Autorité de Certification « ARIADNEXT Root CA G2 »

Politique de Certification

Version 1.8 - Rev aa381c9f31916a7e30ef3ea871b5efdc2ab9927e, 10/01/2024

IDnow.

Table des matières

Préface . . . 1
Identification du document . . . 1
Information de contact . . . 1
Suivi des modifications . . . 1
1. Introduction . . . 4
1.1. Présentation générale . . . 4
1.2. Identification du document . . . 4
1.3. Définitions et acronymes . . . 4
1.3.1. Acronymes . . . 4
1.3.2. Définitions . . . 5
1.4. Entités intervenant dans l'IGC . . . 8
1.4.1. Autorité de Certification . . . 8
1.4.2. Autorité d'Enregistrement . . . 9
1.4.3. Responsables de certificats . . . 10
1.4.4. Utilisateurs de certificats . . . 10
1.4.5. Autres participants . . . 10
1.5. Usage des certificats . . . 10
1.5.1. Domaines d'utilisation applicables . . . 10
1.5.1.1. Bi-clés et certificats des AC filles . . . 10
1.5.1.2. Bi-clés et certificats de l'AC Racine et de composantes . . . 10
1.5.2. Domaines d'utilisation interdits . . . 11
1.6. Gestion de la PC . . . 11
1.6.1. Entité gérant la PC . . . 11
1.6.2. Point de contact . . . 11
1.6.3. Entité déterminant la conformité d'une DPC avec cette PC . . . 11
1.6.4. Procédures d'approbation de la conformité de la DPC . . . 11
2. Responsabilités concernant la mise à disposition des informations devant être publiées . . . 12
2.1. Entités chargées de la mise à disposition des informations . . . 12
2.2. Informations devant être publiées . . . 12
2.3. Délais et fréquences de publication . . . 12
2.4. Contrôle d'accès aux informations publiées . . . 12
3. Identification et authentification . . . 14
3.1. Nommage . . . 14
3.1.1. Types de noms . . . 14
3.1.2. Nécessité d'utilisation de noms explicites . . . 14
3.1.3. Anonymisation ou pseudonymisation de serveurs . . . 14
3.1.4. Règles d'interprétation des différentes formes de noms . . . 14
3.1.5. Unicité des noms . . . 15
3.1.6. Identification, authentification et rôle des marques déposées . . . 15
3.2. Validation initiale de l'identité . . . 15
3.2.1. Méthode pour prouver la possession de la clé privée . . . 15

3.2.2. Validation de l'identité d'un organisme . . . 15
3.2.3. Validation de l'identité d'un individu . . . 15
3.2.3.1. Enregistrement d'un Responsable d'AC sans MC pour un certificat d'AC Fille à émettre 15
3.2.3.2. Enregistrement d'un nouveau Responsable d'AC sans MC pour un certificat d'AC Fille déjà émis 16
3.2.3.3. Enregistrement d'un Mandataire de Certification . . . 16
3.2.3.4. Enregistrement d'un Responsable d'AC via un MC pour un certificat d'AC Fille à émettre 16
3.2.3.5. Enregistrement d'un nouveau Responsable d'AC via un MC pour un certificat d'AC Fille déjà émis 16
3.2.4. Informations non vérifiées du Responsable d'AC . . . 16
3.2.5. Validation de l'autorité du demandeur . . . 16
3.2.6. Certification croisée d'AC . . . 17
3.3. Identification et validation d'une demande de renouvellement de clés . . . 17
3.3.1. Identification et validation pour un renouvellement courant . . . 17
3.3.2. Identification et validation pour un renouvellement après révocation . . . 17
3.4. Identification et validation d'une demande de révocation . . . 17
4. Exigences opérationnelles sur le cycle de vie des certificats . . . 18
4.1. Demande de certificat . . . 18
4.1.1. Origine d'une demande de certificat . . . 18
4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificats . . . 18
4.2. Traitement d'une demande de certificat . . . 18
4.2.1. Exécution des processus d'identification et de validation de la demande . . . 18
4.2.2. Acceptation ou rejet de la demande . . . 18
4.2.3. Durée d'établissement du certificat . . . 18
4.3. Délivrance du certificat . . . 19
4.3.1. Actions de l'AC concernant la délivrance du certificat . . . 19
4.3.2. Notification par l'AC de la délivrance du certificat au Responsable d'AC . . . 19
4.4. Acceptation du certificat . . . 19
4.4.1. Démarche d'acceptation du certificat . . . 19
4.4.2. Publication du certificat . . . 19
4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat . . . 19
4.5. Usage de la bi-clé et du certificat . . . 19
4.5.1. Utilisation de la clé privée et du certificat par le Responsable d'AC . . . 19
4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat . . . 19
4.6. Renouvellement d'un certificat d'AC Racine ou Fille . . . 19
4.7. Délivrance d'un nouveau certificat Racine ou Fille suite à changement de la bi-clé . . . 20
4.7.1. Causes possibles de changement de bi-clé . . . 20
4.7.2. Origine d'une demande de nouveau certificat . . . 20
4.7.3. Procédure de traitement d'une demande de nouveau certificat . . . 20
4.7.4. Notification au RC de l'établissement du nouveau certificat . . . 20
4.7.5. Démarche d'acceptation du nouveau certificat . . . 20
4.7.6. Publication du nouveau certificat . . . 20
4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat . . . 20

4.8. Modification du certificat . . . 20
4.9. Révocation et Suspension des certificats . . . 20
4.9.1. Causes possibles d'une révocation . . . 20
4.9.1.1. Certificats d'AC Filles ou Racine . . . 20
4.9.1.2. Certificats d'une composante de l'IGC . . . 21
4.9.2. Origine d'une demande de révocation . . . 21
4.9.2.1. Certificats d'AC Fille ou Racine . . . 21
4.9.2.2. Certificats d'une des composantes de l'IGC . . . 21
4.9.3. Procédure de traitement d'une demande de révocation . . . 21
4.9.3.1. Révocation d'un certificat d'AC Fille ou Racine . . . 21
4.9.3.2. Révocation d'un certificat d'une composante de l'IGC . . . 22
4.9.4. Délai accordé au RCC pour formuler la demande de révocation . . . 22
4.9.5. Délai de traitement par l'AC d'une demande de révocation . . . 22
4.9.5.1. Révocation d'un certificat d'AC . . . 22
4.9.5.2. Disponibilité du système de traitement des demandes de révocation . . . 22
4.9.5.3. Révocation d'un certificat d'une composante de l'IGC . . . 22
4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats . . . 23
4.9.7. Fréquence d'établissement des ARL . . . 23
4.9.8. Délai maximum de publication d'une ARL . . . 23
4.9.9. Exigences sur la vérification en ligne de la révocation et l'état des certificats . . . 23
4.9.10. Autres moyens disponibles d'information sur les révocations . . . 23
4.9.11. Exigences spécifiques en cas de compromission de la clé privée . . . 23
4.9.12. Causes possibles d'une suspension . . . 23
4.9.13. Origine d'une demande de suspension . . . 23
4.9.14. Procédure de traitement d'une demande de suspension . . . 24
4.9.15. Limites de la période de suspension d'un certificat . . . 24
4.10. Fonction d'information sur l'état des certificats . . . 24
4.10.1. Caractéristiques opérationnelles . . . 24
4.10.2. Disponibilité de la fonction . . . 24
4.10.3. Dispositifs optionnels . . . 24
4.11. Fin de la relation entre le RC et l'AC . . . 24
4.12. Séquestre de clé et recouvrement . . . 24
4.12.1. Politique et pratiques de recouvrement par séquestre de clés . . . 24
4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session . . . 24
5. Mesures de sécurité non techniques . . . 25
5.1. Mesures de sécurité physique . . . 25
5.1.1. Situation géographique et construction des sites . . . 25
5.1.2. Accès physique . . . 25
5.1.3. Alimentation électrique et climatisation . . . 25
5.1.4. Vulnérabilité aux dégâts des eaux . . . 25
5.1.5. Prévention et protection incendie . . . 25
5.1.6. Conservation des supports . . . 26
5.1.7. Mise hors service des supports . . . 26
5.1.8. Sauvegarde hors site . . . 26

5.2. Mesures de sécurité procédurales . . . 26
5.2.1. Rôles de confiance . . . 26
5.2.2. Nombre de personnes requises par tâche . . . 27
5.2.3. Identification et authentification pour chaque rôle . . . 27
5.2.4. Rôles exigeant une séparation des attributions . . . 27
5.3. Mesures de sécurité vis à vis du personnel . . . 28
5.3.1. Qualifications, compétences, et habilitations requises . . . 28
5.3.2. Procédures de vérification des antécédents . . . 28
5.3.3. Exigences en matière de formation initiale . . . 28
5.3.4. Exigences et fréquence en matière de formation continue . . . 28
5.3.5. Fréquence et séquence de rotations entre différentes attributions . . . 28
5.3.6. Sanctions en cas d'actions non autorisées . . . 28
5.3.7. Exigences vis à vis du personnel des prestataires externes . . . 28
5.3.8. Documentation fournie au personnel . . . 29
5.4. Procédures de constitution des données d'audit . . . 29
5.4.1. Type d'événement à enregistrer . . . 29
5.4.2. Fréquence de traitement des journaux d'événements . . . 29
5.4.3. Période de conservation des journaux d'événements . . . 30
5.4.4. Protection des journaux d'événements . . . 30
5.4.5. Procédure de sauvegarde des journaux d'événements . . . 30
5.4.6. Système de collecte des journaux d'événements . . . 30
5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement . . . 30
5.4.8. Evaluation des vulnérabilités . . . 30
5.5. Archivage des données . . . 30
5.5.1. Types de données à archiver . . . 30
5.5.2. Période de conservation des archives . . . 31
5.5.3. Protection des archives . . . 31
5.5.4. Procédure de sauvegarde des archives . . . 31
5.5.5. Exigences d'horodatage des données . . . 31
5.5.6. Système de collecte des archives . . . 31
5.5.7. Procédure de récupération et de vérification des archives . . . 31
5.6. Changement de clés d'AC . . . 31
5.7. Reprise suite à compromission et sinistre . . . 32
5.7.1. Procédures de remontée et de traitement des incidents et des compromissions . . . 32
5.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) 32
5.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante . . . 33
5.7.4. Capacités de continuité d'activité suite à un sinistre . . . 33
5.8. Fin de vie de l'IGC . . . 33
5.8.1. Transfert d'activité ou cessation d'activité affectant une composante de l'IGC . . . 33
5.8.2. Cessation d'activité affectant l'AC . . . 34
6. Mesures de sécurité techniques . . . 36
6.1. Génération et installation des bi clés . . . 36
6.1.1. Génération des bi clés . . . 36

6.1.1.1. Clés d'AC Racine . . . 36
6.1.1.2. Clés d'AC Filles générées par l'AC . . . 36
6.1.1.3. Clés d'AC Filles générées au niveau des AC Filles . . . 36
6.1.2. Transmission de la clé privée à l'AC Fille . . . 37
6.1.3. Transmission de la clé publique à l'AC Racine . . . 37
6.1.4. Transmission de la clé publique de l'AC Racine aux utilisateurs de certificats . . . 37
6.1.5. Tailles des clés . . . 37
6.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité . . . 37
6.1.7. Objectifs d'usages de la clé . . . 37
6.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques . 38
6.2.1. Standards et mesures de sécurité pour les modules cryptographiques . . . 38
6.2.1.1. Module cryptographique de l'AC Racine . . . 38
6.2.1.2. Dispositifs de protection des clés privées des AC Filles . . . 38
6.2.2. Contrôle de la clé privée par plusieurs personnes . . . 38
6.2.3. Séquestre de la clé privée . . . 38
6.2.4. Copie de secours de la clé privée . . . 38
6.2.5. Archivage de la clé privée . . . 38
6.2.6. Transfert de la clé privée vers / depuis le module cryptographique . . . 38
6.2.7. Stockage de la clé privée dans un module cryptographique . . . 39
6.2.8. Méthode d'activation de la clé privée . . . 39
6.2.8.1. Clés privées d'AC Racine . . . 39
6.2.8.2. Clés privées des AC Filles . . . 39
6.2.9. Méthode de désactivation de la clé privée . . . 39
6.2.9.1. Clés privées de l'AC Racine . . . 39
6.2.9.2. Clés privées des AC Filles . . . 39
6.2.10. Méthode de destruction des clés privées . . . 39
6.2.10.1. Clés privées d'AC Racine . . . 39
6.2.10.2. Clés privées des AC Filles . . . 39
6.2.11. Niveau de qualification du module cryptographique et des dispositifs de création de cachet 40
6.3. Autres aspects de la gestion des bi clés . . . 40
6.3.1. Archivage des clés publiques . . . 40
6.3.2. Durée de vie des bi-clés et des certificats . . . 40
6.4. Données d'activation . . . 40
6.4.1. Génération et installation des données d'activation . . . 40
6.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC Racine 40
6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée des AC Filles 40
6.4.2. Protection des données d'activation . . . 40
6.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC Racine . . . 40
6.4.2.2. Protection des données d'activation correspondant aux clés privées des AC Filles . . . 40
6.4.3. Autres aspects liés aux données d'activation . . . 41
6.5. Mesures de sécurité des systèmes informatiques . . . 41

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques . . . 41
6.5.2. Niveau de qualification des systèmes informatiques . . . 41
6.6. Mesures de sécurité des systèmes durant leur cycle de vie . . . 42
6.6.1. Mesures de sécurité liées au développement des systèmes . . . 42
6.6.2. Mesures liées à la gestion de la sécurité . . . 42
6.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes . . . 42
6.7. Mesures de sécurité réseau . . . 42
6.8. Horodatage / système de datation . . . 42
7. Profils des certificats, OCSP et des LCR . . . 43
7.1. Profils des certificats . . . 43
7.1.1. Certificat de l'AC . . . 43
7.1.1.1. Champs de base . . . 43
7.1.1.2. Extensions . . . 44
7.1.2. Certificats des sous-AC . . . 45
7.1.2.1. Champs de base . . . 45
7.1.2.2. Extensions . . . 46
7.2. Profil des Listes de Certificats Révoqués . . . 46
7.2.1. Champs de base des ARL . . . 46
7.2.2. Extensions des ARL . . . 47
8. Audit de conformité et autres évaluations . . . 48
8.1. Fréquences et / ou circonstances des évaluations . . . 48
8.2. Identités / qualification des évaluateurs . . . 48
8.3. Relations entre évaluateurs et entités évaluées . . . 48
8.4. Sujets couverts par les évaluations . . . 48
8.5. Actions prises suite aux conclusions des évaluations . . . 48
8.6. Communication des résultats . . . 49
9. Autres problématiques métiers et légales . . . 50
9.1. Tarifs . . . 50
9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats d'AC . . . 50
9.1.2. Tarifs pour accéder aux certificats . . . 50
9.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats . . . 50
9.1.4. Tarifs pour d'autres services . . . 50
9.1.5. Politique de remboursement . . . 50
9.2. Responsabilité financière . . . 50
9.2.1. Couverture par les assurances . . . 50
9.2.2. Autres ressources . . . 50
9.2.3. Couverture et garantie concernant les entités utilisatrices . . . 50
9.3. Confidentialité des données professionnelles . . . 50
9.3.1. Périmètre des informations confidentielles . . . 50
9.3.2. Informations hors du périmètre des informations confidentielles . . . 51
9.3.3. Responsabilités en terme de protection des informations confidentielles . . . 51
9.4. Protection des données personnelles . . . 51
9.4.1. Politique de protection des données personnelles . . . 51
9.4.2. Informations à caractère personnel . . . 51

9.4.3. Informations à caractère non personnel . . . 51
9.4.4. Responsabilité en terme de protection des données personnelles . . . 51
9.4.5. Notification et consentement d'utilisation des données personnelles . . . 52
9.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives 52
9.4.7. Autres circonstances de divulgation d'informations personnelles . . . 52
9.5. Droits sur la propriété intellectuelle et industrielle . . . 52
9.6. Interprétations contractuelles et garanties . . . 52
9.6.1. Autorités de certification . . . 52
9.6.2. Service d'enregistrement . . . 53
9.6.3. Utilisateurs de certificats . . . 53
9.6.4. Autres participants . . . 54
9.7. Limite de garantie . . . 54
9.8. Limite de responsabilité . . . 54
9.9. Indemnités . . . 54
9.10. Durée et fin anticipée de validité de la PC . . . 54
9.10.1. Durée de validité . . . 54
9.10.2. Fin anticipée de validité . . . 54
9.10.3. Effets de la fin de validité et clauses restant applicables . . . 55
9.11. Notifications individuelles et communications entre les participants . . . 55
9.12. Amendements à la PC . . . 55
9.12.1. Procédures d'amendements . . . 55
9.12.2. Mécanisme et période d'information sur les amendements . . . 55
9.12.3. Circonstances selon lesquelles l'OID doit être changé . . . 55
9.13. Dispositions concernant la résolution de conflits . . . 55
9.14. Juridictions compétentes . . . 55
9.15. Conformité aux législations et réglementations . . . 55
9.16. Dispositions diverses . . . 56
9.16.1. Accord global . . . 56
9.16.2. Transfert d'activités . . . 56
9.16.3. Conséquences d'une clause non valide . . . 56
9.16.4. Application et renonciation . . . 56
9.16.5. Force majeure . . . 56
9.17. Autres dispositions . . . 56

Préface

Identification du document

Titre	Autorité de Certification « ARIADNEXT Root CA G2 » : Politique de Certification
OID	1.3.6.1.4.1.38226.10.4.1.1.1.1
Référence	PKI_PC_G2_Root_FR
Niveau de diffusion	Public
Version	1.8 - Rev aa381c9f31916a7e30ef3ea871b5efdc2ab9927e
Valideur(s)	Marc NORLAIN
Date	10/01/2024

Information de contact

Addresse	Autorité de Certification IDnow SAS 122 rue Robert Keller 35510 CESSON-SEVIGNE – France
Email	certificats@idnow.io

Suivi des modifications

Version	Date de version	Nature de la modification	Entité/Nom Prénom
v1.0	19/03/2015	Création	ARIADNEXT / Claire-Lise Beaumont

Version	Date de version	Nature de la modification	Entité/Nom Prénom
v1.1	04/09/2019	Mise à jour des sections suivantes : • § 1.1 Référence supprimée au niveau 3 étoiles (***) du RGS V2 • § 1.6.2 Changement d'adresse d'ARIADNEXT • § 2.3 Mise à jour DMIA de la fonction d'information • § 5.4.6 Correction relative à la nature des logs collectés • § 6.2.8.1 Suppression de l'occurrence aux porteurs de secrets • § 8.1 Fréquence du contrôle de conformité interne • § 9.3.1 Suppression du caractère confidentiel de certaines parties de la DPC • § 9.4.1, § 9.14 et § 9.15 suite à l'entrée en vigueur du RGPD	ARIADNEXT / Nicolas GENET
v1.2	14/02/2020	Mise à jour de la charte graphique et mise à jour des sections suivantes: • § 4.10.2 en cohérence avec § 2.3 • § 5.2.4: suppression du cumul des rôles spécifiques au niveau 3 étoiles (***) du RGS V2 • § 5.3.2: ajout détail sur les vérifications des antécédents • § 5.4.2: mise à jour de la fréquence des rapprochements en cohérence avec RGS*	ARIADNEXT / Christian Brunette
v1.3	08/06/2020	Mise à jour des sections suivantes : • § 5.8.2 Ajout de la mention de suppression des sauvegardes	ARIADNEXT / Christian Brunette
v1.4	08/09/2020	Mise à jour suite à évolution de la politique de classification et de marquage de l'information	ARIADNEXT / Christian Brunette
v1.5	01/10/2021	Revue annuelle § 1.3.1 Ajout définition "PSCO" § 5.3.7 Ajout de la possibilité pour l'IGC de faire appel à des prestataires externes	ARIADNEXT / Christian Quivy

Version	Date de version	Nature de la modification	Entité/Nom Prénom
v1.6	02/03/2022	Mise à jour des sections suivantes : • § 1.6.2 Mise à jour de l'adresse postale • § 7 Explicitation des profils de certificats, de CRL et d'OCSP • § 4.9.7 Précision sur la fréquence de génération de l'ARL • § 5.8.1 et § 5.8.2 Ajout de détails concernant les procédures de transfert ou cessation d'activité	ARIADNEXT / Christian Brunette
v1.7	06/10/2023	Mise à jour des sections suivantes : • Mise à jour des informations de contact dans Information de contact et § 1.6.2 • Ajout précision dans § 1.1 concernant le changement de nom de l'entité légale d'ARIADNEXT vers IDnow • Mise à jour de § 5.6 pour indiquer l'existence de la hiérarchie d'AC de remplacement • Ajout rôle dans § 5.2.1 • Mise à jour de la charte graphique	IDnow SAS / Christian Brunette
v1.8	10/01/2024	Indique dans § 5.8.1 la publication du certificat d'AC (comme pour les CRLs)	IDnow SAS / Christian Brunette

1. Introduction

1.1. Présentation générale

ARIADNEXT est un fournisseur de solutions innovantes pour la **dématérialisation** et la **sécurisation** des données. Depuis juin 2023, **ARIADNEXT SAS est devenu IDnow SAS**. IDnow SAS fait partie du groupe IDnow. Les activités de gestion de l'Autorité de Certification sont gérées depuis l'entité française IDnow SAS. Dans le présent document, toute référence à ARIADNEXT correspond à l'entité IDnow SAS, mais l'utilisation de la marque commerciale IDnow est également possible. Le nom ARIADNEXT est conservé dans le nom des Autorités de Certificats.

Pour sécuriser certains usages, **IDnow déploie des certificats** soit à des **personnes physiques**, soit à des **équipements matériels** (serveurs, token…). Ces certificats sont utilisés **soit en interne** dans le système d'information d'IDnow, **soit pour les besoins des solutions** proposées par **IDnow** à ses clients.

L'ensemble de ces besoins de certificats sont adressés par une **PKI propre à IDnow SAS**, hébergée et opérée **en interne**. Cette PKI comporte plusieurs Autorités de Certification filles **d'une même racine, « ARIADNEXT Root CA G2 »**. On appelle cette PKI la **« PKI ARIADNEXT G2 »**.

Cette PKI est mise en œuvre conformément aux standards et aux bonnes pratiques dans le domaine. **Elle est définie et mise en œuvre conformément aux exigences du Référentiel Général de Sécurité, Version 2, niveau* (1 étoile).**

Le présent document constitue la Politique de Certification de l'**Autorité de Certification Racine « ARIADNEXT Root CA G2 »** émettant des certificats d'Autorité de Certification Filles.

1.2. Identification du document

L'Autorité de Certification « ARIADNEXT Root CA G2 » dans sa version 1 est identifiée par l'OID
1.3.6.1.4.1.38226.10.4.1.1.1

La Déclaration de Pratiques de Certification correspondante est identifiée par l'OID
1.3.6.1.4.1.38226.10.4.1.2.1

Le document PKI_OID décrit les règles de définition des OID.

1.3. Définitions et acronymes

1.3.1. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CEN	Comité Européen de Normalisation

CRL	Certificate Revocation List (ou LCR)
CSR	Certificate Signing Request
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
FNTC	Fédération Nationale des Tiers de Confiance
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés (ou PKI, Public Key Infrastructure)
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués (ou CRL)
MC	Mandataire de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSC	Opérateur de Service de Certification
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
PSCO	Prestataire de Services de COnfiance
RGS	Référentiel Général de Sécurité
RSA	Rivest Shamir Adelman
SSL	Secure Sockets Layer
TLS	Transport Layer Security
SSCD	Signature Secure Creation Device
URL	Uniform Resource Locator

1.3.2. Définitions

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une Politique de Certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette Politique de Certification. Le terme de PSCE n'est pas utilisé en dehors du présent paragraphe et du § 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la Politique de Certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Autorité d'enregistrement (AE) - Voir § 1.4.2.

Bi-clé - Une bi-clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

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

Composante - 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. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

CSR (Certificate Signing Request) - Message au format PKCS#10 qui permet d'adresser à l'Autorité de Certification une requête signée de création de certificat et signature de ce certificat, contenant une clé publique préalablement générée.

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

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privée de type associations. Chaque certificat cachet se rapporte à une entité.

Fonction de génération des clés et des certificats - Cette fonction génère les clés dans les différents supports cryptographiques autorisés par l'IGC, et les certificats (création du format, signature électronique avec la clé privée de l'AC) à partir des informations transmises par l'autorité d'enregistrement et de la clé publique de l'entité à certifier.

Fonction de génération des éléments secrets de l'IGC - Cette fonction génère des moyens d'authentification pour l'accès à différents composants de l'IGC, sous la forme de secrets (par exemple, les parts de secret permettant l'accès au HSM).

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.

Fonction de publication - Voir § 2.

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

HSM (Hardware Security Module) - Boîtier cryptographique matériel dans lequel sont stockées les clés publiques et privées des Autorités de Certification.

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC

peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Key Ceremony (KC) - Cérémonie de clés au cours de laquelle des opérations sensibles sont réalisées : initialisation de modules cryptographiques, génération de bi-clés, restauration de bi-clés sur des nouveaux modules cryptographiques etc. Une Key Ceremony a lieu dans un environnement sécurisé, en présence de témoins, et se déroule selon un script pré-établi.

Liste de Certificats Révoqués (LCR) - Liste contenant les identifiants des certificats révoqués ou invalides.

Mandataire de certification - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des Porteurs de cette entité (il assure notamment le face-à-face pour l'identification des Porteurs lorsque celui-ci est requis). Le rôle de mandataire de certification n'est pas utilisé par cette AC.

Motif de révocation - Circonstance pouvant être à l'origine de la révocation d'un certificat. Les motifs de révocation sont détaillés au § 4.9.1.

OID - Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Personne autorisée - Il s'agit d'une personne autre que le Porteur et le mandataire de certification et qui est autorisée par la Politique de Certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du Porteur (demande de révocation, de renouvellement, ...). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du Porteur ou d'un responsable des ressources humaines.

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 clients et les utilisateurs de certificats.

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des Porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Produit de sécurité - Un 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.

Public Key Infrastructure (PKI) - Infrastructure de Gestion de Clés (IGC) - Infrastructure technique

permettant de mettre en œuvre toutes les fonctions de l'Autorité de Certification et de l'Autorité d'Enregistrement.

Qualification d'un prestataire de services de certification électronique - Le décret « RGS » n°2010-112 décrit la procédure de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Qualification d'un produit de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le RGS. La procédure de qualification des produits de sécurité est décrite dans le décret « RGS » n°2010-112. Le RGS précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Renouvellement d'un certificat - Correspond à une nouvelle demande de certificat. Opération effectuée à la demande d'un client ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat sur la base d'une nouvelle bi-clé.

Révocation d'un certificat - Opération dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité. La demande peut être la conséquence de différents types d'événements tels que la compromission d'une bi-clé, le changement d'informations contenues dans un certificat, etc. L'opération de révocation est considérée terminée quand le certificat mis en cause est publié dans la Liste des Certificats Révoqués. Le certificat ne doit alors plus être utilisé.

Système d'information - Tout ensemble de moyen destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Utilisateur de certificat - Voir § 1.4.4.

Validation de certificat - Opération de contrôle du statut (révoqué ou non) d'un certificat.

Validation de signature - Opération de contrôle d'une signature numérique

1.4. Entités intervenant dans l'IGC

1.4.1. Autorité de Certification

IDnow joue le rôle **d'Autorité de Certification Racine**.

L'Autorité de Certification (AC) garantit le niveau de confiance dans les certificats émis.

Elle définit et assure la **mise en œuvre des fonctions** suivantes :

- **Génération de la clé de l'AC racine, du certificat de l'AC racine, des certificats des AC Filles et des éléments secrets de l'IGC** : cette fonction est décrite au § 6.
- **Remise au Responsable de Certificat** : cette fonction consiste à remettre le certificat au Responsable de Certificat (en l'occurrence, le Responsable de l'Autorité de Certification, voir § 1.4.3). Cette fonction est décrite aux § 3 et § 4.

- **Autorité d'Enregistrement et gestion du cycle de vie des certificats** (enregistrement, révocation, renouvellement) : cette fonction est décrite aux § 3 et § 4.
- **Publication des informations réglementaires de l'AC Racine** : cette fonction est décrite au § 2.2.
- **Publication des informations sur le statut (ou l'état) des certificats des AC filles** : cette fonction est décrite au § 4.10.
- **Gestion des révocations** : cette fonction est décrite au § 4.9.

L'Autorité de Certification remplit les exigences suivantes :

- Être une **entité légale** au sens de la loi française.
- Être en **relation par voie contractuelle / hiérarchique / réglementaire avec l'entité** pour laquelle elle a **en charge** la gestion **des certificats** de cette entité.
- **Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux RC, aux utilisateurs de certificats**, ceux qui mettent en œuvre ses certificats.
- **S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées** par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- **Mettre en œuvre les différentes fonctions identifiées dans sa PC**, correspondant au minimum aux fonctions obligatoires de la présente PC Type, notamment en matière de génération des certificats, de remise au RC, de gestion des révocations et d'information sur l'état des certificats.
- **Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles**, concernant ses installations, ses systèmes et ses biens informationnels.
- **Mener une analyse de risques permettant de déterminer les objectifs de sécurité** propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. L'AC élabore sa DPC en fonction de cette analyse.
- **Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC**, et correspondant au minimum aux exigences des PC Types du RGS, notamment en termes de fiabilité, de qualité et de sécurité.
- **Générer**, et renouveler lorsque nécessaire, **ses bi-clés et les certificats correspondants** (signature de certificats, de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux RC et utilisateurs de certificats.
- **Suivre les demandes en capacité** et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

1.4.2. Autorité d'Enregistrement

Remarque : toutes les actions de l'Autorité d'Enregistrement ont lieu à l'occasion de « Key Ceremony », qui sont des événements planifiés et documentés.

La fonction d'Autorité d'Enregistrement (AE) de l'AC Racine est assurée au sein d'IDnow.

L'Autorité d'Enregistrement assure **les missions principales suivantes** :

- **La validation de l'identité et de la qualité des porteurs de secret** lors de l'enregistrement des demandes de certificats.

- **L'établissement et la transmission de la demande de certificat** à l'Autorité de Certification, lors d'une Key Ceremony.
- **La gestion opérationnelle du cycle de vie des certificats** (demandes, renouvellement, révocation).

De plus, l'Autorité d'Enregistrement assure les fonctions complémentaires suivantes :

- Archivage des documents de Key Ceremony.
- Conservation et protection des données des personnes concernées par les fonctions de l'IGC.

1.4.3. Responsables de certificats

Tous les certificats d'Autorités de Certification sont de la responsabilité du Responsable d'Autorité de Certification correspondant (voir les rôles de confiance § 5.2.1).

Le Responsable d'Autorité de Certification est responsable de l'utilisation par l'Autorité de Certification de la PKI G2 du certificat électronique identifié dans le certificat et de la clé privée correspondante.

Le Responsable d'AC est une personne interne à IDnow. Le changement de Responsable d'AC est géré par IDnow dans le cadre de la procédure de gestion des autorisations sur les systèmes d'information (SSI_PROC_AUTORISATION).

S'il n'existe plus de Responsable d'AC pour une AC, le certificat d'AC doit être révoqué.

1.4.4. Utilisateurs de certificats

Les **utilisateurs** des certificats émis par l'AC Racine (donc les certificats d'AC Filles) sont tous les services nécessitant de valider la chaîne de confiance d'un certificat d'entité finale de la PKI ARIADNEXT G2.

1.4.5. Autres participants

Sans objet.

1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

1.5.1.1. Bi-clés et certificats des AC filles

La clé privée des certificats des AC Filles est utilisée uniquement dans les cas suivants :

- Signature des certificats d'entité finale.
- Signature des Listes de Certificats Révoqués (LCR ou CRL).

La clé privée est générée et confinée dans un module cryptographique (matériel) qualifié, conformément aux exigences du RGS***.

1.5.1.2. Bi-clés et certificats de l'AC Racine et de composantes

La clé privée de l'Autorité de Certification **ARIADNEXT Root CA G2** est utilisée uniquement dans les cas suivants :

- Signature des certificats des AC Filles.
- Signature des Listes des Autorités Révoquées (LAR ou ARL).

La même bi-clé est utilisée pour les deux opérations mentionnées ci-dessus. S'agissant d'une AC Racine, le certificat de cette bi-clé est auto-signé.

D'autres certificats sont utilisés dans le cadre de l'IGC :

- Authentification mutuelle entre les différents composants logiciels de l'IGC.
- Authentification des administrateurs IDnow lors de l'accès aux serveurs de l'IGC.

1.5.2. Domaines d'utilisation interdits

Les usages autres que ceux autorisés au § 1.5.1 sont interdits.

1.6. Gestion de la PC

1.6.1. Entité gérant la PC

Le responsable d'AC (voir les rôles de confiance au § 5.2.1) est chargé de la validation et de la gestion de la PC.

Des revues de direction sont organisées annuellement au sein d'IDnow sur le sujet de l'AC.

1.6.2. Point de contact

Les questions ou remarques à l'intention de l'AC peuvent être adressées à IDnow par les moyens suivants :

- **Email** : certificats@idnow.io
- **Courrier** : Autorité de Certification IDnow SAS, 122 rue Robert Keller, 35510 Cesson-Sévigné – France.

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

Le responsable d'AC est responsable de la validation de la conformité de la DPC avec la PC.

1.6.4. Procédures d'approbation de la conformité de la DPC

L'AC s'assure de la mise à jour de la DPC conformément aux modifications apportées à l'IGC.

L'AC met en œuvre un processus d'approbation de la conformité de la DPC avec la PC.

L'AC tient à disposition la dernière version de la DPC, pour les personnes autorisées (voir Déclaration des Pratiques de Certification).

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1. Entités chargées de la mise à disposition des informations

IDnow SAS assure la publication de toutes les informations citées au § 2.2, via le site de publication https://certificats.ariadnext.com.

2.2. Informations devant être publiées

L'AC publie les informations suivantes :

- Politique de Certification de l'AC Racine.
- Certificat d'AC Racine.
- Empreinte du certificat d'AC Racine.
- Liste des Autorités Révoquées (LAR).
- Adresse email du point de contact de l'AC.
- Coordonnées de l'Autorité d'Enregistrement : numéro de téléphone, adresse email, adresse postale.

L'AC garantit l'**intégrité** et la **lisibilité** des informations publiées.

S'agissant d'une AC Racine où les certificats sont placés sous la responsabilité des Responsables d'AC :

- Les Conditions Générales d'Utilisation de l'AC Racine ne sont pas formalisées et donc non publiées.
- Les formulaires de gestion des certificats ne sont pas définis et donc non publiés.

2.3. Délais et fréquences de publication

Les informations devant être publiées citées au § 2.2 sont **publiées dans les meilleurs délais** :

- Suite à leur validation (cas de la PC ou des informations de contact).
- Suite à leur mise à jour, **dans un délai maximal de 24 heures ouvrées** (cas du certificat d'AC Racine, de son empreinte, et des LAR).

La fonction **d'information sur l'état des certificats** est disponible **24 heures / 24 et 7 jours / 7**. De plus :

- La **durée maximale d'indisponibilité par interruption** de cette fonction est de **4 heures sur des jours ouvrés**.
- La **durée maximale totale d'indisponibilité par mois** de cette fonction est de **32 heures sur des jours ouvrés**.

La fonction de **publication des certificats d'AC** est disponible **24 heures / 24 et 7 jours / 7**.

2.4. Contrôle d'accès aux informations publiées

Toutes les informations du site de publication sont **libres d'accès en lecture**.

L'accès en modification à ces informations est **autorisé** pour les administrateurs d'IDnow disposant d'un **rôle de confiance** (voir § 5.2.1). Il requiert une **authentification** par certificat sur support physique (voir § 1.5.1.2) et le **contrôle de l'habilitation** de l'administrateur sur le site de publication.

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés sont conformes à la norme X.500.

Les certificats de l'AC Racine et des AC Filles sont identifiés par un DN de type X.501.

Le DN du certificat de l'AC Racine comporte les informations suivantes :

Country	FR
Organization	AriadNEXT
Organization Unit	0002 52076922500027
Common Name	AriadNEXT Root CA G2

Le DN du certificat des AC Filles est construit selon le modèle suivant :

Country	FR
Organization	AriadNEXT
Organization Unit	0002 52076922500027
Common Name	[nom de l'AC Fille]

3.1.2. Nécessité d'utilisation de noms explicites

La décomposition du DN est la suivante :

- Champ C (Country) : contient le pays où est basé le siège social d'IDnow SAS (ARIADNEXT au moment de la création des ACs).
- Champ O (Organization) : contient le nom « AriadNEXT ».
- Champ OU (Organizational Unit) : contient le numéro de SIREN ou SIRET d'IDnow SAS (ARIADNEXT au moment de la création des ACs).
- Champs CN (Common Name) : ce champ contient le nom de l'AC Fille qui doit être unique.

3.1.3. Anonymisation ou pseudonymisation de serveurs

Sans objet.

Les pseudonymes et les certificats anonymes ne sont pas autorisés par la présente Politique de Certification.

3.1.4. Règles d'interprétation des différentes formes de noms

Aucune interprétation particulière n'est à faire sur le nom des certificats.

3.1.5. Unicité des noms

L'AC Racine se porte garante de **l'unicité des noms des certificats qu'elle émet**. Cette unicité repose sur le Distinguished Name (DN) défini dans la norme X.500.

Pour des AC propres à IDnow, le champ Common Name du DN est choisi de manière :

- A correspondre aux usages prévus des certificats émis par l'AC.
- A être unique.

3.1.6. Identification, authentification et rôle des marques déposées

L'AC décide du nom inscrit dans les certificats d'AC Filles sur la base des règles présentées au § 3.1.2 lors de l'enregistrement de la demande.

Toute demande de changement de nom de certificat d'AC Fille se gère via une révocation de certificat suivie d'une nouvelle demande.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

Les clés privées des AC Filles sont générées à l'occasion d'une Key Ceremony sous le contrôle du maître de cérémonie et des témoins.

Les conditions de génération des clés privées sont décrites dans les procédures de Key Ceremony (documents PKI_KC_SCRIPT), qui donnent lieu à des procès-verbaux (documents PKI_KC_PV).

Le déroulement de la Key Ceremony comporte notamment les étapes suivantes :

- Génération des clés privées des AC Filles dans des modules cryptographiques.
- Création des demandes de certificat au format PKCS#10 et transmission à l'AC Racine.
- Vérification par l'AC Racine de la validité cryptographique de la signature des demandes de certificat.

3.2.2. Validation de l'identité d'un organisme

Cf § 3.2.3.

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un Responsable d'AC sans MC pour un certificat d'AC Fille à émettre

L'enregistrement des demandes de certificat a lieu à l'occasion des procédures de Key Ceremony.

Pendant la Key Ceremony, l'identité du Responsable d'AC est validée en face-à-face par le maître de cérémonie en présence des témoins, et sur présentation d'un justificatif d'identité (carte nationale d'identité, permis de conduire, titre de séjour).

Le maître de cérémonie s'assure de l'organisation d'appartenance du responsable d'AC. La présentation d'un justificatif d'appartenance à l'organisation (type contrat de travail) n'est pas obligatoire, s'agissant de personnel interne (déjà vérifié dans le cadre du processus de recrutement).

3.2.3.2. Enregistrement d'un nouveau Responsable d'AC sans MC pour un certificat d'AC Fille déjà émis

Un certificat d'AC Fille doit toujours être placé sous la responsabilité d'un Responsable d'AC faisant partie en interne de l'organisation mentionnée dans le DN du certificat.

Le Responsable d'AC a l'obligation de signaler la fin de ses fonctions de responsable d'AC à l'AE. Si aucun nouveau responsable d'AC n'est désigné pour ce certificat, le certificat doit être **révoqué** (voir § 4.9.1).

En cas de changement de Responsable d'AC, l'AE procède à :

- La **validation de l'identité** du nouveau responsable d'AC par face-à-face, et sur présentation d'un justificatif d'identité.
- La **validation de l'organisation** du nouveau responsable d'AC : il doit faire partie du personnel interne d'IDnow. Il doit être nommé dans le cadre de la nomination des rôles de confiance de la PKI (voir § 5.2.1) et selon une procédure d'habilitation (voir § 5.2.3).

3.2.3.3. Enregistrement d'un Mandataire de Certification

Sans objet.

3.2.3.4. Enregistrement d'un Responsable d'AC via un MC pour un certificat d'AC Fille à émettre

Sans objet.

3.2.3.5. Enregistrement d'un nouveau Responsable d'AC via un MC pour un certificat d'AC Fille déjà émis

Sans objet.

3.2.4. Informations non vérifiées du Responsable d'AC

Sans objet.

3.2.5. Validation de l'autorité du demandeur

Le demandeur d'un certificat d'AC Fille doit être une personne dûment habilitée, à savoir le responsable d'AC.

Le responsable d'AC doit avoir été nommé dans le cadre de la nomination des rôles de confiance de la PKI (voir § 5.2.1).

L'organisation de la Key Ceremony pour la création d'une AC Fille doit être validée par le responsable d'AC.

3.2.6. Certification croisée d'AC

Sans objet.

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

Un renouvellement de bi-clé entraîne nécessairement le renouvellement du certificat correspondant. Réciproquement, un nouveau certificat ne peut pas être délivré sans renouvellement de la bi-clé correspondante.

Voir § 4.6 et § 4.7.

3.3.1. Identification et validation pour un renouvellement courant

Se déroule comme pour la demande initiale (voir § 3.2).

3.3.2. Identification et validation pour un renouvellement après révocation

Se déroule comme pour la demande initiale (voir § 3.2).

3.4. Identification et validation d'une demande de révocation

L'identification et la validation de la demande de révocation nécessitent un face-à-face entre le demandeur et l'AE, avec présentation d'un justificatif d'identité (carte nationale d'identité, permis de conduire, titre de séjour).

L'AE vérifie que le demandeur fait partie de la liste des acteurs autorisés à faire une demande de révocation (voir § 4.9.2).

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Une demande de certificat d'AC Fille doit émaner du Responsable de l'AC Fille dûment nommé (voir § 5.2.1 et § 5.2.3).

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

La demande de certificat d'AC Fille, comportant le nom de l'AC Fille, est enregistrée dans les documents de Key Ceremony (script et PV de KC), après validation par le Responsable d'AC.

La génération de la bi-clé et de la CSR de l'AC Fille a lieu dans un module cryptographique sous le contrôle du maître de cérémonie et en présence des témoins.

Le maître de cérémonie récupère cette CSR pour la transmettre de manière sécurisée à l'AC Racine.

4.2. Traitement d'une demande de certificat

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

Voir § 3.2 pour la validation des informations d'identité et d'organisation.

S'agissant du responsable d'AC, le RC est déjà responsabilisé quant aux modalités d'utilisation du certificat.

Les opérations d'identification et de validation de la demande sont tracées dans les documents de Key Ceremony qui seront ensuite archivés (voir § 5.5).

4.2.2. Acceptation ou rejet de la demande

La demande peut être rejetée uniquement du fait d'un problème technique. Cela est tracé dans les documents de Key Ceremony. Etant présent à la Key Ceremony, le Responsable d'AC en est informé.

4.2.3. Durée d'établissement du certificat

La demande de certificat est traitée dans le cadre d'une Key Ceremony, suite à la planification par le Responsable d'AC de la création d'une nouvelle AC Fille.

4.3. Délivrance du certificat

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

Afin de traiter la demande de certificat, l'AC Racine effectue les actions suivantes :

- Vérification de la **validité cryptographique de la signature** de la CSR.
- **Génération d'un certificat et signature** par l'AC Racine.

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

La remise du certificat se fait en mains propres dans le cadre de la Key Ceremony à laquelle le Responsable d'AC participe.

Les documents de Key Ceremony sont tenus à disposition du Responsable d'AC Fille.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat a lieu durant la Key Ceremony. Le Procès-Verbal de KC (PKI_ENR_KC_PV) comporte l'acceptation explicite du certificat signée par le Responsable d'AC.

Les documents de Key Ceremony sont archivés par l'AC (voir § 5.5).

4.4.2. Publication du certificat

Le certificat d'AC Fille est publié sur le site de de publication de l'AC Racine (voir § 2).

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

Sans objet.

4.5. Usage de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le Responsable d'AC

Le Responsable d'AC Racine s'assure du bon usage qui est fait des certificats d'AC Filles, conformément à leur usage prévu (voir § 1.5).

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

Les utilisateurs de certificat doivent respecter les usages autorisés, décrits au § 1.5).

4.6. Renouvellement d'un certificat d'AC Racine ou Fille

Le renouvellement d'un certificat d'AC Racine ou Fille sans changement de bi-clé tel que défini dans la RFC 3647 n'est pas autorisé dans le cadre de cette PC.

4.7. Délivrance d'un nouveau certificat Racine ou Fille suite à changement de la bi-clé

Ce paragraphe traite du renouvellement de certificat d'AC Racine ou Fille avec changement de bi-clé.

4.7.1. Causes possibles de changement de bi-clé

Deux causes possibles pour le changement de bi-clé et le renouvellement du certificat :

- Expiration du certificat d'AC Racine ou Fille.
- Révocation d'un certificat d'AC Racine ou Fille.

4.7.2. Origine d'une demande de nouveau certificat

Cf. demande initiale : voir § 4.1.

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

Cf. § 4.2.

4.7.4. Notification au RC de l'établissement du nouveau certificat

Cf. § 4.3.2.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. § 4.4.1.

4.7.6. Publication du nouveau certificat

Cf. § 4.4.2.

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

Sans objet.

4.8. Modification du certificat

Les modifications de certificats au sens de la RFC 3647 ne sont pas autorisées.

4.9. Révocation et Suspension des certificats

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats d'AC Filles ou Racine

Les **causes possibles d'une révocation de certificat d'AC Fille** sont les suivantes :

- **Suspicion de compromission, compromission, perte ou vol de la clé privée** de l'AC.
- Décision de **changement dans l'AC** suite à la **détection d'une non-conformité des règles ou procédures de l'AC** avec celles annoncées dans la PC ou la DPC.
- **Détection d'une erreur** dans les documents de **Key Ceremony**.
- **Demande de révocation par une personne autorisée** (voir § 4.9.2).
- **Cessation d'activité** de l'AC.

La réalisation de l'une de ces causes de révocation doit être portée à la connaissance du responsable d'AC qui prend les mesures nécessaires pour traiter la révocation au plus vite.

4.9.1.2. Certificats d'une composante de l'IGC

Les causes possibles d'une révocation d'une composante de l'IGC (§ 1.5.1.2) sont les suivantes :

- **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.
- **Cessation d'activité** de l'entité opérant la composante.

La réalisation de l'une de ces causes de révocation doit être portée à la connaissance de l'AE correspondant à l'AC émettrice du certificat concerné par la révocation. Cette AE prend les mesures nécessaires pour traiter la révocation au plus vite.

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats d'AC Fille ou Racine

Seul le **responsable de l'AC** est autorisé à demander la **révocation d'un certificat d'AC**.

De manière exceptionnelle, dans le cas d'une décision de justice, les autorités judiciaires peuvent demander la révocation d'un certificat d'AC.

4.9.2.2. Certificats d'une des composantes de l'IGC

La révocation des certificats de **composantes de l'IGC** est décidée, conformément à la Politique de Certification correspondante, par l'entité opérant la composante, qui doit en informer le **Responsable de l'AC** dans les meilleurs délais.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat d'AC Fille ou Racine

La révocation d'un certificat d'AC Fille ou Racine se déroule à l'occasion d'une Key Ceremony.

Sous le contrôle du maître de cérémonie, et en présence du responsable de l'AC Fille et des témoins, **le certificat d'AC est révoqué**, et **l'ARL est mise à jour puis publiée. La clé privée de l'AC est détruite** au sein du module cryptographique. Les anciennes sauvegardes des modules cryptographiques sont archivées.

Les certificats émis par l'AC Fille révoquée devront ensuite être révoqués. Les impacts pour les utilisateurs sont anticipés par le Responsable d'AC qui se charge de mener les actions nécessaires (création d'un nouveau certificat d'AC et des certificats d'entité finale).

Les actions réalisées en Key Ceremony sont tracées dans les documents de KC qui sont ensuite archivés. Le Procès-Verbal de KC précise le nom exact du certificat révoqué (DN du sujet, numéro de série), et comporte la signature du Responsable de l'AC Fille.

Le demandeur de la révocation (voir § 4.9.2) est informé de la révocation effective du certificat.

Le point de contact de l'ANSSI est informé de la révocation d'un certificat d'AC Fille.

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

La révocation d'un **certificat d'une composante de l'IGC** est **réalisée par l'AE** en charge du certificat concerné, sur demande de la personne autorisée (voir § 4.9.2.2).

Ces événements sont enregistrés dans les journaux d'événements de l'IGC.

En cas de révocation d'un certificat d'une AC émettrice des certificats des composantes de l'IGC, le responsable de cette AC informe tous les Responsables de Certificats concernés dans les meilleurs délais, et si possible par anticipation.

4.9.4. Délai accordé au RCC pour formuler la demande de révocation

Le Responsable d'AC planifie sans délai une nouvelle Key Ceremony, dès connaissance d'une cause possible de révocation.

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

4.9.5.1. Révocation d'un certificat d'AC

La révocation d'un certificat d'AC doit être effectuée dans les plus brefs délais, notamment en cas de compromission de clé.

4.9.5.2. Disponibilité du système de traitement des demandes de révocation

L'AC Racine est mise offline pour des questions de sécurité. Dans ce cadre la **fonction de gestion des révocations est disponible uniquement quand l'AC Racine est mise en ligne**, dans le cas d'opérations de Key Ceremony.

La **prise en compte des demandes de révocation** d'un certificat d'AC est faite par le Responsable d'AC **dans un délai maximum de 24 heures ouvrées**. Des investigations sont menées afin de s'assurer du motif de la révocation, et de valider l'organisation d'une Key Ceremony afin de procéder à la révocation.

Le **traitement d'une demande de révocation d'un certificat d'AC** est faite dans un délai de 7 jours à compter de la prise en compte de la demande.

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

La révocation d'un certificat d'une composante (entité finale ou AC) doit être effectuée dès la détection de l'évènement décrit dans les causes de révocations, selon les modalités prévues dans la PC de l'AC

émettrice de ce certificat.

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat d'AC est tenu de vérifier, avant son utilisation, l'état des certificats.

Pour cela, l'AC publie des Listes de Autorités Révoquées (LAR, ou ARL).

4.9.7. Fréquence d'établissement des ARL

L'AC Racine établit des **nouvelles ARL au moins tous les ans** (a minima dans le mois précédent son expiration).

Chaque ARL est valable un an.

4.9.8. Délai maximum de publication d'une ARL

Les ARL sont **publiées au maximum 30 minutes après la génération.**

4.9.9. Exigences sur la vérification en ligne de la révocation et l'état des certificats

Aucun service OCSP n'est mis en œuvre.

4.9.10. Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.11. Exigences spécifiques en cas de compromission de la clé privée

Une compromission de clé privée est une cause de révocation, et doit être traitée comme telle dans les meilleurs délais (voir § 4.9.3).

En cas de compromission d'une clé privée d'AC, l'information est diffusée sur le site de publication de l'AC.

La révocation du certificat d'AC Fille entraîne l'arrêt de l'utilisation de la clé privée correspondante. La clé privée de l'AC Fille révoquée est supprimée immédiatement après révocation du certificat d'AC Fille (voir § 4.9.3.1).

4.9.12. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée.

4.9.13. Origine d'une demande de suspension

Sans objet.

4.9.14. Procédure de traitement d'une demande de suspension

Sans objet.

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

Sans objet.

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

L'AC Racine met les ARL à disposition de tous les utilisateurs via son site de publication.

Les ARL sont au format V2. Elles sont accessibles via le protocole http.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures / 24 et 7 jours / 7.

Sa **durée maximale d'indisponibilité par interruption de service** (panne ou maintenance) est de **4 heures les jours ouvrés**.

Sa durée **maximale totale d'indisponibilité par mois** est de **32 heures les jours ouvrés**.

4.10.3. Dispositifs optionnels

Sans objet.

4.11. Fin de la relation entre le RC et l'AC

Dans le cas où il n'existe plus de Responsable d'AC explicitement identifié pour un certificat d'AC, le certificat doit être révoqué.

4.12. Séquestre de clé et recouvrement

Le séquestre de clé privée est interdit.

4.12.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet.

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

Sans objet.

5. Mesures de sécurité non techniques

5.1. Mesures de sécurité physique

Les sites d'hébergement de l'IGC sont décrits dans la DPC. Ils contiennent l'ensemble des ressources matérielles de l'IGC, serveurs, supports de stockage de données, équipements réseau, mais aussi les postes de travail utilisés par les administrateurs IDnow SAS et le personnel de l'AE.

5.1.1. Situation géographique et construction des sites

La situation géographique des sites d'hébergement de l'IGC permet d'écarter les menaces suivantes :

- Menace climatique (tornade, canicule…).
- Menace naturelle (crue, feu de forêt, tremblement de terre…).
- Menace environnementale (industrie chimique / nucléaire…).

5.1.2. Accès physique

L'accès aux sites d'hébergement de l'IGC est contrôlé. Seules les personnes autorisées nominativement peuvent accéder aux sites d'hébergement de l'IGC. La traçabilité des accès est assurée. En-dehors des heures ouvrables, des moyens de détection d'intrusion physique et logique sont mis en œuvre au niveau des sites d'hébergement.

L'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les machines des composantes de l'IGC sont situées dans un périmètre physique dédié, permettant de respecter la séparation des rôles de confiance telle que prévue au § 5.2.4.

5.1.3. Alimentation électrique et climatisation

Les sites d'hébergement de l'IGC disposent d'une alimentation électrique dimensionnée par rapport aux besoins, hautement disponible et secourue.

Les sites d'hébergement de l'IGC disposent d'une climatisation dimensionnée par rapport aux besoins, hautement disponible et secourue.

5.1.4. Vulnérabilité aux dégâts des eaux

Les sites d'hébergement de l'IGC disposent de moyens de détection et de protection contre les dégâts des eaux, permettant d'assurer la continuité de fonctionnement de l'IGC, conformément aux objectifs de disponibilité des fonctions de l'AC.

5.1.5. Prévention et protection incendie

Les sites d'hébergement de l'IGC disposent de moyens de détection et de protection contre les incendies, permettant d'assurer la continuité de fonctionnement de l'IGC, conformément aux objectifs de disponibilité des fonctions de l'AC.

5.1.6. Conservation des supports

L'AC maintient à jour l'inventaire et la classification des données de l'IGC et de leurs supports de stockage.

L'AC met en place les mesures de protection des données adaptées selon leur place dans la classification.

Des procédures de sécurité définissent les conditions de manipulation des différents supports de manière à éviter les dommages, la perte et le vol.

L'AC s'engage à gérer les problématiques d'obsolescence et de détérioration des supports, de manière à assurer la pérennité des données.

5.1.7. Mise hors service des supports

L'AC gère la fin de vie des supports, de manière à garantir la stricte confidentialité des données qu'ils ont portées.

5.1.8. Sauvegarde hors site

L'AC sauvegarde l'intégralité des données de l'IGC.

En complément des sauvegardes sur les sites d'hébergement, des sauvegardes hors site sont mises en œuvre, de manière à prévenir le risque de perte de données suite à des dommages matériels.

L'AC est capable de restaurer les sauvegardes de manière à retrouver les données dans l'état où elles étaient au plus tard 8 heures avant la panne.

Les délais d'intervention et de traitement en cas d'incident permettent de respecter les objectifs de disponibilité des fonctions de l'AC.

Les supports de sauvegarde sont protégés en confidentialité et en intégrité.

Les fonctions de sauvegarde et de restauration sont effectuées par des personnes disposant de rôles de confiance (tels que définis au § 5.2.1) selon des procédures définies.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

L'IGC comporte les rôles de confiance suivants :

- **Responsable de sécurité** : Il est chargé de la mise en œuvre et du contrôle de la politique de sécurité applicable aux composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de l'IGC. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats.
- **Responsable d'application** : Il est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la Politique de Certification et de la Déclaration des Pratiques de Certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application 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 la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise dans le cadre de ses attributions, l'exploitation au quotidien des applications pour les fonctions mises en œuvre par la composante.
- **Opérateur d'enregistrement** : Il réalise toutes les fonctions relevant de l'Autorité d'Enregistrement (voir § 1.4.2).
- **Contrôleur** : Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Porteur de secret** : Il détient une carte d'administration permettant d'exécuter des fonctions critiques sur les modules cryptographiques. Le porteur de secret est responsable de la protection de sa part de secret, en confidentialité et en intégrité. Les différents rôles de porteurs de secret sont détaillés dans la DPC.
- **Responsable des journaux d'événements**: Il est en charge de la protection de l'intégrité et de la confidentialité des journaux d'événements.

5.2.2. Nombre de personnes requises par tâche

Le nombre de personnes requises par tâches est précisé dans la DPC.

5.2.3. Identification et authentification pour chaque rôle

Les rôles de confiance sont attribués conformément à un processus d'habilitation comportant une validation par un responsable hiérarchique.

Chaque porteur de rôle de confiance signe un **formulaire d'autorisation** daté comportant le descriptif des activités relatives au rôle de confiance, et des engagements associés.

L'affectation d'un rôle de confiance à une personne amène le positionnement de droits d'accès (physiques et logiques) au niveau des composants techniques de l'IGC.

Tout accès à l'un des composants techniques de l'IGC est soumis à **authentification** et au **contrôle des droits d'accès**.

La DPC précise les moyens utilisés.

Les contrôles de conformité (voir § 8) portent notamment sur le positionnement des droits d'accès conformément aux rôles de confiance.

5.2.4. Rôles exigeant une séparation des attributions

Les rôles de confiance peuvent être **cumulés** par une même personne pour des questions d'optimisation de la charge de travail. Toutefois, la **règle de non-cumul** suivante s'applique :

- Le rôle de responsable de sécurité ne peut être cumulé avec le rôle d'ingénieur système.

5.3. Mesures de sécurité vis à vis du personnel

5.3.1. Qualifications, compétences, et habilitations requises

Tout le personnel de l'IGC est soumis à une clause de confidentialité.

Le personnel de l'IGC est spécialisé dans le développement et la mise en œuvre d'infrastructures de sécurité. Le personnel d'encadrement dispose de l'expertise appropriée à son rôle.

Les rôles de confiance et leurs attributions respectives sont décrits dans les formulaires d'autorisation mentionnés au § 5.2.3, et que les porteurs de rôle approuvent par signature lors de leur nomination.

Les procédures de sécurité sont accessibles par tout le personnel de l'IGC.

5.3.2. Procédures de vérification des antécédents

L'AC s'assure de l'honnêteté de son personnel au moment du recrutement, et dans le cadre de la gestion des ressources humaines. En particulier, le personnel ne doit pas avoir de condamnation en justice en contradiction avec leurs attributions.

La présence d'éventuels conflits d'intérêts est vérifiée au moment de l'affectation des rôles de confiance, et revue régulièrement, au minimum tous les 3 ans.

5.3.3. Exigences en matière de formation initiale

Le recrutement du personnel de l'IGC permet de vérifier que chacun dispose de la formation initiale adéquate à la réalisation de ses fonctions.

5.3.4. Exigences et fréquence en matière de formation continue

Les évolutions des exigences de sécurité, ainsi que les évolutions techniques sont documentées et diffusées au sein du personnel de l'IGC.

L'affectation d'un nouveau rôle de confiance à une personne peut donner lieu à une formation selon les besoins.

5.3.5. Fréquence et séquence de rotations entre différentes attributions

Sans objet.

5.3.6. Sanctions en cas d'actions non autorisées

Voir la DPC.

5.3.7. Exigences vis à vis du personnel des prestataires externes

En cas de pic de charge, le personnel de l'IGC peut être renforcé par un ou des prestataires externes.

Ce renfort ne concerne que le rôle de confiance **Ingénieur système**, à l'exclusion de tous les autres rôles de confiance qui sont dévolus à des salariés de l'IGC.

Les exigences vis-à-vis des prestataires externes sont les mêmes que celles des salariés de l'IGC, exceptées les sanctions disciplinaires, qui sont du ressort de l'employeur, l'IGC procédant pour sa part à la fin immédiate du contrat de prestation en cas de manquement aux obligations.

5.3.8. Documentation fournie au personnel

L'IGC met à disposition de l'ensemble de son personnel la documentation fonctionnelle, opérationnelle et technique concernant l'IGC.

En particulier les PC et DPC sont diffusées au personnel de l'IGC.

5.4. Procédures de constitution des données d'audit

5.4.1. Type d'événement à enregistrer

Une politique de traçabilité est définie et tenue à jour par l'AC.

Elle liste les événements à journaliser. Cela comprend notamment :

- Création / modification / suppression de comptes utilisateurs et des données d'authentification associées.
- Démarrage et arrêt des systèmes.
- Evénements liés à la journalisation.
- Connexion/déconnexion des utilisateurs.
- Accès physiques.
- Actions de maintenance et de changement de configuration.
- Actions de gestion des supports matériels de données.
- Evénements métiers de l'IGC.

La politique de traçabilité liste les informations à enregistrer pour chaque type d'événement journalisé. Cela comprend notamment le type d'événement, le nom de l'exécutant, la date et l'heure, le résultat de l'événement.

Les événements journalisés sont enregistrés au cours des processus, ou pour les enregistrements manuels, dans la journée de l'événement.

Le système de journalisation est automatique dès le démarrage du système, et sans interruption jusqu'à l'interruption du système.

5.4.2. Fréquence de traitement des journaux d'événements

La politique de traçabilité de l'AC spécifie le type de contrôles réalisés sur la base des journaux d'événements. Ces contrôles sont réalisés une fois par jour ouvré de la manière suivante :

- **Les journaux sont analysés en totalité une fois par jour ouvré, et dès la détection d'une anomalie**. Cette analyse permet d'identifier des anomalies liées à des tentatives en échec. Elle donne lieu à un compte-rendu.
- Un **rapprochement entre les journaux d'événements** est effectué **une fois toutes les 2 semaines**.

5.4.3. Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins 1 mois.

Ils sont archivés sous un délai de 1 mois dans un lieu géographiquement distant du lieu de production.

5.4.4. Protection des journaux d'événements

La PSSI d'IDnow SAS définit les exigences de protection des journaux d'événements, en termes d'intégrité, de disponibilité et de confidentialité.

Le système de datation des journaux d'événements respecte les exigences du § 6.8.

5.4.5. Procédure de sauvegarde des journaux d'événements

La PSSI d'IDnow SAS impose la sauvegarde des journaux d'événements.

5.4.6. Système de collecte des journaux d'événements

Les logs des différents composants de l'IGC sont centralisés sur un serveur de logs. Cependant, la racine de l'IGC étant offline, ces logs sont limités sur l'équipement de gestion de l'AC Racine.

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

Il n'y a pas de notification en cas d'enregistrement d'un événement.

5.4.8. Evaluation des vulnérabilités

Cf § 5.4.2.

5.5. Archivage des données

5.5.1. Types de données à archiver

L'AC a défini une politique d'archivage. Celle-ci définit les données à archiver, au format numérique et papier. Elles comprennent notamment :

- Les logiciels de l'IGC.
- La documentation fonctionnelle de l'AC, dont PC, DPC, CGU.
- Les accords contractuels avec d'autres AC.
- Les certificats et LCR tels qu'émis ou publiés.
- Les notifications.
- Les dossiers d'enregistrement, incluant les formulaires de demande, les CGU signées, les justificatifs d'identité des demandeurs et, le cas échéant, de leur entité de rattachement.
- Les journaux d'évènements.

5.5.2. Période de conservation des archives

Par défaut, les archives sont conservées pendant 7 ans.

- C'est le cas notamment des dossiers d'enregistrement.
- Les journaux d'événements sont archivés pendant 7 ans à compter de leur génération.

Les certificats et CRL sont archivés pendant 5 ans après leur arrivée à expiration.

La politique d'archivage définit le processus de gestion des demandes d'accès aux archives.

La DPC précise les moyens mis en œuvre pour l'archivage.

5.5.3. Protection des archives

La politique d'archivage définit les exigences de protection des archives, en intégrité, en disponibilité, en pérennité et en lisibilité. Elle définit qui a accès aux archives.

La DPC décrit les moyens de protection des archives.

5.5.4. Procédure de sauvegarde des archives

Les archives sont conservées de manière à en assurer la disponibilité au cours du temps.

5.5.5. Exigences d'horodatage des données

Les archives nécessitant une date (journaux d'événements) respectent les exigences du § 6.8.

5.5.6. Système de collecte des archives

Le système de collecte des archives respecte les exigences de protection des archives.

5.5.7. Procédure de récupération et de vérification des archives

Le processus de gestion des demandes d'accès aux archives décrit dans la politique d'archivage garantit qu'une archive peut être récupérée dans un délai inférieur à 2 jours ouvrés.

La politique d'archivage définit qui est autorisé à accéder aux archives.

5.6. Changement de clés d'AC

La durée de vie du certificat de l'AC Racine est de 11 ans.

La durée de vie des certificats émis d'AC Filles est de 10 ans.

Afin de permettre aux utilisateurs de vérifier l'origine des certificats, à tout moment de la vie du certificat, les certificats d'AC Filles ne sont pas renouvelés avec l'ancienne AC Racine, mais dans le cadre de la mise en place d'une nouvelle hiérarchie d'AC, dépendant d'une nouvelle AC Racine.

La nouvelle hiérarchie a déjà été créée et cela forme la 3ème génération d'AC (G3). La nouvelle AC Racine se nomme **ARIADNEXT Root CA G3**.

Après création du nouveau certificat d'AC Racine :

- L'ancienne bi-clé continuera d'être utilisée uniquement pour signer les ARL jusqu'à expiration du dernier certificat d'AC Fille.
- La nouvelle bi-clé sera utilisée pour signer les nouveaux certificats d'AC Fille.

Remarque: les modalités d'utilisation des certificats d'AC Filles après renouvellement sont précisées dans leurs PC respectives.

5.7. Reprise suite à compromission et sinistre

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

L'AC dispose d'une **organisation de gestion des incidents**.

Les incidents sont détectés au travers d'un système de supervision et d'alertes, ainsi que sur la base de l'analyse des journaux d'événements.

La perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, constituent un incident majeur pour l'AC.

Le cas de l'incident majeur est traité dès détection, selon la **procédure de gestion des incidents de sécurité**.

La publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (site Internet, presse etc.). L'AC prévient directement et sans délai l'ANSSI, via le point de contact identifié sur le site : https://www.ssi.gouv.fr.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC Racine ou les AC Filles devient insuffisant pour son utilisation prévue restante, alors l'AC Racine réalise les actions suivantes :

- Informer tous les responsables d'AC et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats.
- Révoquer tout certificat concerné.

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

L'AC dispose d'un **Plan de Continuité d'Activité** (PCA).

Ce Plan se base sur l'étude des besoins de continuité d'activité de l'AC, et des risques d'atteinte à la continuité, pour définir les mesures adaptées. Il répond à deux objectifs : gérer les incidents portant atteinte à la continuité de l'établissement, et prévenir ces incidents.

Le PCA adresse en particulier la problématique de la reprise d'activité, suite à la corruption des ressources informatiques.

Le PCA est testé tous les 2 ans.

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

Le cas de compromission de la clé privée d'une composante de l'IGC fait partie des sinistres traités par le PCA.

Le cas de compromission d'une clé d'AC amène sa révocation (voir § 4.9.1.2).

De plus, l'AC informe de la compromission tous les responsables de certificats et les entités avec lesquelles elle a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information est mise à disposition des autres tiers utilisateurs.

L'AC indique que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

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

Voir la DPC.

5.8. Fin de vie de l'IGC

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

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

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

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

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

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC a pris les dispositions suivantes :

- Mise en place de procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats et des informations relatives aux certificats).
- Mesures pour assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication du certificat d'AC et des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente Politique de Certification.

De plus, les engagements suivants sont pris par l'AC :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des clients ou des utilisateurs de certificats, l'AC les en avisera aussitôt que nécessaire et, au moins, sous le délai d'un mois.
- Le cas échéant, l'AC définira 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 communiquera le plan d'action au point de contact identifié sur https://www.ssi.gouv.fr ainsi qu'à l'organisme en charge de la qualification de l'AC.
  - 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 communiquera à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus.
  - L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement.
  - Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.
- Le cas échéant, l'AC tiendra informés l'ANSSI, l'organisme certificateur et ses clients et utilisateurs de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

Seule l'activité de l'AE pourra, pour des raisons organisationnelles et/ou économiques, être transférée à un tiers. La partie technique de cette activité restera sous contrôle d'IDnow SAS. A ce titre, aucun transfert des données archivées ne sera fait dans le cadre d'un tel transfert d'activité.

L'AC n'est pas transférable à un tiers. Si IDnow SAS venait à décider la cessation de son IGP, alors ce sont les modalités précisées au § 5.8.2 qui s'appliqueraient.

A l'échéance d'une AC (et en respectant les délais de manière à ce qu'aucun certificat ne puisse être émis avec une durée de validité inférieure à celle précisée dans les PC) et si IDnow SAS maintient son activité de PSCE, la ou les activités portées par cette AC seront transférées vers une nouvelle AC sous responsabilité exclusive d'IDnow SAS. Ce transfert ne concerne que les activités et les clients de celles-ci. La création de la nouvelle AC se fait dans le respect des politiques et pratiques définies pour l'AC qu'elle remplace. Dans ce contexte, l'AC en fin de vie reste en place jusqu'à l'échéance du dernier certificat émis, et les données archivées restent accessibles pendant la durée définie dans la PC et les CGU.

5.8.2. Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement).

La cessation partielle d'activité sera progressive de telle sorte que l'AC, ou une entité tierce soit capable de reprendre les activités.

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

En cas de cessation de service, l'AC prendra les dispositions suivantes :

- La notification des entités affectées ;
- L'arrêt d'émission de nouveaux certificats ;
- L'accompagnement des clients vers une ou des nouvelles AC de niveaux de sécurité, de qualification et de services équivalents ;
- Le maintien des engagements définis dans les CGU (notamment les services de révocation) jusqu'à la fin de vie du dernier certificat émis.

Lors de l'arrêt du service :

- L'AC s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats.
- L'AC prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante. Cela concerne la clé privée ainsi que les sauvegardes réalisées.
- L'AC révoque son certificat.
- L'AC révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité.
- L'AC informe les responsables d'AC des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6. Mesures de sécurité techniques

6.1. Génération et installation des bi clés

6.1.1. Génération des bi clés

6.1.1.1. Clés d'AC Racine

La génération de la clé de signature d'AC Racine est effectuée dans un environnement sécurisé, permettant notamment de :

- Protéger le matériel contre les rayonnements parasites.
- Limiter les fuites d'information par observation visuelle ou rayonnements électromagnétiques.

La génération de la clé de signature de l'AC Racine est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (voir § 5.2.1), dans le cadre d'une **« Cérémonie de Clés » (Key Ceremony)**.

La cérémonie de clés se déroule suivant un script préalablement défini, **sous le contrôle d'au moins deux personnes ayant un rôle de confiance, et en présence de plusieurs témoins, dont au moins deux sont externes à l'AC**. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

La clé de signature de l'AC Racine est générée et mise en œuvre dans un module cryptographique qualifié au niveau renforcé, conformément aux exigences du RGS***. **Ce module cryptographique est placé offline dans un endroit sécurisé en-dehors des opérations de Key Ceremony.**

La génération de la clé de signature de l'AC Racine nécessite au préalable la génération de parts de secrets de l'AC Racine. La réunion du quorum des porteurs de parts de secrets permettra ainsi de restaurer la bi-clé de l'AC Racine sur un nouveau module cryptographique.

Chaque part de secret est remise de manière sécurisée à un **porteur de secret**, qui ne peut en détenir deux pour une même AC. Le changement de porteur de part de secret est possible (notamment suite au changement d'activité d'un porteur de part de secret).

6.1.1.2. Clés d'AC Filles générées par l'AC

Sans objet.

6.1.1.3. Clés d'AC Filles générées au niveau des AC Filles

La clé de signature de l'AC Fille est générée et mise en œuvre dans un module cryptographique qualifié au niveau renforcé conformément aux exigences du RGS*** (répondant a fortiori aussi aux exigences du RGS* selon les AC Filles).

Le Responsable d'AC Fille s'engage auprès du Responsable d'AC Racine à utiliser un module cryptographique qualifié au niveau requis par la PC de l'AC Fille.

6.1.2. Transmission de la clé privée à l'AC Fille

Sans objet.

6.1.3. Transmission de la clé publique à l'AC Racine

La transmission de la clé publique de l'AC Fille vers l'AC Racine doit permettre :

- La protection de l'intégrité de la clé.
- La vérification de l'origine de la transmission.

Elle a lieu dans un environnement sécurisé pendant la Key Ceremony.

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

La clé publique de l'AC Racine est publiée sur le site de publication (voir § 2.2).

De plus, l'AC Racine publie l'empreinte de son certificat, de manière à ce que les utilisateurs puissent la comparer avec celle inscrite dans le certificat.

6.1.5. Tailles des clés

Les tailles de clés autorisées dans le cadre de cette PC sont de 4096 bits pour les AC Racine et Filles.

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

Les équipements de génération des bi-clés utilisent des paramètres respectant les normes de sécurité propres aux algorithmes correspondant aux bi-clés.

Les algorithmes utilisés pour la signature des certificats d'AC Filles sont les suivants :

- Algorithme d'empreinte : SHA-512
- Algorithme de signature : RSA

Voir le § 7 pour les profils de certificats.

6.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée d'AC Racine est limitée à la signature de certificats et d'ARL.

L'utilisation d'une clé privée d'AC Fille est limitée à la signature de certificats et de CRL.

Voir le § 7 pour les profils de certificats.

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Module cryptographique de l'AC Racine

La bi-clé d'AC Racine est générée et conservée dans un module cryptographique qualifié comme indiqué au § 6.1.1.1.

6.2.1.2. Dispositifs de protection des clés privées des AC Filles

Voir § 6.1.1.3.

6.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle de la clé privée de signature de l'AC Racine est assuré par des porteurs de parts de secret, comme décrit au § 6.1.1.1.

Le quorum des parts de secrets nécessaire à la restauration de la clé privée sur un module cryptographique est fixé par l'AC Racine à 3 sur 5.

Les porteurs de secrets sont des porteurs de rôle de confiance (voir § 5.2.1).

6.2.3. Séquestre de la clé privée

Le séquestre de clé privée n'est pas autorisé dans cette PC.

6.2.4. Copie de secours de la clé privée

Les clés privées de l'AC Racine et des AC Filles font l'objet de copies de secours.

Ces copies de secours sont effectuées hors du module cryptographique. Elles sont protégées en confidentialité et en intégrité. Le mécanisme de chiffrement utilisé permet de résister aux attaques par cryptanalyse.

Les opérations de chiffrement et déchiffrement des clés privées d'AC sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

Le contrôle des opérations de chiffrement/déchiffrement est conforme aux exigences du § 6.2.2.

6.2.5. Archivage de la clé privée

Les clés privées de l'AC Racine et des AC Filles ne sont pas archivées.

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

Toutes les opérations de génération de clé privée se font dans un module cryptographique.

La mise en œuvre d'une copie de secours dans un module cryptographique respecte les exigences du §

6.2.4.

6.2.7. Stockage de la clé privée dans un module cryptographique

Voir § 6.2.4 et § 6.2.6.

L'AC garantit que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clés privées d'AC Racine

L'activation de la clé privée d'AC Racine dans le module cryptographique est contrôlée par des **données d'activation** (voir § 6.4).

6.2.8.2. Clés privées des AC Filles

Voir PC des AC Filles.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clés privées de l'AC Racine

La désactivation de la clé privée de l'AC dans un module cryptographique est automatique dès que l'environnement du module évolue, notamment en cas d'arrêt ou déconnexion du module, ou en cas d'atteinte à l'intégrité du système.

Les conditions de désactivation de la clé privée de l'AC Racine permettent de répondre aux exigences de la qualification du module cryptographique citée au § 6.1.1.1.

6.2.9.2. Clés privées des AC Filles

Voir PC des AC Filles.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Clés privées d'AC Racine

La méthode de destruction de la clé privée de l'AC Racine permet de répondre aux exigences de la qualification du module cryptographique.

En fin de vie d'une clé privée d'AC Racine, normale ou anticipée (révocation), cette clé est détruite ainsi que ses copies.

6.2.10.2. Clés privées des AC Filles

Voir les PC des AC Filles correspondantes.

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de création de cachet

Voir § 6.1.1.1 et § 6.1.1.3.

6.3. Autres aspects de la gestion des bi clés

6.3.1. Archivage des clés publiques

Les clés publiques d'AC sont archivées dans le cadre de la politique d'archivage (voir § 5.5).

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

Les bi-clés et les certificats des AC Filles ont une durée de vie maximum de 10 ans (voir § 5.6).

L'AC Racine fait en sorte d'être valide pendant toute la durée de validité des AC Filles émises.

Voir le § 5.6 pour les modalités de renouvellement de l'AC Racine et des AC Filles.

6.4. Données 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 Racine

Les **données d'activation** correspondant à la clé privée de l'AC Racine sont générées pendant la phase d'initialisation et de personnalisation du module, **au cours de la Key Ceremony** (voir § 6.1.1.1).

Les données d'activation sont choisies et saisies par les **porteurs de rôle de confiance** correspondants pendant la Key Ceremony.

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée des AC Filles

Voir PC des AC Filles.

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 Racine

Les données d'activation sont conservées de manière à être protégées en confidentialité, intégrité et disponibilité.

Voir DPC.

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

Voir les PC des AC Filles.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

L'AC Racine mène une analyse de risques de manière à identifier les mesures de sécurité applicables sur le périmètre de l'IGC.

Dans le cadre de la gouvernance de la sécurité des SI définie dans la PSSI, la mise en œuvre des mesures de sécurité est contrôlée régulièrement.

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

L'AC définit les 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).
- Eventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (cf. § 1.5.1.2) fait l'objet de mesures particulières, qui peuvent découler de l'analyse de risque.

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

6.5.2. Niveau de qualification des systèmes informatiques

La qualification des systèmes informatiques de l'IGC mettant en œuvre le module cryptographique n'est pas imposée dans le cadre de cette PC.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1. Mesures de sécurité liées au développement des systèmes

L'AC garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

L'AC utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

L'AC documente les éléments suivants :

- L'implémentation des systèmes de l'IGC.
- La configuration des systèmes de l'IGC, ainsi que toute modification.

6.6.2. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC est signalée à l'AC pour validation.

Elle est documentée et apparaît dans les procédures opérationnelles de l'AC.

Dans le cas des produits évalués, l'évolution est conforme au schéma de maintenance de l'assurance de conformité.

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

Aucune exigence n'est posée dans le cadre de cette PC.

6.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de 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 au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

6.8. Horodatage / système de datation

L'AC met en œuvre un système de datation basé sur le protocole NTP.

L'AC garantit une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

Pour les opérations faites hors ligne, cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système permet toutefois d'ordonner les évènements avec une précision suffisante.

7. Profils des certificats, OCSP et des LCR

7.1. Profils des certificats

Les certificats de l'AC et des sous-AC sont conformes au format X.509 V3.

7.1.1. Certificat de l'AC

7.1.1.1. Champs de base

Champ	Valeur
Version	2 pour V3
Numéro de série	<Créé par l'outil> = `0E E8 C9 BC 66 8F 62 B2`
Algorithme de signature	sha512WithRSAEncryption (1.2.840.113549.1.1.13)
DN Émetteur	CN = AriadNEXT Root CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
DN Objet	CN = AriadNEXT Root CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
Valide à partir du	mercredi 20 mai 2015 09:13:15 GMT
Valide jusqu'au	mardi 19 mai 2026 22:00:00 GMT
Algorithme de clé publique	RSAEncryption (1.2.840.113549.1.1.1)

Champ	Valeur
Clé publique	< valeur de la clé publique RSA de 4096 bits > de l'AC = 00 b2 d4 e5 42 d5 68 12 d1 97 7c 16 4e c8 61 d8 fa 04 4e 69 03 76 50 b7 f7 38 34 36 23 fe 3d df 07 8b f5 e9 9a 9a a8 fe a1 6e 79 bf 6a c4 af 61 54 d1 00 a1 f5 25 78 95 f9 16 13 25 45 80 e8 a0 62 73 29 39 fa 1e 64 0a f6 43 00 1d 5e 30 02 92 d6 bb a2 28 e7 c7 6f eb c1 95 90 63 0d 2d 01 b4 9f 90 de c7 f4 af c1 fa 19 35 e0 01 56 fe 9a db 61 3c d2 fe a9 92 99 a1 44 82 06 3a aa cf 18 32 e6 36 94 5e 72 cb a0 a0 ef 9f 45 bd e5 85 20 a2 df 96 cd 2f 0b 3b 66 71 94 ae f3 79 38 6c 2a a3 7b 06 45 4b 7f 1a a6 37 68 d0 4b c4 f2 6f 3e 8b 51 68 2d 0d 39 f7 3f 39 87 6f c9 a3 18 c0 be 60 83 37 ad 9c 12 67 49 07 51 3f 2c 00 66 16 ed 36 98 47 03 39 df 60 7f 78 3d 6d b0 cc 51 89 19 7e 8b 27 26 7c 1e ca 70 bc bf 92 28 b4 45 ff ac d1 bf dd 42 87 48 8c 33 36 fd a0 a8 d6 8b 37 0f 77 fd 4f a6 7f c8 61 a5 d1 c4 82 e4 47 d4 b9 22 78 68 47 92 4c 2a 41 fa 63 8e 10 49 3e b2 cb ef c5 52 c9 ca 31 b3 58 5a c0 b4 bc bb 07 6d f4 00 f4 4e 37 07 f6 d9 57 50 7f 96 9c 59 df bb 19 26 7c 31 88 29 77 11 7d 54 1f c2 a9 d9 36 04 7b 5c ca 24 d6 3f cf 1d 24 c7 35 c8 5e 6a 88 a5 bc 14 ef e7 e3 3b f8 24 9c 55 32 aa 23 9f 9b 1a e7 63 8d e4 1a 47 11 7d e2 ab 87 ac b8 4e 2f b5 bd fc 55 09 9a f2 1d b4 ec 77 57 76 a0 62 37 dd 43 c8 76 50 05 6d 3b 39 06 26 da 07 f2 84 98 dd c7 4c 12 d3 05 28 c2 bc 32 1c 43 47 4b a4 88 6e 6a a9 c7 1f f1 de ff 3c f6 f8 4d 8b 3d e8 a4 8d ab 64 9f 0f a5 5b 8f 10 e8 30 9d b2 3c 78 f5 d9 57 f4 18 50 be 53 e1 1a e8 b2 27 ed 5b 00 51 24 e6 96 3a df 66 72 a0 2e fe 4c a6 14 b8 24 b4 1a 89 97 62 c5 6c 15 d7 11 17 19 6c 41 4d 0b c4 9c df 36 84 a3

7.1.1.2. Extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé de l'autorité	O	N	<valeur de hachage> = 72 86 1A 03 F4 14 9F AF FD 1F 41 A5 22 B8 B2 20 E3 86 19 73
Identificateur de la clé du sujet	O	N	<valeur de hachage> = 72 86 1A 03 F4 14 9F AF FD 1F 41 A5 22 B8 B2 20 E3 86 19 73

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Utilisation de la clé	O	O	Signature du certificat, Signature de la Liste de Révocation des Certificats
Stratégies de certificat	O	N	Identificateur de stratégie = anyPolicy (2.5.29.32.0) Identifiant du qualificatif de stratégie (1.3.6.1.5.5.7.2.1) = CPS Qualificatif = http://pki-g2.ariadnext.fr/pc-g2-root-v1.pdf
Contraintes de base	O	O	CA = TRUE Contrainte de longueur de chemin d'accès = 1
Algorithme d'empreinte	N	N	SHA1
Empreinte numérique	N	N	<valeur de hachage> = D9 C4 F4 4C 02 E5 59 A3 43 EA 04 A5 73 A5 2C 46 DC D6 90 A6

7.1.2. Certificats des sous-AC

7.1.2.1. Champs de base

Champ	Valeur
Version	2 pour V3
Numéro de série	<Créé par l'outil>
Algorithme de signature	sha512WithRSAEncryption (1.2.840.113549.1.1.13)
DN Émetteur	CN = AriadNEXT Root CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
DN Objet	CN = <nom de l'AC Fille> OU = 0002 52076922500027 O = AriadNEXT C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 10 ans
Algorithme de clé publique	RSAEncryption (1.2.840.113549.1.1.1)
Clé publique	< valeur de la clé publique de type RSA 4096 bits >

7.1.2.2. Extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé de l'autorité	O	N	<valeur de hachage> = 72 86 1A 03 F4 14 9F AF FD 1F 41 A5 22 B8 B2 20 E3 86 19 73
Identificateur de la clé du sujet	O	N	<valeur de hachage>
Utilisation de la clé	O	O	Signature du certificat, Signature de la Liste de Révocation des Certificats
Stratégies de certificat	O	N	Identificateur de stratégie = anyPolicy (2.5.29.32.0) Identifiant du qualificatif de stratégie (1.3.6.1.5.5.7.2.1) = CPS Qualificatif = http://pki-g2.ariadnext.fr/pc-g2-root-v1.pdf
Point de distribution de la CRL	O	N	URL = http://pki-g2.ariadnext.fr/arl-g2-root.crl
Basic Constraints	O	O	CA = TRUE Contrainte de longueur de chemin d'accès = 0
Algorithme d'empreinte	N	N	SHA-1
Empreinte numérique	N	N	Valeur de l'empreinte

7.2. Profil des Listes de Certificats Révoqués

Ce paragraphe décrit le profil ARL.

7.2.1. Champs de base des ARL

Champ	Valeur
Version	1 pour V2
Algorithme de signature	sha512WithRSAEncryption (1.2.840.113549.1.1.13)
DN Émetteur	CN = AriadNEXT Root CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
Valide à partir du	YYMMDDHHMMSS

Champ	Valeur
Valide jusqu'au	YYMMDDHHMMSS + 1 an
Certificats révoqués	< liste des certificats révoqués identifiés par leur numéro de série, et comportant la date de révocation >

7.2.2. Extensions des ARL

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé de l'autorité	O	N	<valeur de hachage> = `72 86 1A 03 F4 14 9F AF FD 1F 41 A5 22 B8 B2 20 E3 86 19 73`
Numéro de l'ARL	O	N	< Numéro incrémental pour les ARL >

8. Audit de conformité et autres évaluations

Ce paragraphe concerne les **audits réalisés en interne par l'Autorité de Certification** afin de vérifier la conformité de l'implémentation au regard de la Politique de Certification, dans une démarche d'amélioration continue.

8.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service de son IGC ou suite à toute modification significative au sein d'une composante, l'AC fait procéder à un contrôle de conformité de cette composante.

L'AC procède à un **contrôle régulier de conformité de l'ensemble de son IGC une fois tous les deux ans**.

Des contrôles internes peuvent également être déclenchés sur décision de l'AC, sur des périmètres donnés.

8.2. Identités / qualification des évaluateurs

L'AC s'engage à mandater des contrôleurs qui soient compétents en sécurité des systèmes d'information, en particulier dans le domaine d'activité de la composante de son IGC contrôlée.

8.3. Relations entre évaluateurs et entités évaluées

L'AC veillera à ce que l'équipe d'audit ne soit pas impliquée dans la gestion opérationnelle de l'AC, et à ce qu'elle soit dûment autorisée à pratiquer les contrôles visés.

8.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une partie de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'IGC (contrôles périodiques).

Ils visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC, dans la DPC, et dans les autres documents de politiques ou opérationnels cités dans la PC et la DPC.

Le sujet et le périmètre des évaluations sont préalablement définis dans un programme d'audit qui est validé par l'AC.

Ces évaluations comprennent notamment des audits techniques qui seront réalisés par un prestataire d'audit de la sécurité des systèmes d'information qualifié.

8.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, 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'AC 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'AC et doit respecter ses politiques de sécurité internes.

- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

8.6. Communication des résultats

Les résultats des audits de conformité seront tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats d'AC

Sans objet.

9.1.2. Tarifs pour accéder aux certificats

L'accès aux certificats d'AC via le site de publication de l'AC Racine est libre et gratuit.

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

L'accès aux informations d'état et de révocation des certificats via le site de publication de l'AC Racine est libre et gratuit.

9.1.4. Tarifs pour d'autres services

Sans objet.

9.1.5. Politique de remboursement

Sans objet.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

IDnow dispose d'une couverture par les assurances pour les risques qui pourraient engager sa responsabilité .

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- La DPC de l'AC.

- Les clés privées de l'AC et des composantes.
- Les données d'activation associées aux clés privées d'AC.
- Tous les secrets de l'IGC.
- Les journaux d'évènements des composantes de l'IGC.
- Les dossiers d'enregistrement.
- Les causes de révocations.

9.3.2. Informations hors du périmètre des informations confidentielles

Voir § 9.3.1.

9.3.3. Responsabilités en terme de protection des informations confidentielles

L'AC s'engage à appliquer les procédures de sécurité définies dans la présente PC ainsi que la DPC afin d'assurer la confidentialité des informations identifiées au § 9.3.1 ainsi que leur intégrité en cas d'échange de données.

L'AC s'engage à respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement à des tiers dans le cadre de procédures légales. Elle s'engage également à donner l'accès aux dossiers d'enregistrement aux responsables d'AC.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

L'AC est conforme aux dispositions de la loi n°78-17 « Informatique et Libertés » ainsi que celles issues du Règlement (UE) 2016/679 du Parlement européen et du Conseil « Règlement Général sur la Protection des Données ».

Le droit d'accès, de rectification ou d'opposition des données à caractère personnel conformément à ces textes réglementaires peut être exercé par les personnes concernées auprès d'IDnow SAS.

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les causes de révocation des certificats.
- Les dossiers d'enregistrement.

9.4.3. Informations à caractère non personnel

Voir § 9.4.2.

9.4.4. Responsabilité en terme de protection des données personnelles

L'AC reconnaît avoir procédé aux formalités déclaratives qui lui incombent au titre de la présente PC et des traitements de données à caractère personnel qui seraient réalisés.

9.4.5. Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les clients à l'AC ne seront ni divulguées ni transférées à un tiers sauf dans les cas suivants :

- Consentement préalable du client.
- Décision judiciaire ou autre autorisation légale.

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

Cf. législation et réglementation en vigueur sur le territoire français.

9.4.7. Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5. Droits sur la propriété intellectuelle et industrielle

Cf. législation et réglementation en vigueur sur le territoire français.

9.6. Interprétations 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 PC de l'AC 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 contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. § 8) et l'organisme de qualification.
- Respecter les accords ou contrats qui les lient entre elles ou avec les clients.
- 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. Autorités de certification

L'AC s'engage à :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour une AC donnée et que le Responsable d'AC a accepté le certificat, conformément aux exigences du § 4.4.
- Tenir à disposition des Porteurs, des RCC, et des Utilisateurs de Certificats la notification de Révocation du Certificat d'une composante de l'IGC ou d'un serveur.

- Diffuser publiquement la présente PC et les LCR.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que les clients sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

La relation entre un client et l'AC est formalisée dans les Conditions Générales d'Utilisation (intégrées dans le formulaire de demande) signés par le client, précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, par elle-même ou l'une de ses composantes. Elle reconnaît avoir pris les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

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

9.6.2. Service d'enregistrement

L'AE s'engage à mettre en œuvre les moyens décrits dans la présente PC complétée par la DPC pour :

- Vérifier la validité des pièces justificatives et l'exactitude des mentions du dossier d'enregistrement qui établissent l'identité et l'organisation d'appartenance du client.
- Vérifier l'origine et l'exactitude de toute demande de révocation et mettre en œuvre les moyens permettant de les traiter.
- Respecter les politiques de contrôle d'accès aux composantes techniques de l'Autorité d'Enregistrement.

9.6.3. Utilisateurs de certificats

Les utilisateurs utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis.
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application.
- Pour chaque certificat de la chaîne de certification, du certificat du service applicatif jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation).
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.4. Autres participants

Sans objet.

9.7. Limite de garantie

Sans objet.

9.8. Limite de responsabilité

L'AC décline toute responsabilité à l'égard de l'usage qui est fait des certificats qu'elle a émis dans des conditions et à des fins autres que celles prévues dans la présente politique de certification que dans tout autre document contractuel applicable associé.

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, ceux habituellement retenus par la jurisprudence des cours et tribunaux français.

9.9. Indemnités

Pas d'exigence particulière.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

Le présent document est applicable 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 des PC Types du RGS peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.

En fonction de la nature et de l'importance des évolutions apportées à la PC Type, le délai de mise en conformité de la PC de l'AC sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

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

Pas d'exigence particulière.

9.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra:

- Au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- Au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

L'AC contrôlera que tout projet de modification de sa PC reste conforme aux exigences de la PC Type du RGS, et des éventuels documents complémentaires du RGS. En cas de changement important, l'AC pourra faire appel à une expertise technique pour en contrôler l'impact.

9.12.2. Mécanisme et période d'information sur les amendements

Toutes les composantes et acteurs de l'IGC sont tenus informés des amendements effectués sur la PC, et des impacts pour eux.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

Toute évolution majeure de la PC ayant un impact majeur sur les certificats déjà émis sera traduite par une évolution de l'OID (cf. § 1.2).

9.13. Dispositions concernant la résolution de conflits

En cas de contestation ou de litige relatif à l'interprétation, la formation ou l'exécution des documents contractuels ou de leurs avenants, et faute d'être parvenu à un accord amiable dans un délai d'un mois à compter de la naissance de la contestation ou du litige, les Parties donnent compétence expresse et exclusive aux tribunaux, nonobstant pluralité de défendeurs, d'action en référé, d'appel en garantie ou de mesure conservatoire.

9.14. Juridictions compétentes

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

9.15. Conformité aux législations et réglementations

La présente PC est conforme aux exigences énoncées dans les textes législatifs et réglementaires français et européens applicables cités au cours du § 9.

9.16. Dispositions diverses

9.16.1. Accord global

Pas d'exigence particulière.

9.16.2. Transfert d'activités

Voir § 5.8.

9.16.3. Conséquences d'une clause non valide

Pas d'exigence particulière.

9.16.4. Application et renonciation

Pas d'exigence particulière.

9.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

9.17. Autres dispositions

Pas d'exigence particulière.