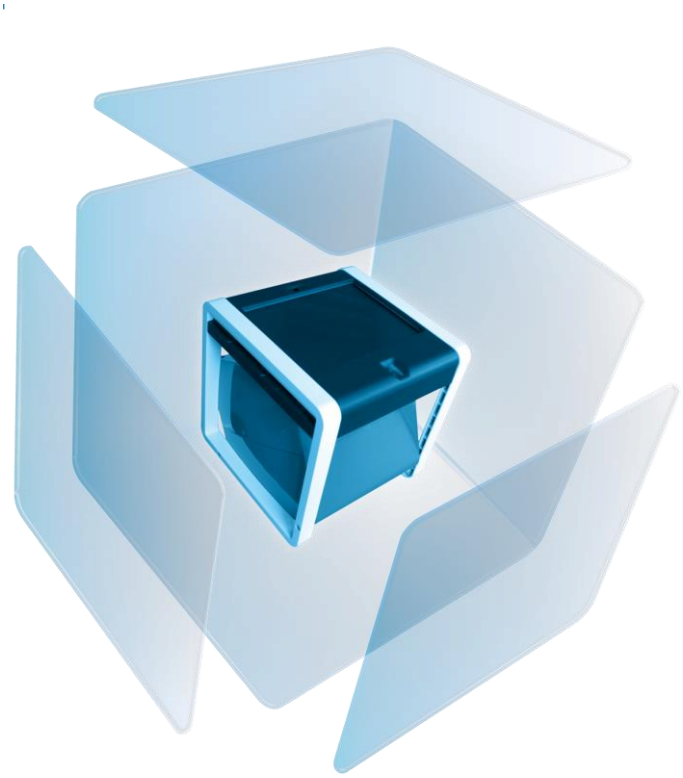
AriadNEXT
secure scan & sign

www.ariadnext.com

AUTORITE DE CERTIFICATION ARIADNEXT « Legal Person CA G2 »

Politique de Certification



Classification	**Identification (OID)**
Document public	1.3.6.1.4.1.38226.10.4.3.1.1.1 (Profil Cachet) 1.3.6.1.4.1.38226.10.4.3.2.1.1 (Profil Horodatage)

SOMMAIRE

Suivi des modifications du document

N° Version	Date de version	Nature de la modification ou de la création	Entité / Nom Prénom/
V1	21/05/2015	Création	AriadNEXT / Claire-Lise Beaumont
V1.1	09/06/2016	Modification concernant l'initialisation des dispositifs de protection des clés privées	AriadNEXT / Claire-Lise Beaumont
V1.2	13/03/2017	Internationalisation de l'identification des entreprises et organisations	AriadNEXT / Claire-Lise Beaumont
V1.3	06/04/2017	Modification de la fenêtre de renouvellement des certificats d'horodatage	AriadNEXT / Claire-Lise Beaumont
V1.4	15/05/2017	Suite de l'internationalisation de l'identification des entreprises et organisations	AriadNEXT / Claire-Lise Beaumont

1. INTRODUCTION

1.1. Présentation générale

AriadNEXT est un fournisseur de solutions innovantes pour la **dématérialisation** et la **sécurisation** des données.

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

Ces besoins de certificats sont adressés par une **PKI propre à AriadNEXT**, hébergée et opérée **en interne**, nommée **« PKI AriadNEXT G2 ».** Cette PKI est mise en œuvre conformément aux standards et aux bonnes pratiques dans le domaine.

L'Autorité de Certification « Legal Person CA G2 » est définie et mise en œuvre conformément aux exigences du Référentiel Général de Sécurité, Version 2, niveau * (1 étoile).

L'Autorité de Certification « Legal Person CA G2 » délivre des certificats à des personnes morales pour réaliser des signatures de type cachet ou signer des jetons d'horodatage.

La présente **Politique de Certification** adresse les deux profils de certificats définis pour cette AC :

- **Un profil « Cachet qualifié »** pour l'émission de cachets serveurs.
- **Un profil « Horodatage qualifié »** pour la signature de jetons d'horodatage.

1.2. Identification du document

Le profil « Cachet qualifié» de l'AC « Legal Person CA G2 » est identifié par l'OID 1.3.6.1.4.1.38226.10.4.3.1.1.1.

La Déclaration de Pratiques de Certification correspondante est identifiée par l'OID 1.3.6.1.4.1.38226.10.4.3.1.2.1.

Le profil « Horodatage qualifié » de l'AC « Legal Person CA G2 » est identifié par l'OID 1.3.6.1.4.1.38226.10.4.3.2.1.1.

La Déclaration de Pratiques de Certification correspondante est identifiée par l'OID 1.3.6.1.4.1.38226.10.4.3.2.2.1.

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
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

Applicatif de vérification de cachet – Il s'agit de l'application mise en œuvre par l'utilisateur pour vérifier le cachet des données reçues à partir de la clé publique du serveur contenue dans le certificat correspondant.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du Porteur du

certificat ou des besoins d'authentification ou de cachet du serveur auquel le certificat est rattaché.

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 chapitre et du chapitre I.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 chapitre 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. Dans le cadre de la présente PC, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RC et portant sur une bi-clé de signature de données (de type cachet ou horodatage), sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

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.

Dispositif de création de cachet – voir **Dispositif de protection des clés privées**.

Dispositif de protection des clés privées – Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée.

Dossier d'enregistrement – ensemble des justificatifs nécessaires à la validation de la demande. Ils sont définis au paragraphe 4.1.2.

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 se rapporte à une entité.

Fenêtre de renouvellement – période de temps pendant laquelle un certificat peut être renouvelé. Elle démarre quelques mois avant la date d'expiration du certificat et peut se

terminer après la date d'expiration du certificat. La valeur de la fenêtre de renouvellement est définie dans la présente PC (paragraphe 4.7.1).

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 du serveur.

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 chapitre 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 l'AC.

Motif de révocation – Circonstance pouvant être à l'origine de la révocation d'un certificat. Les motifs de révocation sont détaillés au paragraphe 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 RC 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 RC 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.

Responsable du Certificat (RC) - Cf. chapitre 1.4.3.

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 est alors inutilisable.

Serveur – Il s'agit d'un service applicatif disposant d'un certificat fourni par l'AC, rattachés à l'entité (identifiée dans le certificat). Ce service est hébergé sur un ou plusieurs serveurs physiques rattachés à un même nom de domaine (FQDN).

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 chapitre 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

AriadNEXT joue le rôle **d'Autorité de Certification** pour les **profils de certificats** objets de la présente Politique de Certification.

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 des clés de l'AC, des certificats de l'AC, des certificats de serveur et des éléments secrets de l'IGC** : cette fonction est décrite au paragraphe 6.
- **Remise au Responsable de Certificat** : cette fonction consiste à remettre le certificat au Responsable de Certificat (voir 1.4.3). Cette fonction est décrite aux paragraphes 3 et 4.
- **Autorité d'Enregistrement et gestion du cycle de vie des certificats** (enregistrement, révocation, renouvellement) : cette fonction est décrite aux paragraphes 3 et 4.
- **Publication des informations réglementaires de l'AC** : cette fonction est décrite au paragraphe 2.2.
- **Publication des informations sur le statut (ou l'état) des certificats** : cette fonction est décrite au paragraphe 4.10.
- **Gestion des révocations** : cette fonction est décrite au paragraphe 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

La fonction d'Autorité d'Enregistrement (AE) est assurée au sein d'AriadNEXT, par des opérateurs d'enregistrement (voir paragraphe 5.2.1).

N.B : il n'existe pas de mécanisme de délégation des pouvoirs de l'AE à des entités tierces.

L'Autorité d'Enregistrement assure **deux missions principales** :

- La **validation de l'identité et de la qualité des Responsables de Certificat** (RC) lors de l'enregistrement des certificats.
- La **gestion opérationnelle du cycle de vie des certificats** :
  - Etablissement de la demande de certificat et transmission à l'IGC pour traitement (voir paragraphes 4.1 à 4.4).
  - Demande de renouvellement (voir paragraphe 4.7).
  - Demande de révocation (voir paragraphe 4.9).

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

- Archivage des pièces du dossier d'enregistrement.

- Conservation et protection des données des personnes concernées par les fonctions de l'IGC (notamment RC).

Les opérateurs d'enregistrement utilisent le logiciel d'AE pour consigner l'ensemble de leurs activités et réaliser les demandes auprès de l'AC.

1.4.3. Responsables de certificats de serveurs

Chaque certificat de serveur est confié à un Responsable de Certificat (RC).

- Le RC a un lien hiérarchique ou contractuel avec l'entité organisationnelle identifiée dans le certificat.
- La qualité du RC est validée par l'Autorité d'Enregistrement lors de la demande initiale (voir paragraphe 3.2.3.1).
- Le RC garantit le lien entre le certificat et le serveur qui le met en œuvre.
- Le RC est responsable du renouvellement du certificat (voir paragraphe 4.7).
- Il fait partie des personnes autorisées à demander une révocation du certificat (voir paragraphe 4.9.2).

La présente PC autorise le **changement de RC**, notamment pour gérer le cas du départ d'un RC : voir le paragraphe 3.2.3.2.

1.4.4. Utilisateurs de certificats

Les utilisateurs de certificats sont tous les services qui mettent en œuvre et qui valident les signatures de type cachet et les jetons d'horodatage émis par l'AC « Legal Person CA G2 ».

1.4.5. Autres participants

Les différentes **composantes de l'IGC** sont présentées dans la Déclaration des Pratiques de Certification.

Le rôle de Mandataire de Certification n'est pas mis en œuvre.

1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

1.5.1.1. Bi-clés et certificats des serveurs

La clé privée délivrée au service applicatif sert exclusivement à produire des signatures de type cachet (pour le profil « Cachet ») ou à signer des jetons d'horodatage (pour le profil « Horodatage »).

Les certificats dans le périmètre de cette Politique de Certification permettent d'adresser des besoins de sécurité moyens eu égard aux risques qui menacent les services applicatifs les mettant en œuvre.

1.5.1.2. Bi-clés et certificats d'AC et de composantes

La clé privée de l'Autorité de Certification est utilisée exclusivement dans les cas suivants :

- Signature des certificats de serveur.
- Signature des Listes de Certificats Révoqués (LCR ou CRL).

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

- Authentification mutuelle entre les différents composants logiciels de l'IGC.
- Authentification des administrateurs AriadNEXT lors de l'accès aux serveurs de l'IGC.
- Authentification du personnel de l'Autorité d'Enregistrement lors de l'accès aux fonctions de l'Autorité d'Enregistrement.

Ces certificats sont émis par une **IGC distincte, propre à AriadNEXT**. Le niveau de sécurité de cette IGC est cohérent avec le niveau de sécurité requis pour l'AC.

1.5.2. Domaines d'utilisation interdits

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

Les Conditions Générales d'Utilisation sont diffusées par l'AC aux utilisateurs de certificats identifiés au paragraphe 1.4.4, via son site de publication (voir paragraphe 2.2).

1.6. Gestion de la PC

1.6.1. Entité gérant la PC

Le responsable d'AC (voir les rôles de confiance au paragraphe 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'AriadNEXT 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 AriadNEXT par les moyens suivants :

- **Email** : certificats@ariadnext.com
- **Courrier** : Autorité de Certification AriadNEXT, 80 av des Buttes de Coësmes 35700 RENNES – France.
- **Téléphone** : +33 (0)825 590 003.

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

2.1. Entités chargées de la mise à disposition des informations

AriadNEXT assure la publication de toutes les informations citées au paragraphe 2.2, via le **site de publication http://certificats.ariadnext.com.**

2.2. Informations devant être publiées

L'AC publie les informations suivantes :

- Politique de Certification.
- Conditions Générales d'Utilisation.
- Certificat d'AC.
- Empreinte du certificat d'AC.
- Liste des Certificats Révoqués (LCR ou CRL).
- Adresse email du point de contact de l'AC.
- Coordonnées de l'Autorité d'Enregistrement : numéro de téléphone, adresse email, adresse postale.
- Formulaire de révocation de certificat.
- Formulaire de nomination d'un nouveau RC (comprenant l'obligation de désigner un successeur en cas de départ).

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

Remarque 1 : les conditions générales d'utilisation décrivent de manière compréhensible par les personnes extérieures à l'AC :

- Les conditions d'obtention et d'acceptation d'un certificat.
- Les conditions de gestion du cycle de vie du certificat.
- Les usages autorisés du certificat.
- Les obligations du RC (dont la génération de la clé privée dans un dispositif de protection des clés privées).
- Les personnes autorisées à demander une révocation du certificat.
- La durée de conservation des archives des dossiers d'enregistrement.

Remarque 2 : le formulaire de demande de certificat n'est pas publié dans la mesure où les demandes doivent être faites via le logiciel d'AE.

2.3. Délais et fréquences de publication

La fréquence de mise à jour des CRL est de 8 heures.

La durée de validité des CRL est de 72 heures.

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

- Suite à leur mise à jour, **dans un délai maximal de 30 minutes (cas des CRL).**
- Suite à leur mise à jour, dans un délai maximal de 24 heures ouvrées (cas du certificat d'AC et de son empreinte).
- Suite à leur validation (cas de la PC ou des informations de contact).

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**. Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats d'entité finale et/ou de LCR correspondantes.

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'AriadNEXT disposant d'un **rôle de confiance** (voir paragraphe 5.2.1). Il requiert une **authentification** par certificat (voir paragraphe 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 et des serveurs sont identifiés par un DN de type X.501.

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

- Country = FR
- Organization = AriadNEXT
- Organization Unit = 0002 52076922500027
- Common Name = Legal Person CA G2

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

- Country = [nom du pays d'implantation du client]
- Organization = [nom de l'organisation du client]
- Organization Unit = [code identifiant le référentiel][espace][numéro identifiant l'organisation du client dans le référentiel]
- Common Name = [nom du certificat tel que décrit au paragraphe 3.1.2]

3.1.2. Nécessité d'utilisation de noms explicites

Le champ Common Name du DN doit contenir le nom du service applicatif selon la **règle de nommage** suivante :

[Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif]

De plus, afin de rendre explicite le nom des certificats, le champ « Subject Alt Name » peut être utilisé. Dans ce cas, il contient le nom complet du service applicatif.

Par exemple : CN = « Société.FacturationPro.Signature » et Subject Alt Name = « Société Signature des factures pro ».

Le nommage des **certificats de tests** suit la règle suivante : le champ Common Name doit contenir la mention TEST en majuscules suivie d'un espace suivie du nom du certificat répondant aux règles de nommage du CN définies ci-dessus.

Le champ Organization Unit du DN comporte un numéro en deux parties :

- Code identifiant le référentiel : ce code est un identifiant alpha-numérique indiquant le référentiel d'identification de l'organisation.
    - Code ICD : ce code sur 4 chiffres est maintenu par la British Standards Institution. Pour la France qui maintient le répertoire SIRENE, le code ICD est 0002.
    - Code GS1 : ce code est basé sur un identifiant défini par l'association GS1 en charge de la standardisation dans le domaine de la logistique. GS1 définit des identifiants nommés « company prefix » correspondant à des pays. Ainsi pour la Belgique, le préfixe GS1 est 540. AriadNEXT convient d'utiliser un code GS1 avec le format suivant [G][company prefix]. Ainsi pour la Belgique, le code d'identification est G540.
- Numéro identifiant l'organisation du client dans le référentiel indiqué. Ce numéro possède un format variable selon les référentiels.
    - Pour la France, selon le code ICD 0002, le numéro est sur 9 (code SIREN) ou 14 chiffres (code SIRET).

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 se porte garante de **l'unicité des noms des certificats d'entité finale au sein de l'Autorité de Certification**.

Cette unicité repose sur le **champ DN** du certificat.

La détection des éventuels cas d'homonymie est réalisée par l'Autorité d'Enregistrement lors de l'enregistrement initial des demandes de certificats.

3.1.6. Identification, authentification et rôle des marques déposées

L'AC valide le nom inscrit dans les certificats sur la base des règles présentées au paragraphe 3.1.2 lors de l'enregistrement de la demande.

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

3.2. Validation initiale de l'identité

L'enregistrement d'une demande de certificat requiert l'enregistrement du RC qui lui est associé.

L'AC AriadNEXT impose la réalisation d'un certain nombre de contrôles sur l'identité et la qualité du RC.

Ces contrôles ont lieu :

- Soit lors de l'enregistrement de la demande de certificat.
- Soit lors de l'arrivée d'un nouveau RC en cours de validité d'un certificat.

Ces deux cas de figure sont précisés respectivement aux paragraphes 3.2.3.1 et 3.2.3.2.

3.2.1. Méthode pour prouver la possession de la clé privée

La bi-clé est générée sous le contrôle du futur RC en charge du certificat. Dans le cas d'une demande initiale, cette génération de bi-clé est réalisée par AriadNEXT en présence du RC (voir DPC).

Le RC doit fournir une demande de certificat au format PKCS#10 à l'AC.

L'AC vérifie la validité cryptographique de la signature de la demande de certificat en provenance du RC.

3.2.2. Validation de l'identité d'un organisme

Cf paragraphe 3.2.3.

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un Responsable de Certificat sans MC pour un certificat serveur à émettre

La phase d'enregistrement de la demande de certificat, décrite au paragraphe 4.1, comporte une **phase de validation de l'identité et de la qualité du RC, réalisée par l'AE.**

La validation de l'identité et de la qualité du RC ne requiert **pas de face-à-face** entre l'AE et le RC, mais la présentation d'un ensemble de justificatifs.

Les vérifications effectuées par l'AE sont les suivantes :

- **Vérification de la qualité du RC** sur la base d'un formulaire de nomination signé par un représentant légal de l'organisation qu'il représente, signé par le RC, et daté de moins de 3 mois.

- **Vérification de l'identité du RC** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE

AriadNEXT vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du RC.

- **Vérification de l'organisation d'appartenance du RC** et de son représentant légal à l'aide d'un extrait de K-Bis ou d'une attestation d'existence de l'organisation équivalente comportant le numéro d'identification unique de l'organisation.

- **Vérification de la qualité du représentant légal** à l'aide de l'extrait de K-Bis fourni (ou pièce équivalente), ou d'une base de connaissances sur l'organisation qu'il représente, ou d'une attestation de représentant légal (nécessaire si le représentant légal n'est pas celui indiqué dans les statuts publics de l'organisation).

- **Vérification de l'identité du représentant légal** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE AriadNEXT vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du représentant légal.

Remarque 1 : Si les justificatifs d'identité originaux ne sont pas présentés directement à l'AE, dans ce cas, des copies papiers des justificatifs d'identité doivent être fournies à l'AE et doivent comporter une date de moins de trois mois, la signature du RC, respectivement du représentant légal, et la mention « copie certifiée conforme à l'original ».

Remarque 2 : Une fois l'enregistrement du RC réalisé, le RC dispose d'un compte au niveau du logiciel d'AE lui permettant de réaliser ses demandes de certificat. Le RC s'authentifie à l'AE par mot de passe ou par certificat.

Remarque 3 : **La totalité du processus d'enregistrement et le contenu du dossier d'enregistrement sont présentés aux paragraphes 4.1 à 4.4.**

3.2.3.2. Enregistrement d'un nouveau Responsable de Certificat sans MC pour un certificat serveur déjà émis

Un certificat doit toujours être placé sous la responsabilité d'un RC disposant d'un lien hiérarchique ou contractuel valide avec l'organisation mentionnée dans le DN du certificat.

Le RC a l'obligation de signaler la fin de ses fonctions de RC à l'AE. Si aucun nouveau RC n'est désigné pour ce certificat, l'AE se réserve le **droit de révoquer** ce certificat (voir paragraphe 4.9.1).

Sinon, l'AE procède à la **validation de l'identité et de la qualité du nouveau RC** qui doit être **nommé par un représentant légal** de son organisation d'appartenance. Les **pièces justificatives suivantes** sont demandées pour effectuer les vérifications suivantes :

- **Vérification de la qualité du RC** sur la base d'un formulaire de nomination signé par un représentant légal de l'organisation qu'il représente, signé par le RC, et daté de moins de 3 mois.

- **Vérification de l'identité du RC** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE AriadNEXT vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du RC.

- **Vérification de l'acceptation des CGU par le RC.** Le nouveau RC doit lire et accepter les CGU pour le certificat dont il devient RC. L'AE enregistre une trace de cette acceptation.

- **Vérification de la qualité du représentant légal** à l'aide d'une base de connaissances sur l'organisation qu'il représente, ou d'une attestation de représentant légal (nécessaire si le représentant légal n'est pas celui indiqué dans les statuts publics de l'organisation).

- **Vérification de l'identité du représentant légal** en tant que personne physique sur la base d'un justificatif d'identité (carte nationale d'identité, passeport, titre de séjour). L'AE AriadNEXT vérifie la validité de ce justificatif d'identité et sa cohérence avec l'identité du représentant légal.

3.2.3.3. Enregistrement d'un Mandataire de Certification

Sans objet.

3.2.3.4. Enregistrement d'un Responsable de Certificat via un MC pour un certificat serveur à émettre

Sans objet.

3.2.3.5. Enregistrement d'un nouveau Responsable de Certificat via un MC pour un certificat serveur déjà émis

Sans objet.

3.2.4. Informations non vérifiées du RC et/ou du serveur informatique

Sans objet.

3.2.5. Validation de l'autorité du demandeur

Voir paragraphe 3.2.3.1, étape de « Vérification de la qualité du RC ».

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 au RC sans renouvellement de la bi-clé correspondante.

3.3.1. Identification et validation pour un renouvellement courant

A l'occasion du **premier renouvellement** d'un certificat, **si la demande provient du RC enregistré pour le certificat,** l'AE vérifie la présence du RC dans sa base de données. S'il est présent, le RC n'a pas besoin de fournir de pièces justificatives pour sa demande de renouvellement de certificat.

Sinon (si le renouvellement s'accompagne d'un changement de RC), l'AE procède à la vérification de l'identité et de la qualité du RC comme indiqué au paragraphe 3.2.3.1 (**enregistrement initial**).

A l'occasion du **renouvellement suivant**, l'AE procède à la vérification de l'identité et de la qualité du RC comme indiqué au paragraphe 3.2.3.1 (**enregistrement initial**).

3.3.2. Identification et validation pour un renouvellement après révocation

Une **révocation** de certificat peut être suivie d'une **nouvelle demande** de certificat.

Dans ce cas, l'AE procède à la vérification de l'identité et de la qualité du RC comme indiqué au paragraphe 3.2.3.1 (**enregistrement initial**).

3.4. Identification et validation d'une demande de révocation

Une demande de révocation peut provenir d'un ensemble d'acteurs autorisés par cette PC (voir paragraphe 4.9.2).

Si le demandeur de la révocation est un opérateur d'enregistrement, l'accès à la fonction de révocation est soumis à :

- Authentification à l'aide d'un moyen **d'authentification forte** (voir paragraphe 1.5.1.2).
- **Contrôle d'accès** sur la base de la vérification des droits d'accès.

Remarque : les droits d'accès auront été positionnés en cohérence avec le rôle de confiance de la personne, lors de l'affectation de son rôle (voir paragraphe 5.2.1).

Si le demandeur de la révocation est le responsable de l'AC, il doit créer sa demande de révocation à l'aide d'un formulaire papier. Le personnel de l'AE valide son identité en face-à-face, puis traite la demande.

Si le demandeur de la révocation est un RC ou un représentant légal de l'organisation identifiée dans les certificats, l'accès à la fonction de révocation est contrôlé de la manière suivante :

- Si la demande de révocation est faite **via le logiciel d'AE** :
  - **Validation de l'identité** de la personne par authentification à l'AE. L'authentification sur le logiciel d'AE se fait par login/mot de passe ou par certificat. En cas d'urgence, une authentification à l'AE par soumission d'une pièce d'identité peut être réalisée.
  - **Validation de l'autorité** de la personne selon les règles de l'AC (voir paragraphe 4.9.2).
- Si la demande de révocation est faite **par mail ou par courrier papier** :

- Envoi **du formulaire de révocation signé** par le demandeur.
- **Validation de l'identité** de la personne sur la base d'une **photocopie d'un justificatif d'identité**, daté de moins de trois mois, signé par la personne et portant la mention « copie certifiée conforme à l'original ».
- **Validation de l'autorité de la personne** selon les règles de l'AC (voir paragraphe 4.9.2).

Remarque : Les demandes de révocation ne peuvent pas être faites par téléphone. L'AE reste disponible par téléphone sur les jours et heures ouvrés pour assister les clients dans leurs démarches en ligne au niveau du logiciel de l'AE.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Un certificat peut être demandé par le **futur RC** qui en aura la responsabilité, ou bien par son **représentant légal**.

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

Remarque : ce paragraphe s'applique aux demandes de certificat réalisées une fois le service applicatif initialisé et le premier certificat émis. Le cas de la première demande est décrit dans la DPC.

Une demande de certificat doit être adressée à l'AE via le logiciel d'AE.

Pour cela, le demandeur aura satisfait aux **pré-requis** suivants **:**

- **Générer une bi-clé dans le dispositif de protection des clés privées** (voir paragraphe 6.1.1.3) et **conformément aux types et tailles de clés attendus pour la présente PC** (voir paragraphe 6.1.5).
- **Préparer les justificatifs** nécessaires pour la constitution du dossier d'enregistrement.
- **Créer un compte d'accès** au niveau du logiciel d'AE.

Le demandeur (voir personnes autorisées au paragraphe 4.1.1) doit **s'authentifier** au niveau du logiciel d'AE (par login/mot de passe ou par certificat).

Un ensemble d'informations doivent être renseignées et des **justificatifs** doivent être transmis à l'AE le cas échéant (via le logiciel d'AE).

La **demande de certificat** doit au moins mentionner :

- Les nom, prénom, adresse email du RC.
- Le nom du certificat (contenu du champ Common Name).
- Le nom de la personne morale (organisation) qui sera identifiée dans le DN du certificat et dans les signatures réalisées avec le certificat.
- Le numéro d'identification de cette personne morale dans un référentiel officiel figurant dans la liste des codes ICD maintenue par le British Standards Institute.
- Les nom, prénom, adresse email du représentant légal.

Le demandeur doit lire les CGU et les accepter. Si le demandeur est le représentant légal, dans ce cas, le RC recevra un email avec un lien vers les CGU. La demande ne sera pas validée par l'AE tant que le RC n'aura pas accepté les CGU.

Le demandeur doit ensuite fournir les justificatifs propres à la demande (et qui constituent, avec les CGU, le dossier d'enregistrement) :

- **Justificatif d'identité du RC** (carte d'identité, passeport ou titre de séjour) : un scan du recto du justificatif d'identité doit être uploadé au niveau de l'AE.
- **Formulaire de nomination du RC** signé par le RC et son représentant légal, daté de moins de 3 mois. Un modèle de formulaire de nomination peut être téléchargé au niveau du site de publication (voir paragraphe 2).
- **Justificatif d'existence de l'organisation du client** (pour la France, extrait K-Bis, ou certification d'identification au répertoire SIRENE, ou pour les administrations, pièce portant délégation de l'autorité responsable de la structure, ou pour les organisations situées à l'étranger, tout document officiel prouvant l'existence de l'organisation et son numéro d'identification).
- **Justificatif d'identité du représentant légal** (carte d'identité, passeport ou titre de séjour) : un scan du recto du justificatif d'identité doit être uploadé au niveau de l'AE.
- **Attestation de représentant légal**, si le représentant légal n'est pas connu à travers les statuts publics de l'organisation (extrait Kbis ou informations publiques sur l'organisation).

Le demandeur doit ensuite uploader au niveau du logiciel d'AE une **demande de certificat au format PKCS#10 (*Certificate Signing Request*, CSR) signée à l'aide de la clé privée générée par le RC dans le dispositif de protection des clés privées** (voir paragraphe 6.1.1.3).

4.2. Traitement d'une demande de certificat

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

L'AE procède au **traitement de la demande d'enregistrement** de certificat :

- L'AE vérifie la **cohérence des justificatifs** présentés dans le dossier d'enregistrement avec les informations d'identité et d'organisation renseignées par le demandeur.
- L'AE **valide l'identité et l'autorité du demandeur** conformément au paragraphe 3.2.3.1.
- L'AE **valide l'existence de l'organisation du client.**
- L'AE **valide la nomination du RC**.
- L'AE vérifie les éventuels **cas d'homonymie**, et statue sur le nom du certificat porté dans le champ Common Name dans le DN du certificat, et éventuellement dans le champ Subject Alt Name conformément aux règles de l'AC (voir paragraphe 3.1). L'AE s'assure que ce nom correspond à un serveur et à une application existants (tels que demandés par le RC ou son représentant légal).
- Si la demande de certificat est acceptée, l'opérateur d'enregistrement valide la demande au niveau du logiciel d'AE. Cela déclenche l'envoi de la CSR auprès de l'AC.

Après validation du **dossier d'enregistrement**, l'AE procède à l'**archivage** des justificatifs reçus au format papier, le cas échéant (voir paragraphe 5.5).

Tous les contrôles réalisés par l'AE, en particulier ceux réalisés sur le titre d'identité, donnent lieu à des **traces** enregistrées au niveau du logiciel d'AE.

4.2.2. Acceptation ou rejet de la demande

L'AE **informe** le demandeur de l'acceptation ou du rejet de la demande de certificat, **par mail**.

4.2.3. Durée d'établissement du certificat

Suite à la validation de la demande par l'AE, le certificat est généré par l'AC dans les meilleurs délais.

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 effectue les actions suivantes :

- Vérification de la **validité cryptographique de la signature** de la CSR.
- Vérification de la **conformité du type et de la taille de clés** par rapport au profil du certificat demandé.
- **Génération d'un certificat et signature** par l'AC.

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

Si la demande est acceptée, l'AC fournit au demandeur, dans le mail de réponse, le certificat correspondant à la demande.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat est tacite à compter de la date d'envoi du certificat par l'AC au RC.

4.4.2. Publication du certificat

Les certificats d'entité finale ne sont pas publiés.

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 RC

Les RC sont responsables de l'usage réalisé du certificat qui leur est remis par l'AC, conformément aux exigences du paragraphe 1.5.

L'extension Key Usage du certificat permet de vérifier les usages autorisés du certificat.

Dans le cadre de la présente PC, les certificats contiennent dans l'extension Key Usage marquée comme critique les valeurs « Digital signature » et « Non-repudiation ».

Pour le profil « Horodatage qualifié », l'extension « Extended Key Usage » est également présente, marquée comme critique et contient uniquement l'identifiant «id-kp-timeStamping».

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 paragraphe 1.5.

4.6. Renouvellement d'un certificat

La notion de renouvellement telle que définie dans la RFC 3647 n'est pas autorisée dans le cadre de cette PC.

Remarque : l'IGC AriadNEXT vérifie qu'un nouveau certificat ne peut pas être établi pour une même bi-clé.

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

Ce paragraphe correspond, conformément au RGS, à la génération d'un nouveau certificat pour une nouvelle bi-clé, le DN du certificat restant inchangé.

4.7.1. Causes possibles de changement de bi-clé

Les causes possibles d'un changement de bi-clé sont les suivantes :

- Expiration du certificat.
- Fin de période d'utilisation de la clé privée.
- Révocation du certificat.

Les bi-clés des certificats du profil « Cachet qualifié » ont une durée de validité de 3 ans.

Les bi-clés des certificats du profil « Horodatage qualifié » ont une durée de validité de 3 ans.

Le renouvellement de certificat est possible à partir de 2 ans avant la date d'expiration du certificat. La fenêtre de renouvellement est donc comprise entre T-2 ans et T, où T est la date d'expiration du certificat.

4.7.2. Origine d'une demande de nouveau certificat

Cf. paragraphe 4.1.1.

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

Voir paragraphe 4.1.2.

Dans le cas du premier renouvellement, les justificatifs indiqués au paragraphe 4.1.2. ne sont pas requis.

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

Cf. paragraphe 4.3.2.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. paragraphe 4.4.1.

4.7.6. Publication du nouveau certificat

Cf. paragraphe 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 ne sont pas autorisées.

4.8.1. Causes possibles de modification d'un certificat

Sans objet

4.8.2. Origine d'une demande de modification de certificat

Sans objet

4.8.3. Procédure de traitement d'une demande de modification de certificat

Sans objet

4.8.4. Notification au RC de l'établissement du certificat modifié

Sans objet

4.8.5. Démarche d'acceptation du certificat modifié

Sans objet

4.8.6. Publication du certificat modifié

Sans objet

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

Sans objet

4.9. Révocation et Suspension des certificats

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats de serveur

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

- **Les informations du service applicatif** figurant dans son certificat **ne sont plus en conformité** avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat.
- **Le RC n'a pas respecté** les **modalités** applicables **d'utilisation** du certificat.
- **Le RC et/ou** le cas échéant **l'entité** n'ont **pas respecté** leurs **obligations** découlant de la PC de l'AC.
    - Remarque : cela concerne le cas où il n'existe plus de RC explicitement identifié pour le certificat de serveur (voir paragraphe 4.11).
- Une **erreur** (intentionnelle ou non) a été détectée **dans le dossier d'enregistrement**.
- **La clé privée du service applicatif est suspectée de compromission**, est **compromise**, est **perdue** ou est **volée**, (éventuellement les données d'activation associées).
- **Le RC ou une entité autorisée** (voir paragraphe 4.9.2.1) **demande la révocation du certificat** (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support).
- **L'arrêt définitif du service applicatif** ou la **cessation d'activité** de l'organisation identifiée dans le DN du certificat de serveur associé (voir paragraphe 4.11).
- Le certificat était destiné à des fins de test et la **période de tests** est **terminée.**

La réalisation de l'une de ces causes de révocation doit être portée à la connaissance de l'AC afin qu'elle révoque le certificat dans les meilleurs délais.

4.9.1.2. Certificats d'une composante de l'IGC

Les causes possibles d'une révocation de certificat d'AC ou d'une composante de l'IGC (voir paragraphe 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 (par exemple, suite à un audit de qualification ou de conformité négatif).

- **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'AC qui révoque immédiatement le certificat.

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats de serveur

Les **personnes autorisées** à demander la **révocation d'un certificat de serveur** sont les suivantes :

- Le Responsable de l'AC.
- Tout opérateur d'enregistrement.
- Le RC en charge du certificat.
- Le représentant légal de l'organisation identifiée dans le certificat.

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

Les **personnes autorisées** à demander la **révocation d'un certificat d'AC** sont les suivantes :

- Le Responsable de l'AC.
- Une Autorité judiciaire via une décision de justice.

La révocation des certificats de **composantes de l'IGC** est décidée par le **Responsable de l'AC**.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat de serveur

La révocation d'un certificat de serveur se déroule par les canaux suivants :

- **Via le logiciel d'AE**.
- Par la transmission à l'AE d'un **formulaire de révocation** par courrier, par mail, ou en face-à-face.

Toutes les personnes autorisées mentionnées au paragraphe 4.9.2 peuvent faire leur demande via le formulaire de révocation. Le logiciel d'AE peut être utilisé uniquement par les opérateurs d'enregistrement, le RC, le représentant légal.

Le demandeur de la révocation est authentifié par l'AE selon les règles définies au paragraphe 3.4.

Quel que soit le canal, la demande de révocation doit comporter les informations suivantes :

- Le numéro de série et le nom du certificat (contenu du champ Common Name) à révoquer.
- L'AC émettrice du certificat.
- L'adresse email et un numéro de téléphone du demandeur de la révocation.

La demande de révocation de certificat est traitée par l'AE dans les délais indiqués au paragraphe 4.9.5. Le demandeur de la révocation ainsi que le RC sont notifiés par l'AE en cas de validation de la demande de révocation et en cas d'invalidation de la demande de révocation.

Si la demande de révocation est validée par l'AE, la révocation de certificat par l'AC est prise en compte par l'AC. La prochaine CRL mentionnera le certificat révoqué.

La demande de révocation et son traitement sont journalisés au niveau du logiciel d'AE.

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

La révocation d'un **certificat d'AC émane du responsable de l'AC** comme indiqué au paragraphe 4.9.2.2. Elle est **mise en œuvre par le responsable d'application** (voir la définition des rôles de confiance au paragraphe 5.2.1).

En cas de besoin de révoquer le certificat d'AC, l'AC informera le point de contact ANSSI identifié sur le site http://ssi.gouv.fr, ainsi que tous les RC, soit au préalable, soit dès que possible.

La révocation d'un **certificat d'une composante de l'IGC** est **demandée par le RC correspondant** et mise en œuvre par l'AE correspondante (selon la PC applicable au certificat).

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

Le RC formule sa demande de révocation sans délai, 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 de serveur

Une demande de révocation doit être traitée en urgence.

4.9.5.2. Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations est disponible les jours ouvrés (lundi au vendredi), sur les heures ouvrées (9h à 19h).

La fonction de gestion des révocations a une **durée maximale d'indisponibilité par interruption de service** (panne ou maintenance) de 2 heures, les jours ouvrés.

La fonction de gestion des révocations a une **durée maximale totale d'indisponibilité par mois** de 16 heures, les jours ouvrés.

L'AC s'engage à traiter les demandes de révocation de certificats de serveur dans un délai inférieur à 72 heures (délai compris entre la réception de la demande de révocation authentifiée, et la mise à disposition de l'information de révocation auprès des utilisateurs).

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

La révocation d'un certificat d'une composante doit être effectuée dès la détection de l'évènement décrit dans les causes de révocations.

En particulier, la révocation d'un certificat d'AC doit être effectuée immédiatement, notamment en cas de compromission de clé.

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

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

Pour cela, l'AC publie des Listes de Certificats Révoqués (LCR, ou CRL).

4.9.7. Fréquence d'établissement et durée de validité des CRL

La fréquence minimale de publication des CRL, par rapport aux exigences du RGS niveau*, est de 72 heures.

En pratique, **l'AC établit des nouvelles CRL toutes les 8 heures.**

Chaque CRL est valable 72 heures.

4.9.8. Délai maximum de publication d'une CRL

Les CRL sont publiées au maximum 30 minutes après sa 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, qu'il s'agisse d'un certificat de serveur ou d'AC, est une cause de révocation, et doit être traitée comme telle dans les meilleurs délais (voir paragraphe 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.

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 met les CRL à disposition de tous les utilisateurs via son site de publication.

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

L'AC publie également sur son site de publication son certificat d'AC et son empreinte, ce qui permet aux utilisateurs de vérifier la validité de la signature des certificats de serveur.

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 la relation contractuelle entre l'AC et la personne morale identifiée dans le DN du certificat de serveur se termine, alors le certificat de serveur doit être révoqué. La clé privée correspondante sera supprimée.

Dans le cas où il n'existe plus de RC explicitement identifié pour un certificat de serveur, 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 SECURITE 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 AriadNEXT 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.

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 paragraphe 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 paragraphe 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 paragraphe 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.

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 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**.

Les contrôles de conformité (voir paragraphe 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 paragraphe 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

Non applicable.

Tout le personnel intervenant sur les composantes de l'IGC est interne.

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 PKI_POL_TRACABILITE 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 (voir PKI_POL_TRACABILITE).

La politique de traçabilité PKI_POL_TRACABILITE 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 PKI_POL_TRACABILITE 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 qui est archivé.
- **Un rapprochement entre les journaux d'événements** est effectué **une fois par semaine.**

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'AriadNEXT 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 chapitre 6.8.

5.4.5. Procédure de sauvegarde des journaux d'événements

La PSSI d'AriadNEXT 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.

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 paragraphe 5.4.2.

5.5. Archivage des données

5.5.1. Types de données à archiver

L'AC a défini une politique d'archivage PKI_POL_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 PKI_POL_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 PKI_POL_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 paragraphe 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 PKI_POL_ARCHIVAGE garantit qu'une archive peut être récupérée dans un délai inférieur à 2 jours ouvrés.

La politique d'archivage PKI_POL_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 « Legal Person CA G2 » est de 10 ans.

La durée de vie des certificats émis par l'AC est de :

- **3 ans** pour les certificats de **cachet qualifié.**
- **3 ans** pour les certificats d'**horodatage qualifié.**

Afin de permettre aux utilisateurs de vérifier l'origine des certificats de serveur, à tout moment de la vie du certificat, l'AC choisit de ne plus émettre de certificats 3 ans avant sa date de fin de validité.

Une nouvelle AC sera créée afin de maintenir la continuité du service. La nouvelle clé privée de cette AC (et seulement cette nouvelle clé) sera utilisée pour signer les nouveaux certificats de serveur.

L'ancien certificat d'AC servira à valider les certificats émis par la première AC. La publication des CRL correspondant à l'ancienne AC sera maintenue jusqu'à expiration du dernier certificat émis par l'ancienne AC.

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 : http://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 une fois tous les 3 ans.

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

Le cas de compromission 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 paragraphe 4.9.1.2).

De plus, l'AC informe de la compromission tous les RC 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 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 RC 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 surwww.ssi.gouv.fr.
    - 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 et ses clients et utilisateurs de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2. Cessation d'activité affectant l'AC

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

La cessation partielle d'activité 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.
- Le transfert des activités d'exploitation à d'autres parties.
- La gestion du statut de révocation pour les certificats non expirés qui ont été délivrés.

Lors de l'arrêt du service :

1. L'AC s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats.
2. L'AC prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante.
3. L'AC révoque son certificat.

4. L’AC révoque tous les certificats qu’elle a signés et qui seraient encore en cours de validité.
5. L’AC informe les RC des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6. MESURES DE SECURITE TECHNIQUES

6.1. Génération et installation des bi clés

6.1.1. Génération des bi clés

6.1.1.1. Clés d'AC

La génération de la clé de signature de l'AC est effectuée dans un environnement sécurisé.

La génération de la clé de signature de l'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (voir paragraphe 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 une personne ayant un rôle de confiance, et en présence de plusieurs témoins.** 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 est générée et mise en œuvre dans un module cryptographique qualifié au moins au niveau élémentaire, conformément aux exigences du RGS* (une étoile).

La génération de la clé de signature de l'AC nécessite au préalable la génération de parts de secrets de l'AC. La réunion du quorum des porteurs de parts de secrets permettra ainsi de restaurer la bi-clé de l'AC 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 serveurs générées par l'AC

Sans objet.

6.1.1.3. Clés serveurs générées au niveau du serveur

La première bi-clé doit être générée après la procédure d'initialisation du dispositif de protection des clés privées.

Dans le cas où l'AC remet le dispositif de protection des clés privées au RC, ce dispositif de protection des clés privées est **qualifié conformément aux exigences du RGS*** (une étoile). Le RC en charge du serveur s'engage, via la signature des conditions générales d'utilisation, à générer la clé privée dans ce dispositif de protection des clés privées qualifié remis par l'AC.

Dans le cas où l'AC ne remet pas le dispositif de protection des clés privées au RC, le RC en charge du serveur s'engage, via la signature des conditions générales d'utilisation, à générer la clé privée dans un **dispositif de protection des clés privées certifié au moins au niveau 2 selon la norme FIPS 140-2**.

6.1.2. Transmission de la clé privée au serveur

Sans objet.

6.1.3. Transmission de la clé publique à l'AC

La transmission de la clé publique du serveur vers l'AC doit permettre :

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

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

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

De plus, l'AC 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 les suivantes :

- Clés des serveurs : 2048 bits.
- Clés de l'AC : 4096 bits.

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 génération des certificats d'entité finale sont les suivants :

- Algorithme d'empreinte : SHA-256
- Algorithme de signature : RSA

Voir le paragraphe 7 pour les profils de certificats.

6.1.7. Objectifs d'usages de la clé

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

L'utilisation d'une clé privée de serveur est limitée au service de signature de type cachet (pour le profil « Cachet qualifié ») ou de signature de jetons d'horodatage (pour le profil « Horodatage qualifié ») délivré par ce serveur.

Voir le paragraphe 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

La bi-clé d'AC est générée et mise en œuvre dans un module cryptographique qualifié comme indiqué au paragraphe 6.1.1.1.

6.2.1.2. Dispositifs de protection des clés privées des serveurs

Les clés des certificats d'entité finale sont générées et conservées dans des dispositifs de protection des clés privées qualifiés au regard du RGS* ou certifiés selon la norme FIPS 140-2 niveau 2 (voir paragraphe 6.1.1.3).

Si l'AC ne fournit pas le dispositif de protection des clés privées au RC, elle s'assure auprès du RC de la conformité du dispositif mis en œuvre par le serveur, au travers d'un engagement contractuel du RC vis-à-vis de l'AC (indiqué dans les CGU).

Si l'AC fournit le dispositif de protection des clés privées au RC, elle s'assure que :

- La préparation des dispositifs de protection des clés privées est contrôlée de façon sécurisée.
- Les dispositifs de protection des clés privées sont stockés et distribués de façon sécurisée.
- Les désactivations et réactivations des dispositifs de protection des clés privées sont contrôlées de façon sécurisée.

6.2.2. Contrôle de la clé privée par plusieurs personnes

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

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

Les porteurs de secrets sont des porteurs de rôle de confiance (voir paragraphe 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 et des serveurs font l'objet d'une copie de secours.

Ces copies de secours sont effectuées hors du module cryptographique (respectivement dispositif de protection des clés privées). 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 paragraphe 6.2.2.

6.2.5. Archivage de la clé privée

Les clés privées 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 ou dans le dispositif de protection des clés privées.

La mise en œuvre d'une copie de secours dans un module cryptographique ou dans le dispositif de protection des clés privées respecte les exigences du paragraphe 6.2.4.

6.2.7. Stockage de la clé privée dans un module cryptographique

Voir paragraphes 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

L'activation de la clé privée d'AC dans le module cryptographique est contrôlée par des **données d'activation** (voir paragraphe 6.4.1.1), et fait intervenir **deux porteurs de secret.**

6.2.8.2. Clés privées des serveurs

L'activation de la clé privée du service applicatif dans le dispositif de protection des clés privées est contrôlée par des **données d'activation** (voir paragraphe 6.4.1.2).

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clés privées d'AC

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 permettent de répondre aux exigences de la qualification du module cryptographique citée au paragraphe 6.1.1.1.

6.2.9.2. Clés privées des serveurs

Dans le cas où l'AC fournit le dispositif de protection des clés privées :

- La désactivation des clés privées dans le dispositif de protection des clés privées est automatique dès que le dispositif s'arrête.
- Les conditions de désactivation des clés privées du service applicatif permettent de répondre aux exigences propres à la qualification du dispositif de protection des clés privées (citée au paragraphe 6.1.1.3).

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Clés privées d'AC

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

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

6.2.10.2. Clés privées des serveurs

En fin de vie d'une clé privée de serveur, cette clé est détruite ainsi que ses copies.

Dans le cas où l'AC fournit le dispositif de protection des clés privées, la méthode de destruction permet de répondre aux exigences de la qualification du module cryptographique (citée au paragraphe 6.1.1.3).

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection des clés privées

Voir paragraphes 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 et les clés publiques des services applicatifs sont archivées dans le cadre de la politique d'archivage PKI_POL_ARCHIVAGE des certificats (voir paragraphe 5.5).

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

Voir le paragraphe 5.6 pour les durées de vie des certificats et pour les modalités de renouvellement du certificat de l'AC.

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

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

Les **données d'activation** correspondant à la clé privée du service applicatif sont générées pendant la phase d'initialisation et de personnalisation du module, **au cours de la procédure d'initialisation du dispositif de protection des clés privées** (voir paragraphe 6.1.1.3).

Les données d'activation sont choisies et saisies par les **porteurs de rôle de confiance** correspondants pendant la procédure d'initialisation du dispositif de protection des clés privées.

6.4.2. Protection des données d'activation

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

Les données d'activation correspondant à la clé privée de l'AC sont conservées de manière à en assurer la disponibilité, l'intégrité, et la confidentialité.

Voir DPC.

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

Les données d'activation des dispositifs de protection des clés privées des services applicatifs sont conservées de manière à en assurer la disponibilité, l'intégrité, et la confidentialité.

Voir DPC.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

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. paragraphe 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.

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

Voir le document PKI_CERT_PROFILS.

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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.

Les audits de qualification de l'AC propres au statut de Prestataire de Service de Certification Electronique (PSCE) ne sont pas traités ici.

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 trois 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 sera 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 PROBLEMATIQUES METIERS ET LEGALES

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

La fourniture et le renouvellement des certificats émis par les AC AriadNEXT sont soumis à tarification. Les tarifs sont consultables directement auprès d'AriadNEXT.

9.1.2. Tarifs pour accéder aux certificats

Non applicable. Les certificats ne sont pas publiés.

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 est libre et gratuit.

9.1.4. Tarifs pour d'autres services

Sans objet.

9.1.5. Politique de remboursement

Les demandes de remboursement doivent être adressées directement à AriadNEXT.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

AriadNEXT 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 partie non-publique de la DPC de l'AC.
- Les clés privées de l'AC, des composantes et des serveurs.

- Les données d'activation associées aux clés privées d'AC et des serveurs.
- Tous les secrets de l'IGC.
- Les journaux d'évènements des composantes de l'IGC.
- Les dossiers d'enregistrement des serveurs et des RC.
- Les causes de révocations, sauf accord explicite du RC.

9.3.2. Informations hors du périmètre des informations confidentielles

Voir paragraphe 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 paragraphe 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 des RC à des tiers dans le cadre de procédures légales. Elle s'engage également à donner l'accès au dossier d'enregistrement au RC et à son représentant légal.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

L'AC respecte la loi n°78-17 « Informatique et Libertés ».

Le droit d'accès, de rectification ou d'opposition des données à caractère personnel conformément à la loi « Informatique et Libertés » peut être exercé par les personnes concernées auprès d'AriadNEXT.

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

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

9.4.3. Informations à caractère non personnel

Voir paragraphe 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 RC à l'AC ne seront ni divulguées ni transférées à un tiers sauf dans les cas suivants :

- Consentement préalable du RC.
- 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. chapitre 8) et l'organisme de qualification.
- Respecter les accords ou contrats qui les lient entre elles ou aux RC.
- 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 un RC donné et que ce RC a accepté le certificat, conformément aux exigences du paragraphe 4.4.
- Tenir à disposition des Porteurs, des RC, 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 RC 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 RC et l'AC est formalisée dans les Conditions Générales d'Utilisation (intégrées dans le formulaire de demande) signés par le RC, précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa PC avec les exigences du RGS. 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 RC.
- 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. RC

Le RC a l'obligation de :

- Générer la Bi-Clé du serveur dans le dispositif de protection des clés privées remis par l'AC ou certifié selon la norme FIPS 140-2 au moins au niveau 2.
- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat (ainsi que toutes les pièces justificatives nécessaires) et informer immédiatement l'AE ou l'AC de toute modification de celles-ci.
- Protéger la Clé Privée du service applicatif dont il a la responsabilité par des moyens appropriés à son environnement.

- Protéger les données d'activation de cette clé privée et le cas échéant les mettre en œuvre.
- Protéger l'accès à la base de certificats du service applicatif.
- Respecter les conditions d'utilisation de la Clé privée du service applicatif et du Certificat correspondant.
- Informer l'AC de toute modification concernant les informations contenues dans le certificat électronique.
- Faire sans délai, une demande de révocation de son certificat auprès de l'AC ou de l'AE en cas de compromission ou de suspicion de compromission de sa clé privée ou de ses données d'activation.

La relation entre le RC et l'AC ou l'AE est formalisée par un engagement du RC visant à certifier l'exactitude des renseignements et des documents fournis (signature des conditions générales d'utilisation dans le formulaire de demande).

9.6.4. 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.

9.6.5. Autres participants

Sans objet.

9.7. Limite de garantie

Les responsabilités des clients et les garanties sont précisées dans les conditions générales d'utilisation.

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. paragraphe 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 cités au cours du paragraphe 9.

9.16. Dispositions diverses

9.16.1. Accord global

Pas d'exigence particulière.

9.16.2. Transfert d'activités

Voir paragraphe 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.