Politique de certification des échanges du Portail AGATE

SER-POL-CERT-AGATE

Résumé

Ce document décrit la politique de certification (PC) de l'autorité de certification (AC) de l'AC Portail AGATE de Strasbourg Électricité Réseaux. Il est le référentiel technique listant les règles de délivrance des certificats électroniques émis par l'AC Portail AGATE.

Version	Date de la version	Nature de la modification
V 1.0	30 avril 2021	Création du document

SOMMAIRE

1. Introduction

1.1. Présentation générale

Ce document décrit la politique de certification (PC) de l'autorité de certification (AC) de l'AC Portail AGATE de Strasbourg Électricité Réseaux. Il est le référentiel technique listant les règles de délivrance des certificats électroniques émises par l'AC Portail AGATE.

L'AC Portail AGATE permet la signature des certificats utilisateurs donnant accès au Portail AGATE du distributeur Strasbourg Électricité Réseaux.

Le Portail AGATE est accessible via le site www.strasbourg-electricite-reseaux.fr du distributeur Strasbourg Électricité Réseaux.

Les certificats électroniques délivrés dans le cadre de ce document concernent uniquement Strasbourg Électricité Réseaux et ses utilisateurs. Ces certificats électroniques sont exclusivement destinés à l'authentification des utilisateurs du Portail AGATE.

Tout autre usage ou certificat est hors périmètre.

La présente PC s'appuie sur les principes indiqués dans la [**RFC3647**].

1.2. Identification du document

Strasbourg Électricité Réseaux ne disposant pas d'un OID, aucun identifiant d'objet n'est attribué à présente politique.

Le tableau ci-dessous résume l'identification de cette Politique de Certification :

Nom	Politique de Certification de l'Autorité de Certification Portail AGATE de Strasbourg Électricité Réseaux
Version	Projet du 19/04/2021

1.3. Acronymes et définitions

1.3.1. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC / CA	Autorité de Certification / *Certification Authority*
AE / RA	Autorité d'Enregistrement / *Registration Authority*
DN	*Distinguished Name*
DNS	*Domain Name System*
DPC/CPS	Déclaration des Pratiques de Certification / *Certification Policy Statement*
FQDN	*Fully Qualified Domain Name*
IGC / PKI	Infrastructure de Gestion de Clés / *Public Key Infrastructure*
LAR / ARL	Liste des certificats d'AC Révoqués / *Authority Revocation List*
LCR / CRL	Liste des Certificats Révoqués / *Certificate Revocation List*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
PC / CP	Politique de Certification / *Certificate Policy*
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*

1.3.2. Définitions

Les termes utilisés dans la présente PC sont les suivants :

Autorité de certification (AC) - Une Autorité de Certification a en charge l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur, dans les certificats émis au titre de cette politique de certification.

Certificat électronique - Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire (personne physique ou service applicatif). Cette attestation prend la forme d'une signature électronique réalisée par un service de certification électronique. Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

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 protection des éléments secrets - Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au porteur (exemples : clé privée, code PIN, etc.). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique ou se présenter au format logiciel (exemple fichier PKCS#12).

FQDN (Fully Qualified Domain Name) - Nom de domaine pleinement qualifié indiquant la position absolue d'un nœud dans l'arborescence DNS et précisant les domaines de niveau supérieur jusqu'à la racine.

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.

Politique de certification (PC) - Ensemble de règles définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Porteur de certificat - Personne physique identifiée dans le certificat et qui est la détentrice de la clé privée correspondant à la clé publique.

Utilisateur de certificat - Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant d'un porteur de certificat ou chiffrer des données à destination d'un porteur de certificat.

1.4. Entités intervenant dans l'IGC

1.4.1. Autorité de certification

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

L'AC Portail AGATE est issue de l'autorité racine de la PKI Groupe ES. Cette racine est hors du périmètre de la présente PC. Elle est gérée uniquement par la succession de cérémonies de clés, pilotées par un expert sécurité, selon des scripts préalablement définis, devant témoin et faisant l'objet de procès-verbaux.

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

La décomposition fonctionnelle d'une IGC qui est retenue dans la présente PC est la suivante :

- *Autorité d'enregistrement (AE)* - Cette fonction vérifie et valide les informations d'identification du futur porteur, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat.

- *Fonction de génération des certificats* - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du service provenant du porteur.
- *Fonction de génération des éléments secrets du porteur* - Cette fonction génère les éléments secrets du service à destination et les prépare en vue de leur remise au porteur. De tels éléments secrets peuvent être, par exemple, directement la bi-clé, les codes (activation / déblocage) liés au dispositif de protection des éléments secrets ou encore des codes ou clés temporaires permettant de mener à distance le processus de génération / récupération du certificat électronique.
- *Fonction de remise* - Cette fonction remet au porteur au minimum le certificat du porteur ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif de protection des éléments secrets, clé privée, codes d'activation…).
- *Fonction de publication* - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides des services applicatifs et des porteurs.
- *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 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) ou selon un mode requête / réponse temps réel (OCSP).

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- *Porteur* - La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- *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).
- *Utilisateur de certificat* - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant porteur auquel le certificat est rattaché, ou pour établir une clé de session.
- *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, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

La Déclaration des Pratiques de Certification (DPC) de l'AC décrit l'organisation opérationnelle de son IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans sa PC.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- 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, notamment en matière de génération des certificats, de remise, 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.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle possède un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC porteurs 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

L'AE a pour rôle de vérifier l'identité du futur porteur. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur porteur, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

L'AE, en tant que de besoin, peut déléguer tout ou partie de ses fonctions à des unités de proximité désignées sous le nom d'autorités d'enregistrement déléguées (AED).

1.4.3. Responsables de certificats électroniques de services applicatifs

Sans objet dans le cadre de l'AC Portail AGATE.

1.4.4. Porteur de certificat

Dans le cadre de l'AC Portail AGATE, les porteurs sont principalement les utilisateurs du Portail AGATE de Strasbourg Électricité Réseaux. Quelques personnels de l'équipe support de Strasbourg Électricité Réseaux sont également susceptibles d'avoir besoin de certificats pour réaliser des tests sur le Portail AGATE.

Le porteur respecte les conditions qui lui incombent définies dans la PC de l'AC.

1.4.5. Utilisateurs de certificats

L'utilisateur (ou accepteur) des certificats électroniques issus de l'AC Portail AGATE est le Portail AGATE de Strasbourg Électricité Réseaux. Le Portail AGATE utilise le certificat présenté par l'utilisateur du Portail AGATE pour l'authentifier.

Attention : ne pas confondre l'utilisateur du Portail AGATE et l'utilisateur du certificat issu de l'AC Portail AGATE.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document. En particulier, l'AC respecte ses responsabilités envers les utilisateurs qui ont « raisonnablement » confiance dans un certificat.

1.4.6. Autres participants

1.4.6.1. Composantes de l'IGC

La décomposition en fonctions de l'IGC est présentée au 1.4.1 ci-dessus. Les composantes de l'IGC mettant en œuvre ces fonctions sont présentées dans la DPC de l'AC Portail AGATE.

1.4.6.2. Mandataire de certification

Pour chaque entité (Client signataire d'un contrat CARD ou Fournisseur) ayant accès au Portail AGATE, un ou plusieurs mandataires (utilisateurs référents) ont la responsabilité de créer des comptes pour les autres utilisateurs (utilisateurs membres) du Portail AGATE.

Ces mandataires sont définis au moment de la signature du contrat, et sont créés directement par Strasbourg Électricité Réseaux. Ils ont en charge de spécifier ; via le Portail AGATE, différentes informations dont l'adresse email qui sera ensuite utilisée pour la récupération des identifiants et du certificat par l'utilisateur.

1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

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

L'AC génère et signe différents types d'objets : certificats, LCR / LAR ou des réponses OCSP.

Pour signer ces objets, l'AC dispose d'une seule bi-clé.

Les bi-clé et certificat de l'AC pour la signature de certificats, de LCR / LAR ou de réponses OCSP ne sont utilisés qu'à cette fin. Ils ne sont notamment utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

1.5.1.2. Bi-clés et certificats de de porteurs

L'unique usage des certificats de porteur est l'authentification du porteur auprès du Portail AGATE, dans le cadre de l'établissement de sessions sécurisées, de type TLS visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

L'établissement de la clé de session doit se faire par un mécanisme à l'état de l'art.

1.5.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous. L'AC respecte ces restrictions et impose leur respect par les porteurs auxquels elle délivre des certificats et les utilisateurs de ces certificats.

À cette fin, elle communique à tous les porteurs et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

Tout usage à destination du grand public de certificat produit par l'AC Portail AGATE est interdit.

1.6. Gestion de la PC

1.6.1. Entité gérant la PC

Le RSSI du Groupe ÉS est responsable de la validation et de la gestion de la PC.

1.6.2. Point de contact

Afin d'obtenir des informations sur la présente PC, il est possible d'envoyer un courrier électronique avec des questions ou commentaires à l'adresse « grd.accueil.contrats@strasbourg-electricite-reseaux.fr».

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

Le RSSI du Groupe ÉS a l'autorité et la responsabilité finale pour déterminer la conformité de la DPC avec la PC.

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

La procédure d'approbation de la conformité d'une DPC est identifiée dans la DPC concernée.

Le responsable d'exploitation SI du Groupe ÉS est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC suit le processus d'approbation mis en place.

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

2.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des porteurs et utilisateurs de certificats, l'AC met en œuvre au sein de l'IGC une fonction de publication et une fonction d'information sur l'état des certificats.

La fonction de publication et d'information sur l'état des certificats s'appuie sur :

- La génération de LCR mises à disposition sur un service web ;
- Un service OCSP.

L'utilisation des certificats issus par l'AC Portail AGATE étant exclusivement faite sur des serveurs de l'infrastructure informatique du Groupe ÉS, les deux types d'informations précédents sont disponibles uniquement sur des URL internes au Groupe ÉS.

La diffusion des informations de révocation est réalisée automatiquement par l'infrastructure mise en œuvre. Il est de la responsabilité du service de publication de s'assurer de la mise à jour de ces informations sur les points de publication web de mise à disposition des LCR.

2.2. Informations devant être publiées

L'AC publie les informations suivantes à destination des **utilisateurs** de certificats :

- Sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647] ;
- L'état des certificats émis par chaque AC, selon le ou les moyens indiqués dans la PC ;
- Le certificat de AC en cours de validité ;
- Pour l'AC Racine, les informations permettant aux utilisateurs de certificats de s'assurer de l'origine de ces certificats et de leur état.

L'AC publie les informations suivantes à destination des **porteurs** de certificats :

- Sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647].

L'AC propose également aux porteurs les moyens nécessaires pour la gestion des certificats (demande d'enregistrement, de renouvellement, de révocation, etc.).

2.3. Délais et fréquences de publication

Les informations liées à l'IGC sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version est communiquée au porteur lors d'une demande de renouvellement. Les systèmes publiant ces informations sont au moins disponibles les jours ouvrés.

Le certificat d'AC est diffusé préalablement à toute diffusion de certificats de porteur et/ou de LCR correspondants et les systèmes les publiant sont disponibles 24h/24 et 7j/7.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres 4.9 et 4.10.

2.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe longs basé sur une politique de gestion stricte des mots de passe.

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (« issuer ») et le porteur (« subject ») sont identifiés par un « Distinguished Name » (DN) répondant aux exigences de la norme [X.501].

Les formats sont précisés au chapitre 0.

3.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les services applicatifs et les porteurs dans les certificats doivent être explicites dans le contexte du Portail AGATE.

Les noms sont précisés au chapitre 0.

3.1.3. Anonymisation ou pseudonymisation des services applicatifs

L'anonymisation et la pseudonymisation ne sont pas mises en œuvre dans le cadre de l'AC Portail AGATE.

3.1.4. Règles d'interprétation des différentes formes de nom

Les significations des différents champs du DN des certificats des AC sont décrites au chapitre 0.

3.1.5. Unicité des noms

Le DN du champ « subject » de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.

Durant toute la durée de vie d'une AC, un DN attribué à un porteur de certificats ne peut être attribué à un autre porteur. La DPC précise les modalités associées à cette exigence.

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

3.1.6. Identification, authentification et rôle des marques déposées

La présente PC ne formule pas d'exigence spécifique sur le sujet.

L'AC est responsable de l'unicité des noms des porteurs utilisés dans ses certificats et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

Sans objet dans le cadre de l'AC Portail AGATE : les bi-clés sont fournies par l'AC.

3.2.2. Validation de l'identité d'un organisme

L'identité des organisations utilisatrices du Portail AGATE est validée contractuellement.

3.2.3. Validation de l'identité d'un individu

Les porteurs mandataires sont définis au moment de la signature du contrat avec Strasbourg Électricité Réseaux.

L'enregistrement d'un porteur non-mandataire pour lequel un certificat doit être délivré est réalisé par les mandataires de chaque organisation, selon des modalités propres à chaque organisation et sous la responsabilité de ladite organisation.

L'authentification du demandeur repose sur la possession de l'accès à l'adresse de messagerie indiquée dans le contrat.

3.2.4. Informations non vérifiées du porteur

Sans objet dans le cadre de l'AC Portail AGATE.

3.2.5. Validation de l'autorité du demandeur

Le demandeur doit faire partie du listing des comptes autorisés auprès de Strasbourg Électricité Réseaux ou être autorisé par un mandataire (ce listing est fourni lors de la contractualisation).

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

Un nouveau certificat ne peut pas être fourni sans renouvellement de la bi-clé correspondante.

Le renouvellement de la bi-clé entraîne automatiquement la génération et la fourniture d'un nouveau certificat.

3.3.1. Identification et validation pour un renouvellement courant

Lors d'un renouvellement, l'AE, saisie de la demande, identifie et autorise la demande selon la même procédure que pour l'enregistrement initial ou offrant un niveau de garantie équivalent.

3.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial ou offrant un niveau de garantie équivalent.

De plus, la délivrance d'un nouveau certificat après une compromission ne peut avoir lieu sans :

- Analyse forensique et retour d'expérience ;
- Contrôle de la remise en condition de sécurité le cas échéant (réinstallation…).

3.4. Identification et validation d'une demande de révocation

Une demande de révocation doit être faite depuis le Portail AGATE via le renouvellement du certificat.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Un certificat doit être demandé par le futur porteur, par un mandataire ou par l'équipe métier de Strasbourg Électricité Réseaux.

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

La seule information nécessaire à la demande de certificat est l'adresse email.

Organisation, prénom et nom, et RTPL (Référence Technique du Point de Livraison) sont également demandées lors de la création du compte de l'utilisateur du Portail AGATE, mais ils ne sont pas utilisés pour la création du certificat.

4.2. Traitement d'une demande de certificat

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

Les identités sont vérifiées conformément aux exigences du chapitre 3.2.

L'autorisation à établir un certificat d'utilisateur du Portail AGATE est déléguée aux contacts précisés dans le contrat avec Strasbourg Électricité Réseaux.

Les autorisations sont traitées manuellement et unitairement par l'AE.

L'AE effectue les opérations suivantes :

- Valider l'identité du futur porteur ;
- Vérifier la cohérence de la demande ;
- S'assurer que le futur porteur a connaissance des modalités applicables pour l'utilisation du certificat ;
- Vérifier que le format des noms demandés respecte les contraintes techniques (espaces, caractères spéciaux) et les contraintes fonctionnelles (nom de domaine, ordre prénom/nom, etc.).

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le porteur en justifiant le rejet.

4.2.3. Durée d'établissement du certificat

La présente PC ne formule pas d'exigence spécifique sur le sujet.

4.3. Délivrance du certificat

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

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, le porteur est notifié par message électronique. Une URL lui est transmise permettant d'aller venir générer de manière synchrone son certificat. L'IGC déclenche alors le processus de génération du certificat complet et exact. La délivrance est immédiate.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 0 et 5 ci-dessous, notamment la séparation des rôles de confiance.

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

L'établissement du certificat déclenche une notification du porteur par mail.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation est tacite à compter de la date de délivrance du certificat au porteur.

4.4.2. Publication du certificat

Les certificats sont disponibles auprès de l'AC pour l'équipe de support du Portail AGATE.

Ils ne sont pas publiés dans un service tiers du SI du Groupe ÉS.

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

Sans objet dans le cadre de l'AC Portail AGATE.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat

L'utilisation de la clé privée et du certificat associé est strictement limitée à la fonction de sécurité concernée. Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés. Cet usage est également clairement explicité dans la présente PC.

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

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6. Renouvellement d'un certificat

Conformément au [**RFC3647**], la notion de « renouvellement de certificat » correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique).

Dans la cadre de l'AC Portail AGATE, le renouvellement de certificat sans renouvellement de la bi-clé correspondante est interdit.

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

Conformément au [**RFC3647**], ce chapitre traite de la délivrance d'un nouveau certificat électronique liée à la génération d'une nouvelle bi-clé.

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

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés, et les certificats correspondants, sont renouvelés au minimum à une fréquence définie au point 6.3.2. Une bi-clé et un certificat peuvent être renouvelés par anticipation.

Une bi-clé et un certificat peuvent être renouvelés également suite à une révocation. Les causes possibles peuvent être les suivants :

- Perte ou vol du support de la clé privée ;
- Compromission ou suspicion de compromission de la clé privée.

Suite à la délivrance d'un nouveau certificat, le précédent certificat est automatiquement et instantanément révoqué (si le précédent certificat était encore valide).

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

Le déclenchement de la fourniture d'un nouveau certificat électronique est à l'initiative du porteur.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus.

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

Cf. chapitre 4.3.2.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1

4.7.6. Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8. Modification du certificat

Conformément au [**RFC3647**], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique et autres qu'uniquement la modification des dates de validité.

Dans la cadre de l'AC Portail AGATE, la modification de certificat sans renouvellement de la bi-clé correspondante est interdit.

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats de services applicatifs et de porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat électronique :

- Le certificat et sa bi-clé ont été renouvelés et le certificat a été accepté ;
- Les informations figurant dans le certificat ne sont plus en conformité avec l'identité du porteur, ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le porteur n'a pas respecté ses obligations découlant de la présente PC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées) ;
- Le porteur ou une entité autorisée demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) ;
- La cessation du contrat du porteur avec Strasbourg Électricité Réseaux.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné est révoqué.

4.9.1.2. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR et/ou de réponses OCSP) :

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

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats de porteurs

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

- Le porteur ou le mandataire de son organisation ;
- Un exploitant du service applicatif.
- Strasbourg Électricité Réseau

4.9.2.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC ne peut être décidée que par une décision conjointe du RSSI, du responsable métier et du responsable d'exploitation SI.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat électronique

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- L'identification du porteur figurant dans le certificat ;
- L'identification du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (AC et n° de série...) ;
- La cause de révocation.

Selon l'urgence et la situation, le responsable métier, responsable d'exploitation SI et le RSSI sont consultés.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

L'information de révocation est diffusée selon les solutions suivantes :

- Via une LCR signée par l'AC elle-même ou par une entité désignée par l'AC ;
- Via un service OCSP dont la réponse est soit signée par l'AC ayant émis le certificat à révoquer ou par un certificat de répondeur OCSP lui-même signé par l'AC ayant émis le certificat à révoquer.

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

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

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

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides.

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

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

4.9.5.1. Révocation d'un certificat électronique

Par nature, une demande de révocation est traitée en urgence.

4.9.5.2. Disponibilité du système de traitement des demandes de révocation

En jours ouvrés, la fonction de gestion des révocations a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures.

En jours ouvrés, cette fonction a une durée maximale totale d'indisponibilité par mois de 16 heures.

Toute demande de révocation d'un certificat porteur est traitée au plus tard à J+1 (ouvré). Ce délai s'entend 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 de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR ou de réponses OCSP) est effectuée dans les plus brefs délais après analyse, particulièrement dans le cas de la compromission de la clé.

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

L'utilisateur d'un certificat électronique est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

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

La fréquence minimale de publication des LCR de l'AC Portail AGATE est de 24 heures.

Une nouvelle LCR est publiée après chaque révocation.

La durée maximale de validité des LCR est de 6 jours.

Une LAR est un LCR qui ne contient que des certificats d'AC.

La LAR de l'AC racine est publiée tous les 12 mois, avec une durée maximale de validité de 18 mois.

4.9.8. Délai maximum de publication d'une LCR

Les LCR sont publiées et disponibles pour le téléchargement au maximum dans les 30 minutes suivant leur génération.

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

Un service OCSP est disponible et respecte les exigences d'intégrité, de disponibilité et de délai de publication décrites dans la présente PC.

4.9.10. Autres moyens disponibles d'information sur les révocations

Sans objet dans le cadre de l'AC Portail AGATE.

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

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

Pour les certificats d'AC, outre les exigences du chapitre ci-dessus, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement et largement diffusée.

4.9.12. Causes possibles d'une suspension

Dans la cadre de l'AC Portail AGATE, la suspension de certificats n'est pas autorisée.

4.9.13. Origine d'une demande de suspension

Sans objet dans la cadre de l'AC Portail AGATE.

4.9.14. Procédure de traitement d'une demande de suspension

Sans objet dans la cadre de l'AC Portail AGATE.

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

Sans objet dans la cadre de l'AC Portail AGATE.

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

4.10.1. Caractéristiques opérationnelles

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR ou des jetons OCSP et l'état du certificat de l'AC racine.

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats deux solutions : LCR et OCSP.

4.10.2. Disponibilité de la fonction d'information sur l'état des certificats

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

En jours ouvrés, cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures.

En jours ouvrés, cette fonction a une durée maximale totale d'indisponibilité par mois de 32 heures.

Le temps de réponse du serveur OCSP à la requête reçue est au maximum de 10 secondes.

4.10.3. Dispositifs optionnels

Sans objet dans la cadre de l'AC Portail AGATE.

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

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

4.12. Séquestre de clé et recouvrement

Dans la cadre de l'AC Portail AGATE, le séquestre des clés privées des services applicatifs est interdit.

Les clés privées d'AC ne sont pas non plus séquestrées.

4.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet dans la cadre de l'AC Portail AGATE.

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

Sans objet dans la cadre de l'AC Portail AGATE.

5. Mesures de sécurité non techniques

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

Les composantes de l'IGC sont situées dans les datacenters du Groupe ÉS.

5.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès physiques aux différentes composantes de l'IGC sont contrôlés.

En outre, aucune personne entrant dans ces zones physiquement sécurisées n'est laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

5.1.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles permettent également de respecter les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6. Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC maintient un inventaire de ces informations. L'AC met en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, clés USB, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7. Mise hors service des supports

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

Les procédures et moyens de destruction et de réinitialisation sont conformes à ce niveau de confidentialité.

5.1.8. Sauvegardes hors site

Une sauvegarde hors site est réalisée sur le site de repli de l'entreprise.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

L'IGC distingue les rôles fonctionnels de confiance suivants :

- *Responsable de sécurité* - Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. 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* - Le responsable d'application 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.
- *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 part de secret d'IGC* - Personne ayant la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

De manière générale, des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification. Ces rôles sont décrits et définis dans la description des postes, sur les principes de séparation des responsabilités et du moindre privilège.

L'AC implémente techniquement le principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

De plus, les opérations de sécurité de l'AC sont séparées des opérations normales. Les responsabilités des opérations de sécurité incluent :

- Les procédures et responsabilités opérationnelles ;
- La planification et la validation des systèmes sécurisés ;
- La protection contre les logiciels malicieux ;
- L'entretien ;

- La gestion de réseaux ;
- La surveillance active des journaux d'audit, l'analyse des évènements et les suites ;
- La manipulation et la sécurité des supports ;
- L'échange de données et de logiciels.

Ces responsabilités sont gérées par les opérations de sécurité de l'AC, mais peuvent être effectivement réalisées par du personnel opérationnel non spécialiste (en étant supervisé), tel que défini dans la politique de sécurité appropriée et les documents relatifs aux rôles et responsabilités.

Des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC soient sortis du site sans autorisation.

5.2.2. Nombre de personnes requises par tâche

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes.

La DPC de l'AC Portail AGATE précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

5.2.3. Identification et authentification pour chaque rôle

L'identité et les autorisations de toute personne amenée à travailler au sein de la composante sont contrôlées avant de lui attribuer un rôle et les droits correspondants, notamment :

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

Ces contrôles sont décrits dans la DPC de l'AC Portail AGATE.

Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit.

5.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Concernant les rôles de confiance, le cumul entre responsable de sécurité et ingénieur système est interdit.

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC.

5.3. Mesures de sécurité vis-à-vis du personnel

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis du Groupe ÉS.

Le Groupe ÉS s'assure que les attributions de ses personnels, amenés à travailler au sein d'une composante de l'IGC, correspondent à leurs compétences professionnelles.

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

L'AC informe toute personne intervenant dans des rôles de confiance de l'IGC :

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

En particulier, les personnels intervenant dans des rôles de confiance y sont formellement affectés par l'encadrement supérieur chargé de la sécurité.

5.3.2. Procédures de vérification des antécédents

La présente PC ne formule pas d'exigence spécifique sur ce sujet.

5.3.3. Exigences en matière de formation initiale

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

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

5.3.4. Exigences et fréquence en matière de formation continue

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

5.3.5. Fréquence et séquence de rotation entre différentes attributions

La présente PC ne formule pas d'exigence spécifique sur le sujet.

5.3.6. Sanctions en cas d'actions non autorisées

Tout personnel effectuant des actions non autorisées s'expose à des sanctions conformément au règlement interne du Groupe ÉS.

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC respectent également les exigences du présent chapitre 5.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8. Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, la présente PC lui est remise.

5.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1. Type d'évènements à enregistrer

Pour chaque composante de l'IGC, sont au minimum journalisés les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

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

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

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

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

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction...) ;
- Le cas échéant, génération des éléments secrets du porteur (bi-clé, codes d'activation…) ;
- Génération des certificats de porteur ;
- Transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs ;
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR (et éventuellement des deltaLCR) ou des, requêtes / réponses OCSP.

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

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat est enregistrée) ;
- Résultat de l'évènement (échec ou réussite).

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

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

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

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture est faite, sauf exception, le même jour ouvré que l'évènement.

5.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8 ci-dessous.

5.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant toute la durée de vie de l'AC Portail AGATE pour les évènements non-associés aux utilisateurs, et pendant la période de validité additionnée d'1 an pour les certificats des utilisateurs.

5.4.4. Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des évènements respecte les exigences du chapitre 6.8.

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

5.4.5. Procédure de sauvegarde des journaux d'évènements

Des mesures sont mises en place afin d'assurer l'intégrité et la disponibilité des journaux d'évènements.

5.4.6. Système de collecte des journaux d'évènements

La présente PC ne formule pas d'exigence spécifique sur le sujet.

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

La présente PC ne formule pas d'exigence spécifique sur le sujet.

5.4.8. Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont automatiquement analysés par un service de détection d'incident de sécurité, qui notifie le RSSI et le responsable exploitation SI en cas d'anomalie.

5.5. Archivage des données

5.5.1. Types de données à archiver

Des dispositions en matière d'archivage sont prises par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Il permet également la conservation des éventuelles pièces papier, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC et DPC ;
- Les certificats et LCR tels qu'émis ou publiés ;
- Les journaux d'évènements des différentes entités de l'IGC.

5.5.2. Période de conservation des archives

5.5.2.1. Dossiers de demande de certificat

Le dossier de demande de certificat est un sous ensemble du dossier de création de compte dans le Portail AGATE.

5.5.2.2. Certificats et LCR et réponses OCSP émis par l'AC

Les certificats de services applicatifs, de porteurs et d'AC, ainsi que les LCR / LAR, sont archivés pendant au moins une année après leur expiration.

5.5.2.3. Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 ne sont pas archivés au-delà de leur durée de conservation au sein de l'AC Portail AGATE.

5.5.2.4. Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre 5.4, aucune exigence n'est stipulée.

5.5.3. Protection des archives

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

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

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

5.5.4. Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes est au moins équivalent au niveau de protection des archives.

5.5.5. Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.

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

5.5.6. Système de collecte des archives

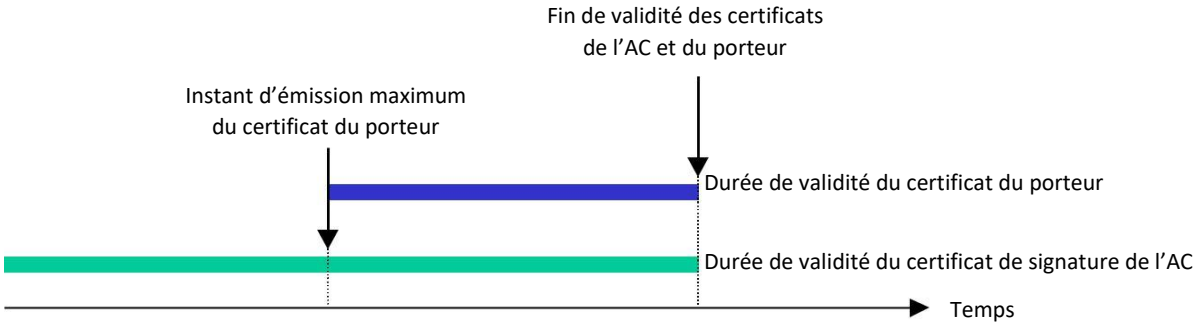
Le système de collecte des archives respecte les exigences de protection des archives concernées.

5.5.7. Procédures de récupération et de vérification des archives

Sans objet dans le cadre de l'AC Portail AGATE.

5.6. Changement de clé de l'AC

Une AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe.



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

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7. Reprise suite à compromission et sinistre

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

Des procédures et des moyens de remontée et de traitement des incidents sont mis en œuvre, notamment au travers de la sensibilisation et de la formation des personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens permettent de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements. Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui en informe immédiatement l'AC. Le cas de l'incident majeur est impérativement traité dès détection et 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.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

- Informe tous les porteurs et utilisateurs de certificats ;
- Révoque tout certificat concerné.

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

L'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan est testé au minimum une fois tous les 3 ans.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante en tant que sinistre.

Dans le cas de compromission de la clé d'AC, le certificat correspondant est révoqué dans les plus brefs délais après analyse.

En outre, l'AC respecte au minimum les engagements suivants :

- Informer les entités suivantes de la compromission : tous les porteurs et utilisateurs de certificats ;
- Indiquer 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

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC.

5.8. Fin de vie de l'IGC

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 :

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

De plus, dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire et, au moins, sous le délai d'un mois.

5.8.2. Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées aux 1) et 2) ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC assure la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC.

L'AC stipule dans sa DPC les dispositions prises en cas de cessation de service. Elles incluent :

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

Lors de l'arrêt du service, l'AC :

1. S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2. Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3. Révoque son certificat ;
4. Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
5. Informe tous les porteurs des certificats révoqués ou à révoquer.

6. Mesures de sécurité techniques

6.1. Génération et installation de bi-clés

6.1.1. Génération des bi-clés

6.1.1.1. Clé d'AC

La génération de la clé de signature de l'AC est effectuée dans un environnement sécurisé au sein de la solution d'IGC.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre de « cérémonies de clés ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

Les cérémonies de clés se déroulent sous le contrôle d'au moins une personne ayant au moins un rôle de confiance et en présence de témoin. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.1.2. Clés de porteur générées par l'AC

Les bi-clés sont générées par l'AC.

6.1.1.3. Clés de porteur générées au niveau du porteur

Sans objet dans le cadre de l'AC Portail AGATE.

6.1.2. Transmission de la clé privée au porteur

La clé privée est transmise au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. L'autorité de certification ne conserve ni ne duplique cette clé privée.

6.1.3. Transmission de la clé publique à l'AC

Sans objet dans le cadre de l'AC Portail AGATE.

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

La clé publique de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

La clé publique de l'AC racine est diffusée dans un certificat autosigné. La clé publique de l'AC Portail AGATE est diffusée dans un certificat signé par l'AC racine.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) peuvent être récupérées aisément par les utilisateurs de certificats.

6.1.5. Tailles des clés

Les clés de l'AC et des porteurs respectent les exigences de caractéristiques du document [RGS_B1].

La clé de l'AC sont des clés ECDSA de taille 256 bits, avec la courbe NIST P-256.

Les clés de porteurs sont des clés ECDSA de taille 256 bits, avec la courbe NIST P-256.

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. [RGS_B1]).

Les paramètres et les algorithmes utilisés sont documentés par l'AC.

6.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et de réponses OCSP (cf. [RGS_A4]).

L'utilisation de la clé privée du porteur, et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. [RGS_A4]).

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. Modules cryptographiques de l'AC

Sans objet dans le cadre de l'AC Portail AGATE.

6.2.1.2. Dispositifs de protection des éléments secrets du porteur

Les dispositifs de protection des clés privées des porteurs, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre **Erreur ! Source du renvoi introuvable.** ci-dessous.

L'AC s'assure auprès du porteur de la conformité du dispositif mis en œuvre, au minimum au travers d'un engagement clair et explicite.

6.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC Portail AGATE est assuré par du personnel de confiance.

6.2.3. Séquestre de la clé privée

Ni la clé privée de l'AC, ni les clés privées des porteurs ne sont en aucun cas séquestrées.

6.2.4. Copie de secours de la clé privée

La clé privée de l'AC fait l'objet de copies de secours. La protection de ces copies est au moins équivalente à la protection de la clé privée de l'AC utilisée par la solution d'IGC. Le chiffrement s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les règles définies dans le document [RGS_B1] sont respectées.

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

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

6.2.5. Archivage de la clé privée

La clé privée de l'AC n'est en aucun cas archivée.

Les clés privées des porteurs ne sont en aucun cas archivées ni par l'AC ni par aucune des composantes de l'IGC.

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

Tout transfert de la clé privée de l'AC se fait sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7. Stockage de la clé privée dans un module cryptographique

Sans objet dans le cadre de l'AC Portail AGATE.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clés privées d'AC

L'activation de la clé privée de l'AC est contrôlée via des données d'activation et fait intervenir au moins deux personnes ayant au moins un rôle de confiance.

La solution d'IGC stocke les clés privées de l'AC afin de permettre un redémarrage automatique et la continuité de la disponibilité des fonctions fournies.

6.2.8.2. Clés privées des porteurs

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clés privées d'AC

La désactivation de la clé privée d'AC est automatique lors de l'arrêt de la solution d'IGC.

6.2.9.2. Clés privées des services applicatifs et des porteurs

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.2.10. Méthode de destruction des clés privées

6.2.10.1.Clé privée d'AC

La méthode de destruction de la clé privée de l'AC permet de répondre aux exigences définies dans les chapitres **Erreur ! Source du renvoi introuvable.**.

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

6.2.10.2.Clés privées des services applicatifs et des porteurs

La présente PC ne formule pas d'exigence spécifique sur le sujet.

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

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

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

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

Les bi-clés et les certificats des porteurs couverts par la présente PC ont une durée de vie maximale de 730 jours.

La fin de validité du certificat d'AC est postérieure à la fin de vie des certificats de porteur qu'elle émet.

La durée de vie de la clé de signature d'AC et du certificat correspondant est de 11 ans. Cette durée de vie est cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés (cf. [RGS_B1]).

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

La génération et l'installation des données d'activation correspondant à la clé privée de l'AC se fait lors d'une cérémonie des clés. Les données d'activation sont définies directement par les porteurs de part de secret.

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

Sans objet dans le cadre de l'AC Portail AGATE.

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 porteurs de part de secret ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des données d'activation.

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

Les fichiers PKCS#12 transmis à un porteur sont protégés par un mot de passe défini par le porteur lui-même.

6.4.3. Autres aspects liés aux données d'activation

La présente PC ne formule pas d'exigence spécifique sur le sujet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC de l'AC. Il répond au moins aux objectifs de sécurité suivants :

- Identification et authentification des utilisateurs pour l'accès au système ;
- Gestion des droits des utilisateurs ;
- Gestion de sessions d'utilisation ;
- 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 ;
- Éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle font l'objet de mesures particulières.

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.

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

6.6.1. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation.

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

L'AC :

- Garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception ;
- Utilise des systèmes et des produits fiables qui sont protégés contre 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 apparait dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

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

La présente PC ne formule pas d'exigence spécifique sur le sujet.

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 la composante au sein de l'IGC.

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

De plus, des mesures particulières sont mises en place pour les échanges entre composantes au sein de l'IGC.

6.8. Horodatage / Système de datation

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC.

Pour dater ces évènements, les différentes composantes de l'IGC recourent à l'heure système de l'IGC en assurant 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.

7. Profils des certificats, OCSP et des LCR

7.1. Certificats d'utilisateur du Portail AGATE

7.1.1. Champs de base

Champs	Exigence
Version	« 2 », pour indiquer un certificat version 3
Serial number	Unique et non prédictible
Signature	SHA-256 avec chiffrement ECDSA
Issuer	C=FR, O=Strasbourg Electricite Reseaux, CN=Portail AGATE G1
Validity	730 jours à partir de la date d'émission
Subject	C=FR, O=Strasbourg Electricite Reseaux, OU=Portail AGATE, CN=<email>
Subject Public Key Info	ECDSA P-256, à renseigner
Unique Identifiers (issuer et subject)	Non utilisé
Extensions	Cf. chapitre suivant

7.1.2. Extensions

Champs	Critique	Exigence
Basic Constraints	O	cA : False
Key Usage	O	digitalSignature
Extended Key Usage	N	-
Authority Key Identifier	N	Obligatoire
Subject Key Identifier	N	Obligatoire
Certificate Policies	N	-
Subject Alternative Name Issuer Alternative Name	N	rfc822Name à renseigner

7.2. Liste de certificats révoqués

7.2.1. Champs de base

Champs	Exigence
Version	« 1 », pour indiquer une LCR version 2
Signature	SHA-256 avec chiffrement ECDSA
This Update	À renseigner
Next Update	Date d'émission + 6 jours
Revoked Certificates	À renseigner
Extensions	Cf. chapitre suivant

7.2.2. Extensions

Champs	Critique	Exigence
Authority Key Identifier	N	Obligatoire
Issuer Alternative Name	N	-
CRL Number	N	Obligatoire

8. Audit de conformité et autres évaluations

Les audits et les évaluations concernent ceux que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

La suite du présent chapitre ne concerne donc que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

8.1. Fréquences et / ou circonstances des évaluations

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

L'AC procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC tous les 3 ans.

8.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante est assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

8.3. Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et est dûment autorisée à pratiquer les contrôles visés.

8.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

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 respecte 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 sont tenus à la disposition de la direction de Strasbourg Électricité Réseaux.

9. Autres problématiques métiers et légales

9.1. Tarifs

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.2. Responsabilité financière

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La DPC de l'AC ;
- Toutes les clés privées, notamment celles de l'AC, des composantes, des serveurs et des porteurs ;
- Les données d'activation associées aux clés privées d'AC et des porteurs ;
- Tous les secrets de l'IGC ;
- Les journaux d'évènements des composantes de l'IGC ;
- Les causes de révocations, sauf accord explicite du porteur.

9.3.2. Informations hors du périmètre des informations confidentielles

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

L'AC respecte la législation et la réglementation en vigueur sur le territoire français.

9.4. Protection des données à caractère personnel

L'ensemble des données à caractère personnel sont sous la responsabilité du DPO du Groupe ÉS.

9.4.1. Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL] et le [RGPD].

9.4.2. Données à caractère personnel

Les données considérées comme personnelles sont au moins les suivantes :

- Les adresses électroniques des porteurs ;
- Les causes de révocation des certificats des services applicatifs et porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur).

9.4.3. Données à caractère non personnel

La présente PC ne formule pas d'exigence spécifique sur le sujet.

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

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

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

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne doivent être ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

9.4.6. Conditions de divulgation de données personnelles aux autorités judiciaires ou administratives

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

9.4.7. Autres circonstances de divulgation de données personnelles

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.5. Droits de propriété intellectuelle

La présente PC ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la 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 ;
- 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 et l'organisme de qualification ;
- Respecter les accords ou contrats qui les lient entre elles aux porteurs ;
- 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 a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que le porteur correspondant a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

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 les instances de haut niveau de l'AC.

9.6.2. Service d'enregistrement

Cf. les obligations pertinentes du chapitre 9.6.1.

9.6.3. Porteur

Le porteur a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger la clé privée 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 ;
- Respecter les conditions d'utilisation de la clé privée 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 du certificat électronique dont il est responsable auprès de l'AE ou de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

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 ;
- Pour chaque certificat de la chaîne de certification, du certificat du porteur 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

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.7. Limite de garantie

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.8. Limite de responsabilité

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.9. Indemnités

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

La PC de l'AC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2. Fin anticipée de validité

L'AC peut faire évoluer sa PC.

Cette évolution 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

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.11. Notifications individuelles et communications entre les participants

Sans objet dans le cadre de l'AC Portail AGATE.

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

L'AC contrôle que tout projet de modification de sa PC reste conforme aux exigences légales et règlementaires. 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

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

Aucun OID n'est défini pour cette PC.

Toute évolution de cette PC implique une évolution de son numéro de version.

9.13. Dispositions concernant la résolution de conflits

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.14. Juridictions compétentes

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.15. Conformité aux législations et réglementations

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

10. Références

10.1. Règlementation

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

10.2. Documents techniques

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 2.0
[RGS_A4]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0
[RGS_B1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007 et Corrigendum 2 de novembre 2008)

ANNEXE 1 : Exigences de sécurité des modules cryptographiques

Exigences sur les objectifs de sécurité

Sans objet dans le cadre de l'AC Portail AGATE.

Exigences sur la qualification

Sans objet dans le cadre de l'AC Portail AGATE.

ANNEXE 2 : Exigences de sécurité du dispositif de protection

Exigences sur les objectifs de sécurité

Le dispositif de protection des éléments secrets, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Garantir que la génération de la bi-clé est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Détecter les défauts lors des phases d'initialisation, et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- Garantir la confidentialité et l'intégrité des clés privées ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une authentification ou une fonction de sécurité qui ne peut être falsifiée sans la connaissance de la clé privée ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Exigences sur la qualification

La présente PC ne formule pas d'exigence spécifique sur le sujet.

(Fin du document)