Service} = service proposé aux Utilisateurs par le Client, et pour lequel le Certificat est utilisable
- \${SIREN} = SIREN du Client
- \${Client} = raison sociale du Client

³ Non utilisée dans le cas d'un certificat pour un utilisateur Particulier

7.3 PROFIL DE LCR

Le tableau suivant fournit les valeurs par défaut des attributs de la Liste de Certificats Révoqués (LCR) émise par l'AC User Signing.

Le format de cette LCR ainsi que ses attributs respectent le profil X.509v2 décrit dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

tbsCertList		Valeur
version		1 (c'est-à-dire version2)
signature		
▶ algorithm		Sha2withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN = ALMERY'S USER SIGNING CA NA OU = ADVANCED SERVICES OU = 0002 432701639 O = ALMERY'S C = FR
thisUpdate		Date de création (référentiel temporel de l'AC)
nextUpdate		nextUpdate + 72 heures
revokedCertificates		
▶ userCertificate		n° de série du certificat révoqué
▶ revocationDate		date de révocation du certificat
▶ crlEntryExtensions		
↪ reasonCode		unspecified (0) <i>valeur par défaut</i>
crlExtensions	Critique :	
▶ authorityKeyIdentifier	Non	160 bits du haché SHA-1 de la clé publique de l'issuer
▶ issuerAltName	-	Extension non utilisée
▶ cRLNumber	Non	Numéro de séquence de la LCR (incrémental simple).
▶ deltaCRLIndicator	-	Extension non utilisée
▶ freshestCRL	-	Extension non utilisée
signatureAlgorithm		
algorithm		Sha2withRSAEncryption
parameters		NULL

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre concerne que les audits et évaluations de la responsabilité de l'AC ou de l'AE afin de s'assurer du bon fonctionnement de son IGC.

Dans ce cadre, le Client du service de signature d'Almerys a, quant à lui, la charge des audits et de l'évaluation de l'Autorité d'Enregistrement (AE), en tant que responsable de la gestion de cette AE. Almerys est donc habilitée, en tant qu'Autorité de Gouvernance de l'AC « Almerys User Signing CA NA », à demander un audit de l'AE, en tout ou partie.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Suite à toute modification significative d'une composante de l'IGC, l'AG procède à une analyse de sécurité et faire évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.

L'AG procède également régulièrement à un contrôle de conformité de l'IGC, en tout ou partie. La fréquence de ce contrôle est fournie dans la DPC associée à la présente PC.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

L'AG choisit et assigne une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité contrôlée.

8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC, et être dûment autorisée à pratiquer les contrôles visés.

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

Les audits de sécurité portent sur tout ou partie de l'IGC et visent à vérifier le respect des engagements et pratiques définies dans la présente PC et dans sa DPC.

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un audit de sécurité, l'équipe d'audit rend à l'AG, un avis parmi les suivants : « réussite », « échec », « à confirmer ».

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

- en cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AG qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du Certificat de la composante, la révocation de l'ensemble des Certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AG et doit respecter ses politiques de sécurité internes ;
- en cas de résultat « à confirmer », l'AG remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus ;

- en cas de réussite, l'AG confirme à la composante contrôlée la conformité aux exigences de la PC et de la DPC.

8.6 COMMUNICATION DES RESULTATS

Les modalités de communication concernant les résultats des audits de conformité sont précisées dans la DPC.

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

Les informations suivantes sont fournies dans les différents documents contractuels établis entre les parties : (i.e. Almerys, le Client du service de signature électronique (l'AE), les Utilisateurs du service, et éventuellement les fournisseurs assurant en tout ou partie certaines fonctions de l'AC « Almerys User Signing CA NA » ou de l'AE) :

- les conditions de facturation du service de certification électronique et de signature électronique proposé par Almerys,
- les responsabilités,
- les responsabilités financières,
- le montant des indemnités.
- L'accès à la fonction sur l'état des certificats n'est pas soumis à tarification.

9.2 RESPONSABILITE FINANCIERE

Cf 9.1 « Tarifs ».

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1. Périmètre des informations confidentielles

La classification des informations se décompose en :

- secret (niveau 4 de la Politique de Sécurité) ;
- confidentiel (niveau 3 de la Politique de Sécurité) ;
- interne (niveau 2 de la Politique de Sécurité).

Les informations considérées comme « secret » sont au moins les suivantes :

- les clés privées des AC de l'IGC Almerys, des composantes et des porteurs de certificats ;
- tous les secrets de l'IGC, notamment les informations liées à la gestion des modules cryptographiques (HSM) ;
- les données d'activation associées aux clés privées d'AC et de Porteurs.

Les informations considérées comme « confidentiel » sont au moins les suivantes :

- la DPC de l'AC ;
- les journaux d'événements des composantes de l'IGC..

9.3.2. Informations hors du périmètre des informations confidentielles

Par défaut, en complément des informations déjà explicitement listées dans les paragraphes 9.3.1 et 9.4, une information est considérée comme confidentielle à l'exception des informations publiées dont la liste est fournie dans la section 2.2 « Informations devant être publiées », et n'est diffusée qu'avec le consentement explicite de l'AG de l'IGC Almerys aux personnes ayant le besoin d'en connaître.

9.3.3. Responsabilités en terme de protection des informations confidentielles

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

9.4 PROTECTION DES DONNEES A CARACTERE PERSONNEL

9.4.1. Politique de protection des données à caractère personnel

Toute collecte et tout traitement de données à caractère personnel par l'AE et l'AC « Almerys User Signing CA NA » sont réalisés dans le strict respect de la réglementation en vigueur, et en particulier de la 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, dite « Loi Informatique et Libertés » [CNIL].

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les informations d'enregistrement de l'Utilisateur.

Elles doivent être traitées dans le strict respect de la réglementation en vigueur dite « Loi Informatique et Libertés ».

9.4.3. Responsabilité en termes de protection des données à caractère personnel

Le Client est responsable du respect de la réglementation en vigueur dite « Loi Informatique et Libertés ».

9.4.4. Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations à caractère personnel remises par les Porteurs aux Clients ne sont ni divulguées ni transférées à un tiers, sauf dans les cas suivants : consentement préalable de la personne concernée, décision judiciaire ou autre autorisation légale.

9.4.5. Conditions de divulgation d'informations à caractère personnel aux autorités judiciaires ou administratives

Toute diffusion et communication des données à caractère personnel vers des tiers autorisés doivent être en conformité aux lois spécifiques y afférant.

9.4.6. Autres circonstances de divulgation d'informations personnelles

Sans objet pour la présente PC.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

Tous les droits de propriété intellectuelle détenus par l'IGC Almerys sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et

pénale en cas de non respect. Par exemple, conformément au droit applicable les bases de données réalisées par les composantes de l'IGC sont protégées.

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 les articles L. 716-1 et suivants du Code de la propriété intellectuelle.

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux audits de sécurité et aux contrôles de conformité demandés par les parties prenantes dûment identifiées et habilitées,
- respecter les accords ou contrats qui les lient entre elles ou avec les Utilisateurs,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1. Autorité de Certification

L'AC « Almerys User Signing CA NA » a pour obligation de :

- pouvoir démontrer aux Applications utilisatrices de ses Certificats qu'elle a émis un Certificat pour un Utilisateur donné et que cet Utilisateur a accepté le Certificat, conformément aux exigences du chapitre 4.4 « Acceptation du certificat » ci-dessus ;
- protéger la clé privée des Porteurs conformément aux exigences de la présente PC ;
- garantir et maintenir la cohérence de la DPC avec la PC.

9.6.2. Autorité de Gouvernance

L'AG est responsable de la conformité de la PC de l'AC « Almerys User Signing CA NA », avec les exigences émises dans la PC de l'ACR. L'AG assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la PC de l'ACR, par l'AC « Almerys User Signing CA NA » ou l'une des composantes de l'IGC. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées aux opérations et/ou activités de l'AC « Almerys User Signing CA NA » et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC de l'ACR.

De plus, l'AG reconnaît engager sa responsabilité en cas de faute ou de négligence de l'AC « Almerys User Signing CA NA » ou de l'une des composantes de l'IGC, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données à caractère personnel des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des Certificats de l'AC « Almerys User Signing CA NA ».

Par ailleurs, l'AG reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des Certificats délivrés par l'AC « Almerys User Signing CA NA » ou l'une des composantes de l'IGC. Elle est

responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services.

9.6.3. Autorité d'enregistrement

Outre ses responsabilités décrites dans l'introduction de la section 9.6, et dans les sections 1.3.4 et 4, le Client en tant qu'AE doit :

- conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées
- et prendre toutes les mesures raisonnables pour s'assurer que les Utilisateurs qui requêtent l'AE 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 éventuellement utilisés.

9.6.4. Porteurs de certificats

Le Porteur doit :

- communiquer à l'AE (le Client) des informations exactes et à jour lors de la phase d'identification,
- protéger ses données d'activation de génération du Certificat et de Signature,
- accepter les Conditions Générales d'Utilisation des Certificats User signing.

9.6.5. Applications utilisatrices de certificats

Les Applications utilisant les Certificats doivent :

- vérifier et respecter l'usage pour lequel un Certificat a été émis ;
- contrôler que le Certificat émis par l'AC « Almerys User Signing CA NA » est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- vérifier la signature électronique de l'AC « Almerys User Signing CA NA » émettrice du Certificat en parcourant la chaîne de certification jusqu'à l'ACR « Almerys Root CA1 » ;
- vérifier et respecter les obligations des Applications utilisatrices de certificats exprimées dans la présente PC ;
- contrôler la validité des Certificats (dates de validité, statut de révocation).

9.6.6. Autres participants

Outre ses responsabilités décrites dans les chapitres 0 et 4, le Service support doit conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées.

9.7 LIMITE DE GARANTIE

Cf 9.1 « Tarifs ».

9.8 LIMITE DE RESPONSABILITE

Cf 9.1 « Tarifs ».

9.9 INDEMNITES

Cf 9.1 « Tarifs ».

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1. Durée de validité

La PC de l'AC « Almerys User Signing CA NA » 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

La publication d'une nouvelle version de la PC de l'AC Racine Almerys peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.

Suite à publication interne au sein de l'AC d'une nouvelle version de la PC AC racine, l'AC « Almerys User Signing CA NA » dispose d'un délai de 1 an pour se mettre en conformité.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3. Effets de la fin de validité et clauses restant applicables

Suite à l'arrêt de l'AC « Almerys User Signing CA NA » et donc à la fin de validité de cette politique, étant donné que le dernier certificat aura été émis avec une date de fin de validité T_{FIN_VAL} , les exigences des sections suivantes :

- 2 « RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES »
- 3.4 « Identification et validation d'une demande de révocation »
- 4.5 « Usages de la bi-clé et du certificat »
- 4.8 « Modification du certificat »
- 4.9 « Révocation et suspension des certificats »
- 4.10 « Fonction d'information sur l'état des certificats »

doivent rester applicables pendant cette même durée T_{FIN_VAL} .

9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC, L'AG devra au plus tard un mois avant le début de l'opération, faire valider ce changement, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC « Almerys User Signing CA NA » et de ses différentes composantes.

9.12 AMENDEMENTS A LA PC

9.12.1. Procédures d'amendements

Tout projet de modification de la présente PC doit rester conforme aux exigences de la politique de sécurité de l'IGC Almerys, de la PC de l'ACR et respecter les engagements avec les Utilisateurs existants du service de

signature. En cas de changement important, l'AG de l'IGC Almerys pourra faire appel à une expertise technique pour en contrôler l'impact.

La procédure d'amendement devra intégrer l'information et les délais d'information concernant les amendements. Les détails sont fournis dans la DPC..

La présente PC devra faire l'objet d'une revue au moins une fois par an, pouvant entraîner ou non un amendement.

9.12.2.Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC « Almerys User Signing CA NA » étant inscrit dans les Certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les Certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des Utilisateurs, qui ne peuvent donc pas s'appliquer aux Certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les Applications utilisatrices puissent clairement distinguer quels Certificats correspondent à quelles exigences.

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

En cas de litige sur l'interprétation du contenu ou l'exécution de la présente PC, une résolution amiable des conflits est privilégiée.

9.14 JURIDICTIONS COMPETENTES

Le droit applicable à tout litige relatif à l'interprétation et l'exécution de la présente PC est le droit français.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués en Annexe 1.

10. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 REGLEMENTATION

Renvoi	Document
[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
[LCEN]	Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés
[SIG_LOI]	Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
[SIG_DEC]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique

10.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS_A_3]	RGS - Fonction de sécurité « Signature électronique » - Version 2.3
[RGS_A_13]	RGS - Politiques de Certification Types - Variables de Temps - Version 2.3
[RGS_A_14]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3
[ETSI_NQCP]	ETSI TS 102 042 V2.1.1 (2002-04) Policy Requirements for Certification Authorities issuing public key certificates
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - 11/2003
[PROG_ACCRED]	COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf www.cofrac.fr
[CC]	Norme ISO/IEC 15408 : Critères communs version 2.1
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Recommendation X.509, version 3
[PC?]	Procédures et politiques de certification de clés, CISSI, version 2.2 de Janvier 2001.
[RFC822]	Standard for the format of Arpa internet text messages, August 13, 1982, Revised by David H. Crocker
[RFC5280]	Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280 May 2008
[ROLES_IGC]	Rôles des exploitants d'une infrastructure de gestion de clés, CISSI, version 1.2 de janvier 2001

Renvoi	Document
[DCSSI_ALGO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.0 du 3 mai 2004 N°1064 SGDN/DCSSI/SDS/AsTeC du 3 mai 2004
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)
[CWA14167-4]	CWA 14167-4 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSO-PP)