Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre	Ministère du budget, des comptes publics et de la réforme de l'État
Agence nationale de la sécurité des systèmes d'information	Direction générale de la modernisation de l'État

Référentiel Général de Sécurité

version 1.0

Annexe A9

Politique de Certification Type

« Authentification Serveur »

Version 2.3 du 11 février 2010

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
06/11/2006	2.1	*Document constitutif de la Politique de Référencement Intersectorielle de Sécurité – PRISv2.1.*	DCSSI / SDAE
12/12/2008	2.2	*Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A9.* Modifications principales : • Réécriture d'exigences conformément à la norme ETSI TS 101456 ; • Introduction de la notion de qualification des produits de sécurité et des offres de prestataires de services de certification électronique conformément à l'ordonnance n° 2005-1516.	DCSSI / DGME
11/02/2010	2.3	*Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A9.* Modifications principales : • Suppression de la notion de référencement ; • Suppression de l'obligation pour l'AC de réaliser une analyse de risques pour les niveaux * et ** ; • Modification des exigences sur les certificats de recette / test ; • Modification des variables de temps (cf annexe A13) ; • Réécriture des exigences sur l'enregistrement d'une demande de certificat d'authentification serveur ; • Réécriture des chapitres III.2.6, III.3.1, VI.2.11, XI.2 et XII.2.	ANSSI / DGME

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

rgs@ssi.gouv.fr

Direction générale de la modernisation de l'État

Service Projets

64-70 allée de Bercy
75012 Paris

rgs.dgme@finances.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

Le présent document « Politique de Certification Type Authentification Serveur » (PC Type Authentification Serveur) fait partie du Référentiel Général de Sécurité [RGS]. Il en constitue l'annexe [RGS_A_9].

Ce référentiel technique liste les règles que les prestataires de service de certification électronique (PSCE) délivrant des certificats électroniques de type authentification de serveurs et d'établissement de sessions sécurisées doivent respecter. Les PSCE délivrant des certificats électroniques pour d'autres usages se reporteront aux PC Types associées, également en annexe du [RGS]. Dans le cadre de cette PC Type, les certificats sont à destination de serveurs informatiques[1] afin que ces serveurs puissent établir des sessions sécurisées (de type SSL / TLS) serveur / poste client et serveur / serveur : authentification du serveur et établissement d'une clé de chiffrement symétrique de session commune entre le serveur et le poste client ou entre les deux serveurs.

Dans le présent document, le terme « serveur » représente un ou plusieurs serveurs physiques détenant un même FQDN (fully qualified domain name).

Cette PC Type distingue trois niveaux de sécurité aux exigences croissantes : *, ** et ***. De manière à faciliter l'identification des différences entre les trois niveaux de sécurité définis pour les certificats, cette PC Type couvre ces trois niveaux. Les exigences spécifiques à un ou deux niveaux sont encadrées, le titre du cadre précisant le ou les niveaux auxquels l'exigence s'applique. Les exigences qui ne sont pas encadrées s'appliquent de manière identique aux trois niveaux.

Conformément à l'[Ordonnance], il est du ressort de l'autorité administrative (AA) de déterminer le niveau de sécurité ainsi que les fonctions de sécurité qu'elle souhaite mettre en place au sein de son SI. Elle peut, par conséquent, décider de recourir à la fonction de sécurité « Authentification Serveur » basée sur des mécanismes cryptographiques asymétriques nécessitant notamment l'usage de certificats électroniques. Le cas échéant, une fois le niveau de sécurité déterminé parmi (*), (**) et (***), l'autorité administrative doit utiliser des certificats électroniques d'authentification serveur délivrés par des PSCE conformes à la présente PC Type au dit niveau.

Un PSCE peut demander la qualification de son offre de services selon les modalités précisées dans le [DécretRGS][2]. Ce label permet d'attester de la conformité de l'offre du PSCE à un (ou plusieurs) niveau(x) de sécurité du présent référentiel.

La présente PC Type concerne à la fois les certificats de serveurs du secteur privé, de type "entreprises"[3], et ceux du secteur public. Les exigences spécifiques à l'un ou à l'autre de ces secteurs, lorsqu'elles existent, sont clairement identifiées en faisant précéder le paragraphe concerné respectivement par [ENTREPRISE] ou [ADMINISTRATION]. Dans la suite de la présente PC Type, le terme "entité" est utilisé pour désigner une entreprise ou une autorité administrative (cf. chapitre I.6.2).

De même, cette PC Type concerne les certificats pour des serveurs de type serveur SSL/TLS ou des serveurs qui lors de l'établissement d'une session sécurisée avec un autre serveur se trouve être en mode client. Les exigences spécifiques à l'un ou à l'autre de ces types de serveurs, lorsqu'elles existent, sont clairement identifiées en faisant précéder le paragraphe concerné respectivement par [SERVEUR-SERVEUR] ou [SERVEUR-CLIENT].

---

[1] Cf. définition de "serveur informatique" au chapitre I.6.2.

[2] En particulier, ce label est délivré par un organisme privé, accrédité par un organisme d'accréditation (le COFRAC en France) et habilité par l'ANSSI.

[3] La dénomination "entreprise" recouvre les entreprises au sens le plus large et également les personnes morales de droit privé : sociétés, associations ainsi que les artisans et les travailleurs indépendants.

Certaines exigences sont liées à des fréquences et/ou des délais. Ces fréquences et délais étant communs aux différentes PC Types, ils ont été regroupés, sous forme de variables de temps, dans un document séparé [RGS_A_13]. Une variable de temps est identifiée par une étiquette : par exemple, F_PUB_LCR correspond à la fréquence de publication des LCR. Dans la présente PC Type, ces étiquettes sont identifiées sous la forme "VT::Nom_Variable". De plus, la valeur de chaque variable dépend en général du niveau de sécurité. Ainsi, le lecteur de la présente PC Type doit substituer l'étiquette d'une variable de temps par la valeur dans [RGS_A_13] correspondant au niveau de sécurité considéré.

Les exigences, communes à tous les niveaux et particulières à un niveau donné, spécifiées dans la présente PC Type doivent être respectées intégralement par les PSCE moyennant l'exception suivante : dans la présente PC Type, un certain nombre de recommandations sont formulées. Les PSCE sont incités à les respecter également dès maintenant car ces recommandations, qui ne sont pas d'application obligatoire dans la présente version de ce document, devraient le devenir dans une version ultérieure.

Cette PC Type n'est pas une PC à part entière : elle ne peut pas être utilisée telle quelle par un PSCE en tant que PC pour être mentionnée dans ses certificats et sa DPC. Un PSCE souhaitant être qualifié par rapport à un des niveaux de sécurité de la présente PC Type doit en reprendre, dans sa propre PC, l'ensemble des exigences correspondant au niveau visé. Ceci dit, afin de faciliter l'utilisation de cette PC Type et son incorporation dans une PC complète, sa structure est totalement conforme au [RFC3647].

Afin de favoriser l'interopérabilité, dans le cadre de la sécurisation des échanges électroniques entre autorités administratives et usagers et entre autorités administratives, des règles et recommandations sur les formats de certificats et de listes de révocations, compatibles avec la norme [X.509] sont formulées dans le document [RGS_A_14].

I.2. Identification du document

La présente PC Type est dénommée "RGS - Politique de Certification Type - Authentification Serveur". Elle peut être identifiée par son numéro d'identifiant d'objet (OID - cf. page de garde et pied de page de chaque page). D'autres éléments, plus explicites, comme par exemple le nom, numéro de version, date de mise à jour permettent également de l'identifier.

Le numéro d'OID de cette PC Type est indiqué à titre de gestion documentaire. Il ne doit pas être utilisé dans les certificats. L'AC doit attribuer à sa propre PC, reprenant les exigences de la présente PC Type, un OID qui sera porté dans ses certificats correspondants.

Le numéro d'OID du présent document est : **1.2.250.1.137.2.2.1.2.2.5**

En réalité, le document correspond aux PC Types suivantes:

Service	Type de serveur	Niveau de sécurité	Type de certificat
Authentification Serveur	Serveur	*	Entreprise ou Administration
Authentification Serveur	Client	*	Entreprise ou Administration
Authentification Serveur	Serveur	**	Entreprise ou Administration
Authentification Serveur	Client	**	Entreprise ou Administration
Authentification Serveur	Serveur	***	Entreprise ou Administration
Authentification Serveur	Client	***	Entreprise ou Administration

Une PC correspond :

- à un service donné : authentification serveur
- à un type de serveur : serveur ou client
- un niveau de sécurité : *, ** ou ***

- un type de certificat : entreprise ou administration

Les exigences relatives aux certificats d'entreprise ou d'administration étant similaires, une même PC peut être utilisée pour ces 2 types de certificats.

Chaque PC doit être identifiée de manière non ambigüe. L'OID de la PC doit être changé dans des circonstances précisées au chapitre IX.12.3.

I.3. Entités intervenant dans l'IGC

I.3.1. Autorités de certification

La notion d'Autorité de Certification (AC) telle qu'utilisée dans la présente PC Type est définie au chapitre I.6.2 ci-dessous.

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).

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.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. [ETSI_NQCP]), la décomposition fonctionnelle d'une IGC qui est retenue dans la présente PC Type est la suivante[4] :

- **Autorité d'enregistrement (AE)[5]** - Cette fonction vérifie les informations d'identification du futur responsable du certificat d'authentification serveur (RCAS) et du serveur informatique auquel le certificat doit être rattaché, 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 revérification des informations du RCAS et/ou du serveur informatique lors du renouvellement du certificat de celui-ci.
- **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 serveur provenant soit du RCAS, soit de la fonction de génération des éléments secrets du serveur, si c'est cette dernière qui génère la bi-clé du serveur informatique.
- **Fonction de génération des éléments secrets du serveur** - Cette fonction génère les éléments secrets du serveur à destination du RCAS, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au RCAS (par exemple, personnalisation d'une carte à puce ou d'une carte cryptographique destinée au serveur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du serveur, les codes (activation / déblocage) liés au dispositif de protection de la clé privée du serveur ou encore des codes ou clés temporaires permettant au RCAS de mener à distance le processus de génération / récupération du certificat du serveur.

[4] Cette décomposition est donnée à titre d'illustration pour les besoins de la présente PC Type et n'impose aucune restriction sur la décomposition d'une implémentation effective d'une IGC.

[5] Les documents de l'ETSI, notamment [ETSI_NQCP], utilisent le terme Service d'Enregistrement. Le [RFC3647] utilise le terme Autorité d'Enregistrement. En cohérence avec ce dernier document, il est conservé l'utilisation du terme Autorité d'Enregistrement, mais qui doit être compris, dans la présente PC Type, en tant que fonction et non pas en tant que composante technique de l'IGC.

- **Fonction de remise au RCAS** - Cette fonction remet au RCAS au minimum le certificat du serveur ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif de protection de la clé privée du serveur, clé privée du serveur, 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 RCAS et/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 serveurs.
- **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) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

Les fonctions ci-dessus sont les fonctions minimales que doit obligatoirement mettre en œuvre une IGC gérant des certificats d'authentification serveur, à l'exception de la fonction de génération des éléments secrets du serveur qui est optionnelle et qui dépend des prestations effectivement offertes par l'AC.

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

- **Responsable du certificat d'authentification serveur (RCAS)** - La personne physique responsable du certificat d'authentification du serveur, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat.
- **Mandataire de certification (MC)** - 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 RCAS et des serveurs informatiques de cette entité (il assure notamment le face-à-face pour l'identification des RCAS 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 du serveur auquel le certificat est rattaché, ou pour établir une clé de session.
- **Personne autorisée** - Il s'agit d'une personne autre que le RCAS 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 RCAS (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du RCAS ou d'un responsable des ressources humaines.

L'organisation et l'ordonnancement des différentes fonctions de l'IGC les unes par rapport aux autres dépendent du modèle adopté par l'AC. La présente PC Type n'impose aucun modèle particulier, dans la limite où l'AC respecte les exigences qui y sont définies.

Cependant, les parties de l'AC concernées par la génération de certificat et la gestion des révocations doivent être indépendantes d'autres organisations en ce qui concerne leurs décisions concernant la mise en place, la fourniture, le maintien et la suspension des services ; en particulier, leurs cadres dirigeants, leur personnel d'encadrement et leur personnel ayant des rôles de confiance, doivent être libres de toute pression d'ordre commercial, financier ou autre, qui pourraient influer négativement sur la confiance dans les services fournis par l'AC. Les parties de l'AC concernées par la génération de certificat et de la gestion des révocations doivent avoir une structure documentée qui préserve l'impartialité des opérations.

L'organisation adoptée dépend notamment des prestations fournies par l'AC : génération ou non de la bi-clé du serveur, fourniture ou non du dispositif de protection de la clé privée du serveur et, si oui, fourniture avant ou après génération de la bi-clé du serveur, etc.

L'AC doit préciser dans sa PC les prestations effectivement fournies et son organisation fonctionnelle correspondante.

Dans la pratique, la mise en œuvre opérationnelle de ces fonctions peut être effectuée par une ou plusieurs composante(s) de l'IGC (opérateurs techniques et/ou autorités tel que OC, AE, SP, AH, …), qui peuvent être internes à l'AC et/ou opérées par des entités externes.

La Déclaration des Pratiques de Certification (DPC) de l'AC doit décrire 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.

Quelle que soit l'organisation opérationnelle mise en œuvre, l'AC reste in fine responsable vis-à-vis de toute partie externe à l'IGC (utilisateurs, autorités publiques, etc.) des prestations fournies et doit garantir le respect des engagements pris dans sa PC et sa DPC, relatifs à son activité de certification. Le cadre contractuel entre l'AC et ses différentes composantes opérées par des entités externes doit être clairement documenté.

En particulier, les politiques et les procédures, en fonction desquelles l'AC fonctionne, doivent être non-discriminatoires.

Le cadre contractuel entre l'AC et ses différentes composantes opérées par des entités externes doit être clairement documenté.

Si elle veut être qualifiée conformément à l'[ORDONNANCE] et au [DécretRGS] pour son offre de certificat d'authentification de serveurs, l'AC doit respecter les exigences décrites dans la présente PC Type (correspondant au niveau de sécurité visé) et s'engager à ce que les composantes de l'IGC, internes et externes à l'AC, respectent aussi les exigences qui les concernent.

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 :

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats d'authentification serveur de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux RCAS, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC Type, notamment en matière de génération des certificats, de remise au RCAS, 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.

Niveau (***)
L'AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité

Niveau (***)
propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.

Niveaux (* et **)
Il est recommandé que l'AC mène une analyse de risque.

- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la présente PC Type, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder 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 aux RCAS 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.

I.3.2. Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur RCAS et les informations liées au serveur informatique. Pour cela, l'AE assure les tâches suivantes :

- la prise en compte et la vérification des informations du futur RCAS et du serveur informatique, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- le cas échéant, la prise en compte et la vérification des informations du futur MC (cf. dernier paragraphe du I.3.2) et de son 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 ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RCAS ou, le cas échéant, du MC, 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 peut s'appuyer sur un MC désigné et placé sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations (cf. chapitre I.3.5.2 ci-dessous). Dans ce cas, l'AE doit s'assurer que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé. Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE (cf. chapitre V.5).

I.3.3. Responsables de certificats d'authentification serveur

Dans le cadre de la présente PC Type, un RCAS est une personne physique qui est responsable de l'utilisation du certificat du serveur informatique identifié dans le certificat et de la clé privée

correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RCAS a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RCAS respecte les conditions qui lui incombent définies dans la PC de l'AC, qui doit reprendre les conditions définies dans la présente PC Type.

Il est à noter que le certificat étant attaché au serveur informatique et non au RCAS, ce dernier peut être amené à changer en cours de validité du certificat : départ du RCAS de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RCAS de ses fonctions et lui désigner un successeur. Une AC doit révoquer un certificat d'authentification serveur pour lequel il n'y a plus de RCAS explicitement identifié.

I.3.4. Utilisateurs de certificats

La présente PC Type traitant de certificats d'authentification serveur (cf. chapitre I.4), un utilisateur de certificats[6] peut être notamment :

- Un agent (personne physique) accédant à un serveur informatique et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager accédant à un serveur informatique d'une autorité administrative et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, afin d'établir une clé de session partagée entre son poste et le serveur.
- Un serveur informatique accédant à un autre serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.

I.3.5. Autres participants

I.3.5.1. Composantes de l'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre I.3.1 ci-dessus. Les composantes de l'IGC mettant en œuvre ces fonctions devront être présentées dans la DPC de l'AC.

I.3.5.2. Mandataire de certification

Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC.

Dans le cas où elle y a recours, le MC doit être formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'IGC.

Les engagements du MC à l'égard de l'AC doivent être précisés dans un contrat écrit avec l'entité responsable du MC. Ce contrat stipule notamment que le MC doit :

- effectuer correctement et de façon indépendante les contrôles d'identité et des éventuels attributs des futurs RCAS et serveurs informatiques de l'entité pour laquelle il est MC,
- respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

[6] Certains ouvrages utilisent le terme de "accepteur de certificats".

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

Le MC ne doit en aucun cas avoir accès aux moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat d'authentification serveur délivré au RCAS.

I.4. Usage des certificats

I.4.1. Domaines d'utilisation applicables

I.4.1.1. Bi-clés et certificats du serveur

La présente PC Type traite des bi-clés et des certificats à destination de serveurs informatiques, afin que ces serveurs puissent être authentifiés dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS, avec les catégories d'utilisateurs de certificats identifiées au chapitre I.3.4 ci-dessus et établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

Ceci correspond notamment aux relations suivantes :

- établissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager,
- établissement d'une session sécurisée entre un serveur et un agent,
- établissement d'une session sécurisée entre deux serveurs.

D'autres usages peuvent être autorisés par l'AC dans sa PC, notamment dans des relations autres qu'avec l'Administration, mais sous la responsabilité de l'AC et à conditions que ces autres usages ne remettent pas en cause la conformité aux exigences de la présente PC Type. Notamment, l'utilisation de la clé privée du serveur et du certificat associé doit rester strictement limitée à l'établissement de sessions sécurisées (cf. chapitre IV.5.1 ci-dessous).

L'utilisateur du certificat a ainsi l'assurance que le serveur auquel il se connecte est celui identifié dans le certificat et que les données échangées au cours de cette session, entre l'utilisateur du certificat et le serveur, seront chiffrées. Le niveau d'assurance dépend, notamment, des moyens mis en œuvre par l'AC tout au long du cycle de vie du certificat, ainsi que des mesures prises pour protéger la clé privée au niveau du serveur.

Dans le cadre d'une application d'échanges dématérialisés avec l'Administration, le responsable de l'application décide quel niveau de sécurité de la présente PC Type est requis.

Niveau (***)

Les certificats d'authentification serveur objets de la présente PC Type sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité du serveur afin de tromper l'utilisateur et/ou d'accéder aux données protégées transmises par l'utilisateur sont **très forts** (intérêt pour les usurpateurs, attraits des données considérées comme confidentielles, etc.).

Niveau (**)

Les certificats d'authentification serveur objets de la présente PC Type sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité du serveur afin de tromper l'utilisateur et/ou d'accéder aux données protégées transmises par l'utilisateur sont **forts** (intérêt pour

Niveau (**)
les usurpateurs, attraits des données considérées comme sensibles, etc.).

Niveau (*)

Les certificats d'authentification serveur objets de la présente PC Type sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité du serveur afin de tromper l'utilisateur et/ou d'accéder aux données protégées transmises par l'utilisateur existent mais sont **moyens** (intérêt pour les usurpateurs, attraits des données, etc.).

I.4.1.2. Bi-clés et certificats d'AC et de composantes

Cette PC Type comporte également des exigences, lorsque nécessaire, concernant les bi-clés et certificats de l'AC (signature des certificats d'authentification serveur, des LCR / LAR et, éventuellement, des réponses OCSP) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

L'AC génère et signe différents types d'objets : certificats, LCR / LAR et, éventuellement, réponses OCSP. Pour signer ces objets, l'AC dispose d'au moins une bi-clé, mais il est recommandé qu'elle mette en œuvre des bi-clés séparées pour ces différents types.

Les certificats des clés publiques de ces bi-clés peuvent être générés par différentes AC. Les cas les plus courants sont les suivants :

1) L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).

2) L'AC dispose d'une seule bi-clé et le certificat correspondant est un certificat racine (certificat autosigné non rattaché à une AC de niveau supérieur).

3) L'AC dispose de bi-clés séparées, le certificat correspondant à la bi-clé de signature de certificats est un certificat racine (certificat autosigné non rattaché à une AC de niveau supérieur) et les certificats des autres bi-clés sont signés par cette bi-clé de signature de certificats de l'AC.

4) L'AC dispose de bi-clés séparées, le certificat correspondant à la bi-clé de signature de certificats est rattaché à une AC de niveau supérieur (hiérarchie d'AC) et les certificats correspondant aux autres bi-clés sont signés par cette bi-clé de signature de certificats de l'AC.

5) L'AC dispose de bi-clés séparées, les certificats correspondant à ces bi-clés sont rattachés à une AC de niveau supérieur (hiérarchie d'AC).

La présente PC Type recommande la mise en œuvre de ce dernier cas, qui permet notamment à l'AC de niveau supérieur de générer et diffuser de manière plus simple des LAR en cas de révocations des certificats d'AC de niveau inférieur.

Quelle que soit l'approche retenue par l'AC (bi-clés séparées ou non), les bi-clés et certificats de l'AC pour la signature de certificats, de LCR / LAR et/ou de réponses OCSP ne doivent être utilisés qu'à cette fin. Ils ne doivent notamment être utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

Conformément au [CWA14167-1], les différentes clés internes à l'IGC peuvent être décomposées suivant les catégories suivantes :

- la (ou les) clé(s) de signature d'AC, utilisée(s) pour signer les certificats générés par l'AC ainsi que les informations sur l'état des certificats (LCR / LAR et, éventuellement, réponses OCSP) ;
- les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'authentification, de signature des journaux d'évènements, de chiffrement des données échangées ou stockées au sein de l'IGC, etc. ;

- les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc.

Les deux derniers types de clés peuvent être des clés asymétriques et/ou symétriques.

Ces différents types de clés, et éventuellement les certificats correspondants, doivent être couverts par leurs propres engagements, complets et à part entière. Ces engagements doivent faire partie directement de la propre PC de l'AC, couvrant les certificats d'authentification serveur (cf. chapitre I.1), ou bien faire l'objet de PC séparées (par exemple, PC d'une AC Racine couvrant les certificats d'AC).

La PC de l'AC répondant à la présente PC Type doit au minimum reprendre les exigences de cette dernière sur les certificats d'AC et de composantes. En cas de traitement de ces certificats dans des PC séparées, ces PC doivent être cohérentes avec les exigences de la PC de l'AC et de la présente PC Type.

I.4.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre IV.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par les RCAS auxquels elle délivre des certificats d'authentification serveur et les utilisateurs de ces certificats serveur.

À cette fin, elle doit communiquer à tous les RCAS, MC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

I.5. Gestion de la PC

I.5.1. Entité gérant la PC

La direction de l'AC est responsable de la validation et de la gestion de la PC répondant aux exigences de la présente PC Type.

I.5.2. Point de contact

À préciser dans la PC de l'AC.

I.5.3. Entité déterminant la conformité d'une DPC avec cette PC

L'AC doit être pourvue d'une direction ayant autorité et une responsabilité finale pour déterminer la conformité de la DPC avec la PC.

I.5.4. Procédures d'approbation de la conformité de la DPC

L'AC doit mettre en place un processus d'approbation de la conformité de la DPC avec la PC.

L'AC est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place. Toute nouvelle version de la DPC doit être publiée, conformément aux exigences du paragraphe IX.12.3 sans délai.

I.6. Définitions et acronymes

I.6.1. Acronymes

Les acronymes utilisés dans la présente PC Type sont les suivants :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la SSI
DGME	Direction Générale de la Modernisation de l'État
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
RCAS	Responsable du Certificat d'Authentification Serveur
RSA	Rivest Shamir Adelman
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

I.6.2. Définitions

Les termes utilisés dans la présente PC Type sont les suivants :

Agent - Personne physique agissant pour le compte d'une autorité administrative.

Applicatif de vérification d'authentification - Il s'agit de l'application mise en œuvre par l'utilisateur ou le serveur pour vérifier l'authentification d'un autre serveur et établir une session sécurisée avec ce serveur, notamment générer la clé symétrique de session et la chiffrer avec la clé publique du serveur contenue dans le certificat correspondant.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat ou des besoin d'authentification ou de cachet du serveur auquel le certificat est rattaché.

Autorités administratives - Ce terme générique, défini à l'article 1 de l'[ORDONNANCE], désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif,

les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'enregistrement - Cf. chapitre I.3.1.

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type du [RGS]).

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC Type, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC Type, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC Type, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RCAS et portant sur une bi-clé d'authentification et d'échange de clés symétriques de session, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

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

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Fonction de génération des certificats - Cf. chapitre I.3.1.

Fonction de génération des éléments secrets du porteur - Cf. chapitre I.3.1.

Fonction de gestion des révocations - Cf. chapitre I.3.1.

Fonction de publication - Cf. chapitre I.3.1.

Fonction de remise au porteur - Cf. chapitre I.3.1.

Fonction d'information sur l'état des certificats - Cf. chapitre I.3.1.

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.

Mandataire de certification - Cf. chapitre I.3.1.

Personne autorisée - Cf. chapitre I.3.1.

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

Porteur - Cf. chapitre I.3.1.

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

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

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

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

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

Responsable du certificat d'authentification serveur - Cf. chapitre I.3.1.

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

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

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de certificat - Cf. chapitre I.3.1.

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

II.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des RCAS et des utilisateurs de certificats, l'AC doit mettre en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (cf. chapitre I.3.1 ci-dessus).

La PC de l'AC doit préciser les méthodes de mise à disposition et les URL correspondantes (annuaire accessible en protocole LDAP et/ou HTTP, serveur Web, serveur OCSP, etc.).

II.2. Informations devant être publiées

L'AC a pour obligation de publier au minimum les informations suivantes à destination des RCAS et utilisateurs de certificats :

- sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647][7] et conforme à la présente PC Type, ainsi que les éventuels documents complémentaires (par exemple, profils des certificats s'ils sont définis dans un document séparé) ;
- la liste des certificats révoqués (serveurs et AC) ;
- les certificats de l'AC, en cours de validité ;
- si l'AC est rattachée à une hiérarchie d'AC, les certificats en cours de validité des AC de cette hiérarchie, les différentes politiques de certification correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine ;
- pour les certificats d'AC autosignés (AC Racine), les informations permettant aux utilisateurs de certificats de s'assurer de l'origine de ces certificats (cf. chapitre VI.1.4) et de leur état (cf. chapitre IV.10).

L'AC a l'obligation de publier, à destination des RCAS et utilisateurs de certificats, sa déclaration des pratiques de certification ainsi que toute autre documentation pertinente pour rendre possible l'évaluation de la conformité avec sa politique de certification. Cependant, elle n'est en général pas tenue de rendre publics tous les détails relatifs à ses pratiques.

L'AC a également pour obligation de publier, à destination des RCAS et le cas échéant, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.).

De plus, compte tenu de la complexité de lecture d'une PC pour des personnes non spécialistes du domaine, il est **obligatoire** que l'AC publie également des conditions générales d'utilisation correspondant aux "PKI Disclosure Statement" (PDS) définis par [ETSI_NQCP] et [RFC3647]. Il est recommandé que ces conditions générales aient une structure conforme à celle décrite en annexe B de [ETSI_NQCP] et reprennent ainsi, à destination des RCAS et des utilisateurs de certificats, les informations pertinentes de la PC de l'AC :

- les conditions d'usages des certificats et leurs limites,
- l'identifiant : OID de la PC applicable,
- les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un certificat pour les utilisateurs,

[7] Si sa PC n'est pas strictement conforme au plan du [RFC3647], l'AC devra y joindre un tableau de correspondance démontrant la complétude de sa PC par rapport au [RFC3647].

- les garanties et limites de garanties de l'AC,
- les informations sur comment vérifier un certificat,
- la durée de conservation des dossiers d'enregistrement et des journaux d'évènements,
- les procédures pour la résolution des réclamations et des litiges,
- le système légal applicable,
- si l'AC a été déclarée conforme à la politique identifiée et dans ce cas au travers de quel schéma.

Ces conditions générales font notamment partie intégrante du dossier d'enregistrement.

Le moyen utilisé pour la publication de ces informations, sauf pour les LCR / LAR (cf. chapitre IV.10), est libre mais doit être précisé dans la PC de l'AC. Il doit garantir l'intégrité, la lisibilité, la compréhensibilité et la clarté des informations publiées.

II.3. Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) doivent être 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 doit être communiquée au RCAS ou MC lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent avoir une disponibilité de VT::T_INF_DISP.

Les certificats d'AC doivent être diffusés préalablement à toute diffusion de certificats de serveurs et/ou de LCR correspondants et les systèmes les publiant doivent avoir une disponibilité de VT::T_AC_DISP.

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 IV.9 et IV.10.

Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une non disponibilité de cette information et que les exigences ci-dessus s'appliquent également à la disponibilité des informations publiées sur ces systèmes.

II.4. Contrôle d'accès aux informations publiées

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

Niveau (***)

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un **contrôle d'accès fort** (basé sur une authentification au moins à deux facteurs).

Niveau (**)

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un **contrôle d'accès fort** (basé sur une authentification au moins à deux facteurs).

L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un **contrôle d'accès de type mots de passe** basé sur une politique de gestion stricte des mots de passe.

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

III. Identification et authentification

III.1. Nommage

III.1.1. Types de noms

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

Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le serveur informatique (subject) sont identifiés par un "Distinguished Name" (DN) de type [X.501].

Des règles sur la construction du DN de ces champs sont précisées dans le document [RGS_A_14].

III.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les serveurs dans les certificats doivent être explicites.

L'identification de l'entité à laquelle le serveur est rattaché est obligatoire.

Le DN du serveur contient son FQDN (« Fully Qualified Domain Name » ou nom de domaine totalement qualifié. Exemple : www.monHote.monDomaine.fr) auquel le serveur est rattaché.

Nota – Le certificat d'authentification serveur est associé au FQDN et pas au serveur physique sur lequel la bi-clé est déployée. Autrement dit, une bi-clé d'authentification serveur peut être déployée sur plusieurs machines physiques rattachées à ce FQDN (cas notamment d'architecture de répartition de charge).

III.1.3. Anonymisation ou pseudonymisation des serveurs

S'agissant de certificats de machines, les notions d'anonymisation ou de pseudonymisation sont sans objet.

III.1.4. Règles d'interprétation des différentes formes de nom

Le document [RGS_A_14] fournit des règles à ce sujet. Le cas échéant des précisions seront fournies par l'AC dans sa PC.

III.1.5. Unicité des noms

Afin d'assurer l'identification unique du FQDN d'un serveur au sein du domaine de l'AC, notamment dans le cas du renouvellement du certificat associé, et pour éviter toute ambiguïté, le DN du champ "subject" de chaque certificat d'authentification serveur doit permettre d'identifier de façon unique le FQDN du serveur au sein du domaine de l'AC. Durant toute la durée de vie de l'AC, le FQDN d'un serveur rattaché à une entité ne peut être attribué à une autre entité.

L'AC précisera dans sa PC et sa DPC comment elle répond à cette exigence et respectera notamment les spécifications sur le DN définies dans le document [RGS_A_14].

III.1.6. Identification, authentification et rôle des marques déposées

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

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

Des précisions seront fournies dans la PC de l'AC.

III.2. Validation initiale de l'identité

L'enregistrement d'un serveur auquel un certificat doit être délivré se fait via l'enregistrement du RCAS correspondant.

[SERVEUR-SERVEUR] Le RCAS devra démontrer que le nom de domaine inclus dans le FQDN du serveur appartient bien à l'entité qu'il représente.

Un RCAS peut être amené à changer en cours de validité du certificat d'authentification serveur correspondant (cf. chapitre I.3.3). Dans ce cas, tout nouveau RCAS doit également faire l'objet d'une procédure d'enregistrement.

L'enregistrement d'un RCAS, et du serveur informatique correspondant, peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

- Enregistrement d'un RCAS sans MC pour un certificat d'authentification serveur à émettre : validation par l'AE de l'identité "personne morale" de l'entité de rattachement du RCAS, de l'identité "personne physique" du futur RCAS, de son habilitation à être RCAS pour le serveur informatique considéré et pour l'entité considérée, ainsi que du nom de domaine du serveur.
- Enregistrement d'un nouveau RCAS sans MC pour un certificat d'authentification serveur déjà émis : validation par l'AE de l'identité "personne physique" du futur RCAS et de son habilitation à être RCAS pour le serveur informatique considéré et pour l'entité considérée.
- Enregistrement d'un MC : validation de l'identité "personne morale" de l'entité pour lequel le MC interviendra et de l'identité "personne physique" du futur MC.
- Enregistrement d'un RCAS via un MC pour un certificat d'authentification serveur à émettre ou d'un nouveau RCAS pour un certificat d'authentification serveur déjà émis : validation par le MC de l'identité "personne physique" du futur RCAS, de son habilitation à être RCAS pour le serveur informatique considéré et pour l'entité considérée, ainsi que du nom de domaine du serveur.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre III.2.3.

III.2.1. Méthode pour prouver la possession de la clé privée

Lorsque la bi-clé du serveur n'est pas générée par l'AC, le RCAS doit alors fournir à l'AC, via le MC le cas échéant, une preuve de possession de la clé privée correspondant à la clé publique contenue dans la demande de certificat d'authentification serveur.

III.2.2. Validation de l'identité d'un organisme

Cf. chapitre III.2.3

III.2.3. Validation de l'identité d'un individu

III.2.3.1. Enregistrement d'un RCAS sans MC pour un certificat d'authentification serveur à émettre

L'enregistrement du futur RCAS (personne physique) représentant une entité nécessite l'identification de cette entité et l'identification de la personne physique. S'agissant d'un certificat d'authentification serveur, le RCAS doit de plus être habilité en tant que RCAS pour le serveur informatique considéré et justifier que ce serveur appartient bien à cette entité.

[SERVEUR-SERVEUR] Le RCAS doit justifier que son entité de rattachement détient le nom de domaine auquel le FQDN du serveur informatique est rattaché.

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- [SERVEUR-SERVEUR] une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le FQDN du serveur concerné par cette demande,
- [SERVEUR-CLIENT] une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du serveur concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour la ou les machines sur lesquelles seront déployés le certificat d'authentification serveur devant être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCAS,
- [ENTREPRISE] toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- [ENTREPRISE] tout document attestant de la qualité du signataire de la demande de certificat,
- [ADMINISTRATION] une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du futur RCAS comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- [SERVEUR-SERVEUR] une preuve de possession par l'entité du nom de domaine correspondant au FQDN du serveur,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le RCAS,
- les conditions générales d'utilisation signées.

Nota - Le RCAS doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Niveau (***)

L'authentification du RCAS par l'AE est réalisée lors d'un face-à-face physique[8].

Niveau (**)

L'authentification du RCAS par l'AE est réalisée lors d'un face-à-face physique[9] ou sous forme dématérialisée à condition que la demande soit signée par le RCAS à l'aide d'un procédé de signature

[8] Le face-à-face physique permettant à l'AE de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

Niveau (**)
électronique conforme au minimum aux exigences du niveau (**)[10] décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.

Niveau (*)

L'authentification du RCAS peut notamment se faire :

- Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RCAS) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").
- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RCAS à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.
- Soit par la communication d'un élément propre au futur RCAS permettant de l'identifier au sein d'une base de données administrative pré-établie.

III.2.3.2. Enregistrement d'un nouveau RCAS sans MC pour un certificat d'authentification serveur déjà émis

Dans le cas de changement d'un RCAS en cours de validité d'un certificat d'authentification serveur, le nouveau RCAS doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RCAS.

L'enregistrement du nouveau RCAS (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le serveur est rattaché et en tant que RCAS pour le serveur considéré.

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être le nouveau RCAS pour le serveur informatique auquel le certificat a été délivré, en remplacement du RCAS précédent. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCAS,
- [ENTREPRISE] tout document attestant de la qualité du signataire du mandat,
- [ADMINISTRATION] une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du futur RCAS comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- les conditions générales d'utilisation signées.

---

[9] Le face-à-face physique permettant à l'AE de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[10] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

Nota - Le RCAS doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Niveau (***)

L'authentification du RCAS par l'AE est réalisée lors d'un face-à-face physique[11].

Niveau (**)

L'authentification du RCAS par l'AE est réalisée lors d'un face-à-face physique[12] ou sous forme dématérialisée à condition que la demande soit signée par le RCAS à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[13] décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.

Niveau (*)

L'authentification du RCAS peut notamment se faire :

- Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RCAS) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").
- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RCAS à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.
- Soit par la communication d'un élément propre au futur RCAS permettant de l'identifier au sein d'une base de données administrative pré-établie.

III.2.3.3.Enregistrement d'un Mandataire de Certification

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification pour répondre aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les RCAS présentés par le MC.

[11] Le face-à-face physique permettant à l'AE de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[12] Le face-à-face physique permettant à l'AE de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[13] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

- Éventuellement, fourniture d'un certificat au MC pour qu'il puisse signer les dossiers d'enregistrement de certificats d'authentification serveur de l'entité qu'il représente et les transmettre sous forme électronique.

Le dossier d'enregistrement d'un MC doit comprendre :

- une demande écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité,
- un mandat, daté de moins de 3 mois, désignant le MC. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le MC,
- un engagement signé, et daté de moins de 3 mois, du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs,
- un engagement signé, et daté de moins de 3 mois, du MC à signaler à l'AE son départ de l'entité,
- [ENTREPRISE] toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- [ENTREPRISE] tout document attestant de la qualité du signataire de la demande,
- [ADMINISTRATION] une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie.

Nota - Le MC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Niveau (***)

L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique[14].

Niveau (**)

L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique[15] ou sous forme dématérialisée à condition que le dossier de demande soit signé par le MC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[16] décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.

[14] Le face-à-face physique permettant à l'AE de vérifier l'identité du MC peut être réalisé lors de la remise par l'AC au MC du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du MC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[15] Le face-à-face physique permettant à l'AE de vérifier l'identité du MC peut être réalisé lors de la remise par l'AC au MC du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du MC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[16] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

Niveau (*)

L'authentification du MC par l'AE peut se faire par l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, MC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ces papiers d'identité, précédées de la mention "copie certifiée conforme à l'original"). Cette authentification peut également se faire sous forme dématérialisée à condition que les différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.

III.2.3.4. Enregistrement d'un RCAS via un MC pour un certificat d'authentification serveur à émettre

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- une demande de certificat écrite, datée de moins de 3 mois, signée par le MC et comportant :
  - [SERVEUR-SERVEUR] le FQDN du serveur concerné par cette demande,
  - [SERVEUR-CLIENT] le nom du serveur concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour le serveur informatique auquel le certificat doit être délivré. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur RCAS,
- un document officiel d'identité en cours de validité du RCAS comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté au MC qui en transmet une copie à l'AE pour conservation,
- [SERVEUR-SERVEUR] une preuve de possession par l'entité du nom de domaine correspondant au FQDN du serveur,
- les conditions générales d'utilisation signées.

Nota - Le RCAS doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Niveau (***)

L'authentification du RCAS par le MC est réalisée lors d'un face-à-face physique[17].

Niveau (**)

L'authentification du RCAS par le MC est réalisée lors d'un face-à-face physique[18] ou sous forme dématérialisée à condition que la demande soit signée par le RCAS à l'aide d'un procédé de signature

[17] Le face-à-face physique permettant au MC de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[18] Le face-à-face physique permettant au MC de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations

Niveau (**)
électronique conforme au minimum aux exigences du niveau (**)[19] décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.

Niveau (*)

L'authentification du RCAS peut notamment se faire :

- Soit par l'envoi du dossier papier au MC accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RCAS) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").
- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RCAS à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.
- Soit par la communication d'un élément propre au futur RCAS permettant de l'identifier au sein d'une base de données administrative pré-établie.

Lors de la transmission des dossiers de RCAS par le MC, celui-ci doit s'authentifier auprès de l'AE :

- soit à l'aide d'un certificat électronique remis par l'AC,
- soit au cours d'un face-à-face et/ou par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages.

III.2.3.5. Enregistrement d'un nouveau RCAS via un MC pour un certificat d'authentification serveur déjà émis

Dans le cas de changement d'un RCAS pour un certificat d'authentification serveur en cours de validité de ce certificat, le nouveau RCAS doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RCAS.

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- un mandat, daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être le nouveau RCAS pour le serveur informatique auquel le certificat a été délivré, en remplacement du RCAS précédent. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur RCAS,
- un document officiel d'identité en cours de validité du RCAS comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté au MC qui en transmet une copie à l'AE pour conservation,
- les conditions générales d'utilisation signées.

Nota - Le RCAS doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

---

contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[19] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

Niveau (***)

L'authentification du RCAS par le MC est réalisée lors d'un face-à-face physique[20].

Niveau (**)

L'authentification du RCAS par le MC est réalisée lors d'un face-à-face physique[21] ou sous forme dématérialisée à condition que la demande soit signée par le RCAS à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[22] décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.

Niveau (*)

L'authentification du RCAS peut notamment se faire :

- Soit par l'envoi du dossier papier au MC accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RCAS) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").
- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RCAS à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.
- Soit par la communication d'un élément propre au futur RCAS permettant de l'identifier au sein d'une base de données administrative pré-établie.

Lors de la transmission des dossiers de RCAS par le MC, celui-ci doit s'authentifier auprès de l'AE :

- soit à l'aide d'un certificat électronique remis par l'AC,
- soit au cours d'un face-à-face et/ou par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages.

III.2.4. Informations non vérifiées du RCAS et/ou du serveur informatique

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

III.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).

---

[20] Le face-à-face physique permettant à l'AE de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[21] Le face-à-face physique permettant à l'AE de vérifier l'identité du RCAS peut être réalisé lors de la remise par l'AC au RCAS du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RCAS. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[22] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

III.2.6. Certification croisée d'AC

Toute certification croisée ou filiation directe ou indirecte d'une AC avec une AC racine certifiée par l'[IGC/A] est interdite sans l'accord formel de l'AC racine de l'IGC/A.

Si elle peut être mise en œuvre, il est recommandé qu'une certification croisée ou filiation directe ou indirecte d'une AC avec une AC qualifiée RGS ne soit réalisée que si l'AC rattachée est elle-même qualifiée.

III.3. Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'un serveur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat d'authentification serveur ne peut pas être fourni au RCAS sans renouvellement de la bi-clé correspondante (cf. chapitre IV.6).

Ce chapitre concerne aussi bien le cas où la bi-clé est générée au niveau du serveur que le cas où elle est générée par l'AC.

III.3.1. Identification et validation pour un renouvellement courant

Niveaux (**, ***)

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

Niveau (*)

Lors du premier renouvellement, la vérification de l'identité du RCAS et des informations du serveur informatique correspondant est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé.

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le RCAS et vérifiera les informations du serveur informatique selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

III.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 doit être identique à la procédure d'enregistrement initial ou doit être une procédure offrant un niveau de garantie équivalent.

III.4. Identification et validation d'une demande de révocation

Niveau (***)

Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer.

Par exemple : série d'au moins 4 ou 5 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou

Niveau (***)
lors du retrait du certificat (cf. chapitre III.2.3), utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).

Niveau (**)

Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer.

Par exemple : série d'au moins 3 ou 4 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou lors du retrait du certificat, utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).

Niveau (*)

Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), elle doit faire l'objet d'un minimum d'authentification : vérification d'une ou deux informations de base du demandeur (adresse, n° de téléphone, etc.) et de son autorité par rapport au certificat à révoquer.

Une demande de révocation peut également être faite par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. Demande de certificat

IV.1.1. Origine d'une demande de certificat

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

IV.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre III.2 ci-dessus) :

- [SERVEUR-SERVEUR] le FQDN du serveur à utiliser dans le certificat ;
- [SERVEUR-CLIENT] le nom du serveur à utiliser dans le certificat ;
- les données personnelles d'identification du RCAS ;
- les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC).

Le dossier de demande est établi soit directement par le futur RCAS à partir des éléments fournis par son entité, soit par son entité et signé par le futur RCAS. Si l'entreprise n'a pas mis en place de MC, le dossier est transmis directement à l'AE. Si l'entreprise a mis en place un MC, le dossier lui est remis.

Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le MC ou le futur RCAS du certificat.

IV.2. Traitement d'une demande de certificat

IV.2.1. Exécution des processus d'identification et de validation de la demande

Les identités "personne physique" et "personne morale" sont vérifiées conformément aux exigences du chapitre III.2.

L'AE, ou le MC le cas échéant, doit effectuer les opérations suivantes :

- [SERVEUR-SERVEUR] valider le FQDN du serveur informatique auquel le certificat doit être rattaché. Il peut utiliser le service d'interrogation whoIs de l'AFNIC par exemple pour vérifier les FQDN se terminant par « .fr ». Par ailleurs l'AE, ou le MC, vérifiera que le FQDN du serveur est correctement formaté et ne contient pas le caractère NUL ;
- [SERVEUR-CLIENT] l'AE, ou le MC, vérifiera que le nom du serveur est correctement formaté ;
- valider l'identité du futur RCAS ;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le futur RCAS a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Dans le cas d'une demande via un MC, celui-ci retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE doit alors s'assurer que la demande correspond bien au mandat du MC.

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et, le cas échéant, de la bi-clé vers la fonction adéquate de l'IGC (cf. chapitre I.3.1).

L'AE conserve ensuite une trace des justificatifs présentés :

- si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le futur RCAS et par l'AE, ou le MC le cas échéant, les signatures étant précédées de la mention "copie certifiée conforme à l'original" ;
- si le dossier est au format électronique, les différents justificatifs sous une forme électronique ayant valeur légale.

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le RCAS, ou le MC le cas échéant, en justifiant le rejet.

IV.2.3. Durée d'établissement du certificat

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. A préciser par l'AC dans sa PC, en visant une durée d'établissement la plus courte possible.

IV.3. Délivrance du certificat

IV.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, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au RCAS : au minimum, le certificat[23], et, selon les cas, la bi-clé du serveur, son dispositif de protection de clés privées, les codes d'activation, etc. (cf. chapitre I.3.1).

Si l'AC génère la bi-clé du serveur, le processus de génération du certificat doit être lié de manière sécurisée au processus de génération de la bi-clé : l'ordonnancement des opérations doit être assuré ainsi que, le cas échéant en fonction de l'architecture de l'IGC, l'intégrité et l'authentification des échanges entres les composantes. Par ailleurs, la clé privée doit être transmise de façon sécurisée au RCAS, en en garantissant l'intégrité et la confidentialité.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres V et VI ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre V.2).

IV.3.2. Notification par l'AC de la délivrance du certificat au RCAS

Niveaux (**) et (***)

La remise du certificat doit se faire en mains propres (face-à-face) au minimum dans le cas où l'authentification du RCAS se fait via un face-à-face et que ce face-à-face n'a pas eu lieu au moment de l'enregistrement (cf. chapitre III.2).

Si la remise du certificat ne se fait pas en mains propres, l'AC précisera dans sa PC comment elle s'assure que le certificat est bien remis au bon RCAS ou à une personne dûment autorisée (par exemple, envoi sur carte à puce ou sur disquette en courrier recommandé, téléchargement grâce à un code d'accès préalablement fourni au RCAS, ...).

Niveau (***)

De plus, si l'AC n'a pas généré elle-même la bi-clé du serveur, elle doit s'assurer que le certificat est bien associé, dans l'environnement du serveur, à la clé privée correspondante (par exemple, mise à disposition d'une application en ligne permettant de réaliser une authentification de test). Il s'agit

[23] Si la bi-clé est générée au niveau du serveur, la clé publique doit être transmise à l'AC (cf. chapitre VI.1.3).

Niveau (***)
notamment du cas où le certificat est associé à une clé privée stockée sur une carte à puce non fournie par l'AC : le certificat doit alors être téléchargé sur la bonne carte à puce.

Niveau (*)

Le certificat peut-être transmis par message électronique à une adresse fournie par le RCAS, ou bien l'URL permettant de télécharger le certificat peut être envoyée à une telle adresse.

Le certificat complet et exact doit être mis à la disposition du MC ou du RCAS.

Nota – Si la remise du certificat doit se faire en main propre auprès de l'AE, le RCAS ou MC sera également tributaire des modalités d'accueil de l'AE.

IV.4. Acceptation du certificat

IV.4.1. Démarche d'acceptation du certificat

Niveau (***)

L'AC doit obtenir confirmation de l'acceptation explicite du certificat par le RCAS sous la forme d'un accord signé (papier ou électronique).

L'AC doit garder une trace de l'acception du certificat par le RCAS.

Niveau (**)

L'AC doit obtenir confirmation de l'acceptation du certificat par le RCAS, si possible de façon explicite sous la forme d'un accord signé (papier ou électronique).

Si la remise du certificat au RCAS, ou le cas échéant à son MC, peut faire l'objet d'une date connue avec un degré suffisant de certitude, l'AC peut s'appuyer sur un mécanisme d'acceptation tacite du certificat moyennant un délai maximum laissé au RCAS, à compter de la date de réception du certificat d'authentification serveur, pour signaler sa non-acceptation du certificat. La première utilisation du certificat peut également valoir acceptation tacite. Dans le cas d'une acceptation tacite, les obligations du RCAS et le délai correspondant doivent être clairement mentionnés dans la PC de l'AC ainsi que dans les conditions générales d'utilisation (cf. chapitre II.2) et/ou le contrat pour le certificat d'authentification serveur considéré.

L'AC doit garder une trace de l'acception du certificat par le RCAS si celle-ci est explicite.

Niveau (*)

L'acceptation peut être tacite à compter de la date d'envoi du certificat (ou des informations de téléchargement) au RCAS. Le processus d'acceptation du certificat et les obligations correspondantes du RCAS doivent être clairement mentionnés dans la PC de l'AC ainsi que dans les conditions générales d'utilisation (cf. chapitre II.2) et/ou le contrat pour le certificat d'authentification serveur considéré.

IV.4.2. Publication du certificat

Si le certificat fait l'objet d'une publication par l'AC, les conditions d'une telle publication doivent être précisées par l'AC dans sa PC. Notamment, cette publication ne peut avoir lieu sans l'accord du RCAS et qu'après acceptation du contenu du certificat par celui-ci.

IV.4.3. Notification par l'AC aux autres entités[24] de la délivrance du certificat

L'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

IV.5. Usages de la bi-clé et du certificat

IV.5.1. Utilisation de la clé privée et du certificat par le RCAS

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée : authentification du serveur, échange de la clé symétrique de session (cf. chapitre I.4.1.1). Les RCAS doivent s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du serveur et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (cf. [RGS_A_14]). Cet usage doit également être clairement explicité dans la PC de l'AC, ainsi que dans les conditions générales d'utilisation et/ou le contrat pour le certificat d'authentification serveur considéré. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RCAS ou du MC par l'AC avant d'entrer en relation contractuelle.

IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre I.4.

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

IV.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 du serveur).

Dans la cadre de la présente PC Type, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. Aussi, si c'est l'AC qui génère les bi-clés des serveurs, elle doit garantir qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du [RFC3647]. Dans le cas contraire, elle doit s'en assurer auprès du RCAS, au minimum au travers d'un engagement contractuel clair et explicite du RCAS vis-à-vis de l'AC.

IV.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

IV.6.2. Origine d'une demande de renouvellement

Sans objet.

IV.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

[24] Internes et/ou externes à l'IGC.

IV.6.4. Notification au RCAS de l'établissement du nouveau certificat

Sans objet.

IV.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

IV.6.6. Publication du nouveau certificat

Sans objet.

IV.6.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

IV.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 d'authentification serveur liée à la génération d'une nouvelle bi-clé.

IV.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 des serveurs, et les certificats correspondants, seront renouvelées au minimum à une fréquence définie par VT::T_PORT_MAX.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du serveur (cf. chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat". Ce terme recouvre également, dans le cas où elle est générée par l'AC, la fourniture de la nouvelle bi-clé du serveur.

IV.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat d'authentification serveur peut-être automatique ou bien à l'initiative du RCAS.

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

IV.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 III.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre IV.3.1.

IV.7.4. Notification au RCAS de l'établissement du nouveau certificat

Cf. chapitre IV.3.2.

IV.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre IV.4.1.

IV.7.6. Publication du nouveau certificat

Cf. chapitre IV.4.2.

IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre IV.4.3.

IV.8. Modification du certificat

Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.6).

La modification de certificat n'est pas recommandée dans la présente PC Type. Toutefois, si elle est mise en œuvre, elle doit modifier le numéro de série du certificat, révoquer le certificat initial et ne concerner que les certificats d'utilisateurs finaux.

IV.8.1. Causes possibles de modification d'un certificat

Sans objet.

IV.8.2. Origine d'une demande de modification d'un certificat

Sans objet.

IV.8.3. Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

IV.8.4. Notification au RCAS de l'établissement du certificat modifié

Sans objet.

IV.8.5. Démarche d'acceptation du certificat modifié

Sans objet.

IV.8.6. Publication du certificat modifié

Sans objet.

IV.8.7. Notification par l'AC aux autres entités de la délivrance du certificat modifié

Sans objet.

IV.9. Révocation et suspension des certificats

IV.9.1. Causes possibles d'une révocation

IV.9.1.1. Certificats d'authentification serveur

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'authentification serveur :

- les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN ou du nom du serveur), ceci avant l'expiration normale du certificat ;
- le RCAS n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le RCAS et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- la clé privée du serveur est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées) ;
- le RCAS ou une entité autorisée (représentant légal de l'entité ou MC par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- l'arrêt définitif du serveur ou la cessation d'activité de l'entité du RCAS de rattachement du serveur.

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 doit être révoqué.

IV.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) ;
- cessation d'activité de l'entité opérant la composante.

IV.9.2. Origine d'une demande de révocation

IV.9.2.1. Certificats serveurs

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

- le RCAS pour le serveur considéré ;
- le MC ;
- un représentant légal de l'entité ;
- l'AC émettrice du certificat ou l'une de ses composantes (AE).

Nota : Le RCAS doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité.

IV.9.2.2. Certificats d'une composante de l'IGC

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

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

IV.9.3. Procédure de traitement d'une demande de révocation

IV.9.3.1. Révocation d'un certificat d'authentification serveur

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 III.4.

L'AC doit préciser dans sa PC comment la fonction de gestion des révocations est organisée et quels sont les points d'accès à cette fonction pour les demandeurs de révocation.

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

- [SERVEUR-SERVEUR] le FQDN du serveur utilisée dans le certificat ;
- [SERVEUR-CLIENT] le nom du serveur utilisée dans le certificat
- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...) ;
- éventuellement, la cause de révocation.

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 doit être diffusée au minimum via une LCR signée par une entité désignée par l'AC. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC (cf. chapitre IV.9.9).

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le RCAS n'est pas le demandeur, il doit également être informé de la révocation effective de ce certificat.

L'entité, directement ou via son MC le cas échéant (au choix de l'entité), doit être informée de la révocation de tout certificat d'authentification serveur qui lui sont rattachés.

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.

IV.9.3.2. Révocation d'un certificat d'une composante de l'IGC

L'AC précisera 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 doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des RCAS concernés que leurs certificats d'authentification serveur correspondants ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les RCAS en leur indiquant explicitement que leurs certificats d'authentification serveur ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Afin de faciliter la révocation du certificat de l'AC, il est recommandé que le certificat associé à la clé de l'AC signant les certificats d'authentification serveur soit signé par une autre AC et ne soit pas uniquement autosigné (cf. chapitre I.4.1.2).

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

IV.9.4. Délai accordé au RCAS pour formuler la demande de révocation

Dès que le RCAS (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.

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

IV.9.5.1. Révocation d'un certificat d'authentification serveur

Par nature, une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations doit être disponible conformément à VT::T_REV_DISP.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à VT::T_REV_INDIS et une durée maximale totale d'indisponibilité par mois conforme à VT::T_REV_MAX.

Toute demande de révocation d'un certificat d'authentification serveur doit être traitée dans un délai inférieur à VT::T_REV_TRAIT, 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.

IV.9.5.2. Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un 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 et/ou de réponses OCSP) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

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

IV.9.7. Fréquence d'établissement des LCR

La fréquence de publication des LCR doit être conforme à VT::F_PUB_LCR.

Niveaux (***) et (**)

Il est recommandé de mettre en œuvre le mécanisme des deltaLCR et de publier une deltaLCR conformément à VT::F_PUB_dLCR. Ce mécanisme permet en effet de respecter l'exigence de délai de traitement d'une demande de révocation sans avoir à modifier la fréquence de publication des LCR. Les modalités liées à la mise en œuvre des deltaLCR devront être précisées par l'AC dans sa PC en conformité avec le document [RGS_A_14].

Niveau (*)

Si l'AC met en œuvre le mécanisme de deltaLCR, la publication doit se faire suivant la fréquence VT::F_PUB_dLCR.

IV.9.8. Délai maximum de publication d'une LCR

Une LCR doit être publiée dans un délai maximum conforme à VT::T_PUB_LCR suivant sa génération.

IV.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

D'autres formes de publications complémentaires (serveur OCSP par exemple) peuvent être mises en place à condition qu'elles respectent les exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC Type.

La mise en œuvre d'un service OCSP est recommandée.

IV.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre IV.9.6 ci-dessus.

IV.9.11. Autres moyens disponibles d'information sur les révocations

Ces autres moyens d'information sur les révocations peuvent être mis en place à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrites dans la présente PC Type.

À préciser par l'AC dans sa PC.

IV.9.12. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats serveurs, 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 IV.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

Niveau (***)
L'AC doit imposer au RCAS ou au MC qu'en cas de compromission de la clé privée du serveur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le RCAS s'oblige à interrompre immédiatement et définitivement l'usage de la clé privée et de son certificat associé.

IV.9.13. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC Type.

IV.9.14. Origine d'une demande de suspension

Sans objet.

IV.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

IV.9.16. Limites de la période de suspension d'un certificat

Sans objet.

IV.10. Fonction d'information sur l'état des certificats

IV.10.1. Caractéristiques opérationnelles

L'AC doit fournir 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 et l'état du certificat de l'AC Racine.

La fonction d'information sur l'état des certificats doit au moins mettre à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR / LAR. Ces LCR / LAR doivent être des LCR au format V2, publiées au moins dans un annuaire accessible en protocole LDAP V3. Il est par ailleurs recommandé de mettre en œuvre la fonction de vérification en ligne du statut du certificat via le protocole OCSP.

IV.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats doit être disponible conformément à VT::T_ETAT_DISP.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à VT::T_ETAT_INDIS et une durée maximale totale d'indisponibilité par mois conforme à VT::T_ETAT_MAX.

Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue[25] doit être au maximum de VT::T_STATUT_MAX.

IV.10.3. Dispositifs optionnels

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

IV.11. Fin de la relation entre le RCAS et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du serveur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

De plus, l'AC doit révoquer un certificat d'authentification serveur pour lequel il n'y a plus de RCAS explicitement identifié.

IV.12. Séquestre de clé et recouvrement

Le séquestre des clés privées des serveurs est interdit par la présente PC Type.

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

[25] Durée mesurée au niveau du serveur (requête reçue par le serveur et réponse au départ du serveur).

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

V. Mesures de sécurité non techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

V.1. Mesures de sécurité physique

V.1.1. Situation géographique et construction des sites

La présente PC Type ne formule pas d'exigence spécifique concernant la localisation géographique de l'IGC et de ses composantes.

La construction des sites doit respecter les règlements et normes en vigueur ainsi qu'éventuellement des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...).

V.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 aux locaux des différentes composantes de l'IGC doivent être contrôlés.

En outre, toute personne entrant dans ces zones physiquement sécurisées ne doit pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

Niveau (***)

Pour les fonctions de génération des certificats, de génération des éléments secrets du serveur et de gestion des révocations :

L'accès doit être strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC doivent définir un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre doit permettre de respecter la séparation des rôles de confiance telle que prévue dans la PC de l'AC, en conformité avec la présente PC Type. Notamment, il est recommandé que tout local utilisé en commun avec d'autres fonctions que les fonctions rendues par la composante concernée soit en dehors de ce périmètre de sécurité.

Niveau (**)

Pour les fonctions de génération des certificats, de génération des éléments secrets du serveur et de gestion des révocations :

L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique

Afin d'assurer la disponibilité des systèmes, il est recommandé que l'accès aux machines soit limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Nota - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

V.1.3. Alimentation électrique et climatisation

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

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

V.1.4. Vulnérabilité aux dégâts des eaux

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

V.1.5. Prévention et protection incendie

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

V.1.6. Conservation des supports

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

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

Des procédures de gestion doivent protéger 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.

V.1.7. Mise hors service des supports

En fin de vie, les supports devront être, 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 doivent être conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

V.1.8. Sauvegardes hors site

En complément de sauvegardes sur sites, il est recommandé que les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes doivent être organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences de la présente PC Type et aux engagements de l'AC dans sa PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres IV.9.5.1 et IV.10.2).

Les informations sauvegardées hors site doivent respecter les exigences de la présente PC Type en matière de protection en confidentialité et en intégrité de ces informations.

Niveaux (***) et (**)

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, doivent obligatoirement mettre en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

Les fonctions de sauvegarde et de restauration doivent être effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.

V.2. Mesures de sécurité procédurales

V.2.1. Rôles de confiance

Chaque composante de l'IGC doit distinguer au moins les cinq rôles fonctionnels[26] de confiance suivants :

- **Responsable de sécurité** - Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. 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 des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, et en fonction de l'organisation de l'IGC et des outils mis en œuvre, l'AC peut être amenée à distinguer également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC : cf. chapitres VI.1 et VI.2.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

De manière générale, des procédures doivent être établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification. Ces rôles doivent être décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent

[26] En fonction de la taille de l'entité concernée, de la charge de travail correspondant au rôle, etc., ainsi qu'en fonction des exigences de sécurité et de continuité d'activité, un même rôle fonctionnel peut / doit être tenu par différentes personnes.

déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilité des employés.

Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'AC. L'AC doit implémenter techniquement ce 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 doivent être 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 doivent être 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.

V.2.2. Nombre de personnes requises par tâches

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, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC Type définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre VI).

La DPC de l'AC devra préciser 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.).

V.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- 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 doivent être décrits dans la DPC de l'AC et doivent être conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

V.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

Niveaux (***) et (**)

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur
- contrôleur et tout autre rôle
- ingénieur système et opérateur

Niveau (*)

Concernant les rôles de confiance, le cumul suivant est interdit :

- responsable de sécurité et ingénieur système

V.3. Mesures de sécurité vis-à-vis du personnel

V.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents, ceux-ci sont soumis à leur devoir de réserve.

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

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

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

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

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

V.3.2. Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Ils devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire. Les

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

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

V.3.3. Exigences en matière de formation initiale

Le personnel doit être 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 doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

V.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir 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.

V.3.5. Fréquence et séquence de rotation entre différentes attributions

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. A préciser par l'AC dans sa DPC.

V.3.6. Sanctions en cas d'actions non autorisées

À préciser par l'AC dans sa DPC.

V.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 doit également respecter les exigences du présent chapitre V.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

V.3.8. Documentation fournie au personnel

Chaque personnel doit disposer 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, doit lui être remis la ou les politique(s) de sécurité l'impactant.

V.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, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

V.4.1. Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC doit au minimum journaliser les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation doit être 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 doivent aussi être 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 RCAS,...).

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 doivent également être journalisés, notamment[27] :

- 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 serveur (bi-clé, codes d'activation,…) ;
- génération des certificats d'authentification serveur ;
- transmission des certificats aux RCAS et, selon les cas, acceptations / rejets explicites par les RCAS ;
- le cas échéant, remise du dispositif de protection de clés privées du serveur au RCAS ;
- 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, deltaLCR ;
- le cas échéant, requêtes / réponses OCSP.

Chaque enregistrement d'un évènement dans un journal doit contenir 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 doit être enregistrée) ;
- résultat de l'évènement (échec ou réussite).

[27] Les évènements à journaliser doivent être adaptés à l'organisation et l'architecture de l'IGC. Notamment, les échanges entre fonctions de l'IGC et/ou entre composantes de l'IGC peuvent nécessiter une journalisation pour assurer une traçabilité des actions.

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 doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir 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 doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

Les évènements et données spécifiques à journaliser doivent être documentés par l'AC.

V.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre V.4.8 ci-dessous.

V.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements doivent être conservés sur site pendant au moins le délai VT::T_JOUR_SITE. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous le délai VT::T_JOUR_SITE (recouvrement possible entre la période de conservation sur site et la période d'archivage).

V.4.4. Protection des journaux d'évènements

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

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

Le système de datation des évènements doit respecter les exigences du chapitre VI.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.

V.4.5. Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC.

V.4.6. Système de collecte des journaux d'évènements

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

V.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

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

V.4.8. Évaluation des vulnérabilités

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

Les journaux d'évènements doivent être contrôlés suivant la fréquence VT::F_JOUR_ECH, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au moins à une fréquence VT::F_JOUR_ANA. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) doit être effectué à une fréquence au moins égale à VT::F_JOUR_RAP, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

V.5. Archivage des données

V.5.1. Types de données à archiver

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;
- les justificatifs d'identité des RCAS et, le cas échéant, de leur entité de rattachement ;
- les justificatifs de possession des serveurs ainsi que leurs noms;
- [SERVEUR-SERVEUR] les justificatifs de possession des noms de domaine des FQDN des serveurs ;
- les journaux d'évènements des différentes entités de l'IGC.

V.5.2. Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Les facteurs à prendre en compte dans la détermination de la "loi applicable" sont la loi du pays dans lequel l'AC est établie.

Lorsque les RCAS sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays.

Lorsque des MC sont également dans un autre pays, alors il convient de prendre également en compte les exigences contractuelles et légales applicables à ces MC.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du RCAS ou du MC.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle du RCAS responsable, à un instant "t" du serveur désigné dans le certificat émis par l'AC.

Certificats et LCR émis par l'AC

Les certificats d'authentification serveur et d'AC, ainsi que les LCR / LAR produites, doivent être archivés pendant au moins VT::T_ARCHIVE_C années après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre V.4 seront archivés pendant VT::T_ARCHIVE_J après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre V.4, aucune exigence n'est stipulée. L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver ces journaux.

V.5.3. Protection des archives

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

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

L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4. Procédure de sauvegarde des archives

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. À préciser par l'AC dans ses PC et DPC. Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

V.5.5. Exigences d'horodatage des données

Cf. chapitre V.4.4 pour la datation des journaux d'évènements.

Le chapitre VI.8 précise les exigences en matière de datation / horodatage.

V.5.6. Système de collecte des archives

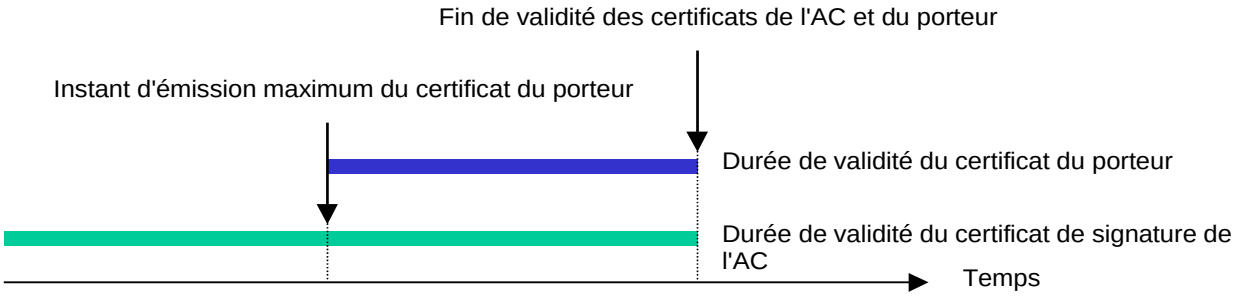
La présente PC Type ne formule pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

V.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à VT::T_REC_ARCH, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

V.6. Changement de clé d'AC

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



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

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

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

V.7. Reprise suite à compromission et sinistre

V.7.1. Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre 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 doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …). L'AC doit également prévenir directement et sans délai le point de contact identifié sur le site : http://www.references.modernisation.gouv.fr.

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 doit :

- informer tous les RCAS et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- révoquer tout certificat concerné.

V.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC doit disposer 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 Type, 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 doit être testé au minimum suivant la fréquence VT::F_TEST_PLAN.

V.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 doit être traité dans le plan de continuité de la composante (cf. chapitre V.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre IV.9.

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

- informer les entités suivantes de la compromission : tous les RCAS, MC et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information doit être mise à disposition des autres tiers utilisateurs ;
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

V.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC Type et de la PC de l'AC (cf. chapitre V.7.2).

V.8. Fin de vie de l'IGC

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

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

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

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

Transfert d'activité ou cessation d'activité[28] affectant une composante de l'IGC

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

1) Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats d'authentification serveur et des informations relatives aux certificats).

2) Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC Type. À défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat d'authentification serveur est encore valide.

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

1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des RCAS ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai VT::T_CESS.

2) L'AC doit communiquer au point de contact identifié sur le site http://www.references.modernisation.gouv.fr, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à la DGME et à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les RCAS et les utilisateurs de certificats.

3) L'AC doit tenir informées la DGME et l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

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 doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) 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 ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC.

L'AC doit stipuler dans ses pratiques les dispositions prises en cas de cessation de service. Elles doivent inclure :

- 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 doit :

[28] Cessation d'activité d'une composante autre que l'AC.

1) s’interdire de transmettre la clé privée lui ayant permis d’émettre des certificats ;

2) prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;

3) révoquer son certificat ;

4) révoquer tous les certificats qu’elle a signés et qui seraient encore en cours de validité ;

5) informer (par exemple par récépissé) tous les MC et/ou RCAS des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3)

VI. Mesures de sécurité techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1. Clés d'AC

La génération des clés de signature d'AC doit être effectuée dans un environnement sécurisé (cf. chapitre V).

Les clés de signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre V.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

Selon le cas, l'initialisation de l'IGC et/ou la génération des clés de signature d'AC peut s'accompagner de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Par exemple, ces parts de secrets peuvent être des parties de la (ou des) clé(s) privée(s) d'AC, décomposée(s) suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer la clé privée), ou encore, il peut s'agir de données permettant de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

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

Niveau (***)

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

Toute manipulation de données secrètes en clair (clés privées d'AC, clés privées des serveurs, parts de secrets d'IGC) doit se faire dans un environnement protégé contre les rayonnements parasites compromettant : matériels protégés, cage de Faraday, locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques, etc.

Niveau (**)

Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

Niveau (*)

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

VI.1.1.2. Clés serveurs générées par l'AC

Les exigences de ce paragraphe ne s'appliquent que si la bi-clé du serveur est générée par l'AC.

La génération des clés des serveurs doit être effectuée dans un environnement sécurisé (cf. chapitre V).

Les bi-clés des serveurs doivent être générées :

- soit directement dans le dispositif de protection de clés privées destiné au serveur conforme aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré,
- soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de protection de clés privées destiné au serveur sans que l'AC n'en garde aucune copie.

VI.1.1.3. Clés serveurs générées au niveau du serveur

Dans le cas où la bi-clé est générée au niveau du serveur, cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré. L'AC doit s'en assurer auprès du RCAS, au minimum au travers d'un engagement contractuel clair et explicite du RCAS vis-à-vis de l'AC.

VI.1.2. Transmission de la clé privée au serveur

Si l'AC génère la bi-clé du serveur (cf. chapitre VI.1.1.2), la clé privée doit être transmise au serveur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission doit se faire de préférence directement dans le dispositif de protection de clés privées destiné au serveur, ou suivant un moyen équivalent.

Niveau (***)

Si la vérification de l'identité du RCAS par l'AE via un face-à-face physique n'a pas eu lieu au moment de l'enregistrement du RCAS (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé générée par l'AC en présence du RCAS.

Niveau (**)

Si la vérification de l'identité du RCAS par l'AE via un face-à-face physique ou via l'emploi d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**) n'a pas eu lieu au moment de l'enregistrement du RCAS (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé générée par l'AC en présence du RCAS.

Il est interdit à l'autorité de certification de conserver ou dupliquer cette clé privée.

VI.1.3. Transmission de la clé publique à l'AC

En cas de transmission de la clé publique du serveur vers une composante de l'AC (cas où la bi-clé est générée au niveau du serveur), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC doivent être diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

Une clé publique d'AC peut être diffusée dans un certificat qui est soit un certificat racine autosigné, soit un certificat rattaché à une hiérarchie d'AC jusqu'à une AC racine (cf. chapitre I.4.1.2 ci-dessus).

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

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

VI.1.5. Tailles des clés

Les clés d'AC et de serveurs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) du document [RGS_A_14].

VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

L'équipement de génération de bi-clés doit utiliser des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. [RGS_A_14]).

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

VI.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et/ou de réponses OCSP (cf. chapitre I.4.1.2 et document [RGS_A_14]).

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée (cf. chapitres I.4.1.1, IV.5 et le document [RGS_A_14]).

VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre des ses clés de signature, ainsi que le cas échéant pour la génération des clés des serveurs, doivent être des modules cryptographiques répondant au minimum aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

VI.2.1.2. Dispositifs de protection de clés privées des serveurs

Les dispositifs de protection de clés privées des serveurs, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré.

Si l'AC ne fournit pas elle-même ce dispositif au RCAS, elle doit s'assurer auprès du RCAS de la conformité du dispositif mis en œuvre par le serveur, au minimum au travers d'un engagement contractuel clair et explicite du RCAS vis-à-vis de l'AC.

En revanche, lorsque l'AC fournit ce dispositif au RCAS, directement ou indirectement, elle doit s'assurer que :

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

Note : L'AC peut s'inspirer du document [ExigencesSitesPerso] pour répondre à ces exigences.

VI.2.2. Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre VI.1.1.1, l'activation de la clé privée au chapitre VI.2.8 et sa destruction au chapitre VI.2.10.

Niveaux (**) et (***)

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).

Niveau (*)

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC).

VI.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des serveurs ne doivent en aucun cas être séquestrées.

VI.2.4. Copie de secours de la clé privée

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

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer 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 à respecter sont définies dans le document [RGS_B_1].

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

Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre VI.2.2.

VI.2.5. Archivage de la clé privée

Les clés privées de l'AC ne doivent en aucun cas être archivée.

Les clés privées des serveurs ne doivent en aucun cas être archivées ni par l'AC ni par aucune des composantes de l'IGC.

VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Si l'AC génère les clés privées des serveurs en dehors du dispositif de protection de clés privées du serveur, le transfert doit se faire conformément aux exigences du chapitre VI.1.1.2 ci-dessus.

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7. Stockage de la clé privée dans un module cryptographique

Il est recommandé de stocker les clés privées d'AC dans un module cryptographique répondant au minimum aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre VI.2.4.

Quelque soit le moyen utilisé, l'AC doit garantir que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

VI.2.8. Méthode d'activation de la clé privée

VI.2.8.1. Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique doit permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

Niveaux (**) et (***)

L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).

Niveau (*)

L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins une personne ayant au moins un rôle de confiance (par exemple, responsable sécurité).

VI.2.8.2. Clés privées des serveurs

La méthode d'activation de la clé privée du serveur dépend du dispositif utilisé. L'activation de la clé privée du serveur doit au minimum être contrôlée via des données d'activation (cf. chapitre VI.4) et doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.9. Méthode de désactivation de la clé privée

VI.2.9.1. Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

VI.2.9.2. Clés privées des serveurs

Les conditions de désactivation de la clé privée d'un serveur doivent permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

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

VI.2.10.2. Clés privées des serveurs

Si les clés privées des serveurs sont générées par l'AC dans un module cryptographique hors du dispositif de protection de clés privées, la méthode de destruction de ces clés privées après leur exportation hors du module cryptographique doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

En fin de vie de la clé privée d'un serveur, la méthode de destruction de cette clé privée doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.11. Niveau de qualification du module cryptographique et des dispositifs protection de clés privées

Les exigences de qualification des produits de sécurité de type module cryptographique et dispositif de protection des clés privées du serveur ne s'appliquent que lorsque :

- le PSCE fait l'objet d'une procédure de qualification de son offre de certificats de cachet, et
- les dispositifs de protection des clés privées du serveur sont délivrés par le PSCE.

Ces exigences sont précisées aux chapitres XI et XII.

VI.3. Autres aspects de la gestion des bi-clés

VI.3.1. Archivage des clés publiques

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

VI.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des serveurs couverts par la présente PC Type doivent avoir une durée de vie au maximum de VT::T_PORT_MAX.

La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats d'authentification serveur qu'elle émet. L'AC doit préciser dans sa PC la durée de vie des clés de signature d'AC et des certificats correspondants. Cette durée de vie doit être cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés (cf. [RGS_A_14]) et doit être au maximum égale à VT::T_C_AC_MAX.

VI.4. Données d'activation

VI.4.1. Génération et installation des données d'activation

VI.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre V.2.1).

VI.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du serveur

Si l'AC génère la clé privée du serveur, elle a pour obligation de transmettre au RCAS les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données. Notamment, la remise de la donnée d'activation doit être séparée dans le temps ou dans l'espace de la remise de la clé privée.

Par exemple : si les éléments secrets d'un serveur sont gérés sur un support matériel dont la mise en œuvre est conditionnée par l'utilisation d'un code personnel, la fourniture du support et celle du code personnel doivent être réalisées par des moyens différents (par exemple retrait du support à un guichet de l'AE et envoi du code par un autre canal).

Si les données d'activation sont sous forme de mots de passe, le RCAS doit être informé de la politique de constitution des mots de passe (par exemple, longueur d'un moins 8 caractères, présence d'un moins un caractère spécial, etc.).

VI.4.2. Protection des données d'activation

VI.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

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

VI.4.2.2. Protection des données d'activation correspondant aux clés privées des serveurs

Si les données d'activation des dispositifs de protection des clés privées des serveurs sont générées par l'AC, elles doivent être protégées en intégrité et en confidentialité jusqu'à la remise aux RCAS.

Si ces données d'activation sont également sauvegardées par l'AC, elles doivent être protégées en intégrité et en confidentialité.

VI.4.3. Autres aspects liés aux données d'activation

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

VI.5. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. chapitre I.3.1).

Une analyse des objectifs de sécurité peut être effectuée en amont de tout projet d'IGC par l'AC, de façon à garantir la prise en compte de la sécurité dans les systèmes informatiques.

VI.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 doit être défini dans la DPC de l'AC. Il doit au moins répondre aux objectifs de sécurité suivants :

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

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (cf. chapitre I.4.1.2) doit faire l'objet de mesures particulières, qui peuvent découler de l'analyse de risque.

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

VI.5.2. Niveau de qualification des systèmes informatiques

Niveaux (***) et (**)

Lorsque le PSCE souhaite faire qualifier son offre de certificats d'authentification serveur, il est recommandé que les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique fassent l'objet d'une qualification conformément à l'[ORDONNANCE], au niveau standard défini par le [RGS] et en respectant les exigences du [CWA 14167-1].

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. rappel au début du présent chapitre VI).

VI.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 doit être documentée et doit respecter 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 doivent être documentées et contrôlées.

L'AC doit :

- garantir que les objectifs de sécurité sont définis lors des phases de spécification et de conception,
- utiliser des systèmes et des produits fiables qui sont protégés contre toute modification

VI.6.2. Mesures liées à la gestion de la sécurité

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

VI.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

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

VI.7. Mesures de sécurité réseau

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

De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

VI.8. Horodatage / Système de datation

Plusieurs exigences de la présente PC Type nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC (cf. chapitre V.4).

Pour dater ces évènements, les différentes composantes de l'IGC peuvent recourir :

- soit à une autorité d'horodatage, interne ou externe à l'IGC, conforme à la politique d'horodatage [RGS_A_12] ;
- soit en utilisant 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. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une

précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

VII. Profils des certificats, OCSP et des LCR

Le document [RGS_A_14] liste les règles concernant les profils des certificats, des listes de révocation (LCR) et OCSP. Elles portent notamment sur :

- Les algorithmes et longueurs des clés cryptographiques ;
- Limitation exclusive de l'usage du certificat à la signature électronique.

VIII. Audit de conformité et autres évaluations

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens de l'[ORDONNANCE] (schéma de qualification des prestataires de services de confiance conformément au [DécretRGS]) et, d'autre part, ceux que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC, ainsi que le cas échéant le ou les MC, est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

La démarche et les exigences liées aux audits de qualification de PSCO de type PSCE sont définies dans [PROG_ACCRED] et ne sont pas reprises ici.

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.

VIII.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 doit procéder à un contrôle de conformité de cette composante.

L'AC doit également procéder régulièrement à un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence VT::F_CONFORM.

VIII.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être 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.

VIII.3. Relations entre évaluateurs et entités évaluées

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

VIII.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.).

VIII.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

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

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

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

VIII.6. Communication des résultats

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

IX. Autres problématiques métiers et légales

IX.1. Tarifs

IX.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

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

IX.1.2. Tarifs pour accéder aux certificats

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

IX.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

L'accès aux LCR et, éventuellement, deltaLCR doit être en accès libre en lecture.

IX.1.4. Tarifs pour d'autres services

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

IX.1.5. Politique de remboursement

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

IX.2. Responsabilité financière

Conformément à ses obligations, l'AC doit prendre les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

IX.2.1. Couverture par les assurances

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

IX.2.2. Autres ressources

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

IX.2.3. Couverture et garantie concernant les entités utilisatrices

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

IX.3. Confidentialité des données professionnelles

IX.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

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

- les données d'activation associées aux clés privées d'AC et des serveurs[29],
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des serveurs et des RCAS,
- les causes de révocations, sauf accord explicite du RCAS.

IX.3.2. Informations hors du périmètre des informations confidentielles

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

IX.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre IX.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 doit en garantir l'intégrité.

L'AC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des certificats d'authentification serveur à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au RCAS et au MC.

IX.4. Protection des données personnelles

IX.4.1. Politique de protection des données personnelles

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].

IX.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des serveurs (qui sont considérées comme confidentielles sauf accord explicite du RCAS) ;
- les dossiers d'enregistrement des RCAS.

IX.4.3. Informations à caractère non personnel

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

IX.4.4. Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre X ci-dessous)

[29] La confidentialité des données d'activation des clés privées des serveurs doit être garantie par l'AC tant qu'elle les détient.

IX.4.5. Notification et consentement d'utilisation des données personnelles

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

IX.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre X ci-dessous)

IX.4.7. Autres circonstances de divulgation d'informations personnelles

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

IX.5. Droits sur la propriété intellectuelle et industrielle

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.6. Interprétations contractuelles et garanties

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VIII) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux RCAS,
- 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.

IX.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 serveur donné et que le RCAS correspondant a accepté le certificat, conformément aux exigences du chapitre IV.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses RCAS sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un RCAS et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

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

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

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

En cas de non-respect ponctuel des obligations décrites dans la présente PC Type, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

IX.6.2. Service d'enregistrement

Cf. les obligations pertinentes du chapitre IX.6.1.

IX.6.3. RCAS

Le RCAS a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger la clé privée du serveur dont il a la responsabilité par des moyens appropriés à son environnement ;
- protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre ;
- protéger l'accès à la base de certificats du serveur ;
- respecter les conditions d'utilisation de la clé privée du serveur et du certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans le certificat d'authentification serveur ;
- faire, sans délai, une demande de révocation du certificat d'authentification serveur dont il est responsable auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

La relation entre le RCAS et l'AC ou ses composantes est formalisée par un engagement du RCAS visant à certifier l'exactitude des renseignements et des documents fournis.

Ces informations s'appliquent également aux MC.

IX.6.4. Utilisateurs de certificats

Les utilisateurs de la sphère publique utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- pour chaque certificat de la chaîne de certification, du certificat du serveur 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 Type.

L'AC ne doit pas émettre dans sa propre PC d'obligations supplémentaires, par rapport aux obligations de la présente PC Type, à l'encontre des utilisateurs de la sphère publique.

IX.6.5. Autres participants

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

IX.7. Limite de garantie

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

IX.8. Limite de responsabilité

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

IX.9. Indemnités

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

IX.10. Durée et fin anticipée de validité de la PC

IX.10.1. Durée de validité

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

IX.10.2. Fin anticipée de validité

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

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

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

IX.10.3. Effets de la fin de validité et clauses restant applicables

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

IX.11. Notifications individuelles et communications entre les participants

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

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

IX.12. Amendements à la PC

IX.12.1. Procédures d'amendements

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

IX.12.2. Mécanisme et période d'information sur les amendements

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

IX.12.3. Circonstances selon lesquelles l'OID doit être changé

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

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC Type) intervient dans les exigences de la présente PC Type applicable à la famille de certificats considérée.

IX.13. Dispositions concernant la résolution de conflits

L'AC doit mettre en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés.

IX.14. Juridictions compétentes

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.15. Conformité aux législations et réglementations

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

IX.16. Dispositions diverses

IX.16.1. Accord global

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

IX.16.2. Transfert d'activités

Cf. chapitre V.8.

IX.16.3. Conséquences d’une clause non valide

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

IX.16.4. Application et renonciation

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

IX.16.5. Force majeure

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

IX.17. Autres dispositions

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

X. Annexe 1 : Documents cités en référence

X.1. Réglementation

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.*
[ORDONNANCE]	*Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*
[DécretRGS]	*Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005*

X.2. Documents techniques

Renvoi	Document
[RGS]	*Référentiel Général de Sécurité – Version 1.0*
[RGS_A_3]	*RGS - Fonction de sécurité « Signature » - Version 2.3*
[RGS_A_4]	*RGS - Fonction de sécurité « Authentification serveur » - Version 2.3*
[RGS_A_13]	*RGS - Politiques de Certification Types - Variables de Temps - Version 2.3*
[RGS_A_14]	*RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3*
[RGS_B_1]	*Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20*
[CWA14167-1]	*CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1*
[ETSI_NQCP]	*ETSI TS 102 042 V1.3.4 (décembre 2007)* *Policy Requirements for Certification Authorities issuing public key certificates*
[ExigencesSitesPerso]	*Exigences de sécurité des sites de personnalisation, V1.0 (août 2007)* *http://www.references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso_V1_0.pdf*
[PROG_ACCRED]	*COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – disponible : www.cofrac.fr*
[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 mars 2000 (complétée par les correctifs techniques n° 1 d'octobre 2001, n° 2 d' avril 2002 et n° 3 d'avril 2004)*
[972-1]	*DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003*

XI. Annexe 2 : Exigences de sécurité du module cryptographique de l'AC

XI.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des serveurs, doit répondre aux exigences de sécurité suivantes :

- si les bi-clés des serveurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- si les bi-clés des serveurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des serveurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des clés privées du serveur et assurer leur destruction sûre après ce transfert ;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Niveaux (**) et (***)

Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.

XI.2. Exigences sur la qualification

Les exigences suivantes ne sont applicables que lorsque le PSCE souhaite faire qualifier son offre de certificats d'authentification de serveur au(x) niveau(x) de sécurité considéré(s) selon la procédure décrite dans le [DécretRGS].

Niveau (***)

Le module cryptographique utilisé par l'AC doit être qualifié au niveau renforcé[30], selon le processus décrit dans le [RGS], et être conforme aux exigences[31] du chapitre XI.1 ci-dessus.

Niveau (**)

Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau standard[32], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XI.1 ci-dessus.

Il est toutefois recommandé d'utiliser un module cryptographique qualifié au niveau renforcé.

Niveau (*)

Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau élémentaire[33], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XI.1 ci-dessus.

Il est toutefois recommandé d'utiliser un module cryptographique qualifié au niveau standard.

[30] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification de serveur doit obtenir une dérogation de l'ANSSI.

[31] Une cible de sécurité conforme au profil de protection [CWA14167-4] (ou [CWA14167-2] s'il y a une fonction de sauvegarde des clés privées de l'AC) permet au module cryptographique d'être considéré comme conforme aux exigences de la présente annexe (hors génération des bi-clés des porteurs). Les exigences de génération des bi-clés des serveurs peuvent être remplies lorsque la cible de sécurité respecte le profil de protection [CWA14167-3].

[32] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification de serveur doit obtenir une dérogation de l'ANSSI.

[33] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification de serveur doit obtenir une dérogation de l'ANSSI.

XII. Annexe 3 : Exigences de sécurité du dispositif de protection de clés privées

XII.1.Exigences sur les objectifs de sécurité

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

- si la bi-clé du serveur est générée par le dispositif, garantir que cette génération 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, de personnalisation 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 de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Nota - Les dispositifs matériels, de types cartes ou boîtiers cryptographiques, sont susceptibles de respecter ces exigences.

XII.2.Exigences sur la qualification

Les exigences suivantes ne sont applicables que lorsque le PSCE souhaite faire qualifier son offre de certificats d'authentification de serveur au(x) niveau(x) de sécurité considéré(s) selon la procédure décrite dans le [DécretRGS] et lorsque le PSCE fournit au RCAS le dispositif de protection des clés privées.

Niveau (***)

Le dispositif de protection des clés privées utilisé par le serveur doit être qualifié au niveau renforcé[34], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XII.1 ci-dessus.

Niveau (**)

Le dispositif de protection des clés privées utilisé par le serveur doit être qualifié au minimum au niveau standard[35], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre

[34] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification de serveur doit obtenir une dérogation de l'ANSSI.

Niveau (**)
XII.1 ci-dessus.

Il est toutefois recommandé d'utiliser un dispositif de protection des clés privées qualifié au niveau renforcé.

Niveau (*)

Le dispositif de protection des clés privées utilisé par le serveur doit être qualifié au minimum au niveau élémentaire, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XII.1 ci-dessus.

Il est toutefois recommandé d'utiliser un dispositif de protection des clés privées qualifié au niveau standard.

[35] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification serveur doit obtenir une dérogation de l'ANSSI.