SG Trust Services
L'Autorité de Certification
du Groupe SOCIÉTÉ GÉNÉRALE

SG Trust Services

Politique de Certification - AC SG TS 2 ETOILES Signature

Référence V1.0 – Octobre 2010

OID 1.2.250.1.124.7.1.2.3.1

Table des matières

1. INTRODUCTION

1.1. Présentation générale

SG Trust Services s'est positionné depuis 2003 comme Prestataire de Services de Certificats électroniques (PSCE), pour les Entreprises ayant des besoins dans le cadre de leurs échanges numériques avec l'Administration : la procédure de déclaration de TVA pour les entreprises, la consultation du Compte fiscal dématérialisé, les télé-déclarations sociales effectuées à partir du portail net-entreprises.fr, les télé-déclarations d'opérations dans le cadre de l'application SIV (ex TéléC@rteGrise), la dématérialisation des appels d'offres publics etc.

A ce titre, la famille de certificats délivrés historiquement par SG Trust Services est « référencée PRIS V1 ».

Suite à la publication du Décret n°2010-112 dit « Référentiel Général de Sécurité » (RGS) le 02 févier 2010, SG Trust Services a entrepris de mettre à niveau son offre de certificats, sur les plans technologique et réglementaire.

Dans ce cadre, SG Trust Services met en place une nouvelle Autorité de Certification, « SG TS 2 ETOILES », respectant le niveau d'exigences ** du RGS. Cette Autorité de Certification a vocation à être qualifiée, en pré-requis à un nouveau référencement pour la conservation du titre de PSCE pour les besoins de l'Administration électronique.

Le présent document constitue la Politique de Certification pour les certificats du profil « Signature » de l'Autorité de Certification « SG TS 2 ETOILES ».

Ce document a été établi sur la base de la Politique de Certification Type pour le profil « Signature » (V2.3), figurant en Annexe A du Référentiel Général de Sécurité, dans sa version du 6 Mai 2010.

1.2. Identification du document

Le numéro d'OID du présent document est **1.2.250.1.124.7.1.2.3.1**

Le numéro d'OID de ce document répond aux principes de nommage suivants :

- Iso : **1**
- member-body : **2**
- f : **250**
- type-org : **1**
- Société Générale : **124**
- SG Trust Services : **7**
- Politique de Certification : **1**
- AC SG TS 2 ETOILES : **2**
- Profil Signature : **3**
- Version : **1**

1.3. Entités intervenant dans l'IGC

1.3.1. Autorité de Certification

L'Autorité de Certification est SG Trust Services, dûment représentée par son responsable, le Président de SG Trust Services.

L'Autorité de Certification est garante du niveau de confiance des certificats qu'elle émet. Ce niveau de confiance repose sur des mesures techniques et organisationnelles et sur une gouvernance, qui sont décrits dans la présente Politique de Certification. L'Autorité de Certification veille à l'application de la présente Politique de Certification

En particulier, l'AC a la responsabilité des fonctions suivantes :

- Mise en application de la PC.
- Gestion des certificats.
- Gestion des supports et de leurs données d'activation (les bi-clés et les certificats sont fournis aux Porteurs sur des supports physiques).
- Publication des Listes de Certificats Révoqués (LCR).
- Journalisation et archivage des événements et informations relatifs au fonctionnement de l'IGC.
- Réception et traitement des demandes de Révocation de Certificats.
- Archivage des dossiers de demande de Certificats ou de Révocation.

1.3.2. Autorité d'Enregistrement

Les rôles de l'Autorité d'Enregistrement sont répartis entre :

- D'une part, les Chargés de Clientèle.
- D'autre part, l'AE Déléguée.

La présente PC ne fait donc pas référence à l'Autorité d'Enregistrement, mais à l'une ou l'autre de ses composantes, ensemble des Chargés de Clientèle, ou AE Déléguée.

1) Le Chargé de Clientèle

Le Chargé de Clientèle appartient à l'organisation d'un des différents réseaux commerciaux du groupe Société Générale.

Le Chargé de Clientèle s'appuie sur les Gestionnaires de Certificats (voir paragraphe 1.3.5.3) pour la validation de l'identité des Porteurs. Cette étape cruciale pour le niveau de confiance des certificats est entièrement déléguée aux Gestionnaires de Certificats, qui sont nommés selon une procédure spéciale (voir paragraphe 3.2.3.3).

Dans ce cadre, le Chargé de Clientèle a pour rôle de :

- Valider la nomination des Gestionnaires de Certificats sur la base d'un dossier d'enregistrement spécifique (dossier de souscription).
- Valider les demandes de certificats en provenance des Gestionnaires de Certificats, sur la base des dossiers d'enregistrement.

Le Chargé de Clientèle transmet les dossiers de souscription et les dossiers d'enregistrement au Back Office.

Il conserve une copie des dossiers de souscription, contenant les signatures des Gestionnaires de Certificats. Cela lui permettra de vérifier leurs demandes ultérieures, sans passer par un face-à-face.

Le Chargé de Clientèle veille à la protection de la confidentialité et de l'intégrité des données qui lui parviennent ou qu'il transmet à d'autres fonctions de l'IGC au cours des processus de gestion du cycle de vie des certificats.

Le Chargé de Clientèle peut également assurer le suivi des demandes d'enregistrement de nouveaux Porteurs en contactant le Back Office par un numéro d'appel spécifique ou par une boîte mail (BAL) spécifique aux agences.

2) Le Back Office Atos Worldline (AE Déléguée)

Le Back Office appartient à l'organisation d'Atos Worldline, qui est l'Opérateur de Service de Certification (voir paragraphe 1.3.5.1) de l'Autorité de Certification.

Atos Worldline joue le rôle d'AE déléguée.

L'AE Déléguée est responsable de la gestion du cycle de vie des certificats. Elle gère pour le compte des Porteurs :

- Les demandes d'enregistrement.
- Les demandes de révocation.
- Le renouvellement des certificats.
- L'archivage des dossiers d'enregistrement.

Elle joue le rôle d'interface auprès de l'Autorité de Certification pour mener à bien les actions ci-dessus.

L'AE Déléguée veille à la protection de la confidentialité et de l'intégrité des données qui lui parviennent ou qu'elle transmet à d'autres fonctions de l'IGC au cours des processus de gestion du cycle de vie des certificats.

L'AE Déléguée est composée d'Opérateurs d'Enregistrement, faisant tous partie d'Atos Worldline. L'AE Déléguée est représentée par un responsable d'AE Déléguée qui nomme les Opérateurs d'Enregistrement. Le Responsable d'AE Déléguée est nommé par le Responsable de l'Autorité de Certification.

Remarque : le Responsable d'AE Déléguée joue également le rôle de Gestionnaire de Certificats au sein d'Atos Worldline.

1.3.3. Porteurs de certificats

Un Porteur de certificat est une personne physique, agissant dans le cadre de ses activités professionnelles, dûment habilitée par le Chargé de Clientèle dans le cadre d'une de ses fonctions ou mandats, à disposer d'un certificat électronique.

Les Porteurs appartiennent à des organisations classés parmi les Clients Professionnels et Entreprises du Groupe Société Générale (voir la définition de Client au paragraphe 1.6.2).

Au sein d'un Certificat X.509 V3, les informations d'identification du Porteur sont regroupées dans le champ "Objet".

1.3.4. Utilisateurs de certificats

Les utilisateurs des certificats concernés par la présente Politique de Certification sont les services de création et validation de signature des applications de l'Administration électronique qui s'appuient sur des certificats délivrés par des PSCE historiquement « référencés PRIS V1 ».

1.3.5. Autres participants

1) Composantes de l'IGC

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

2) Opérateur de Service de Certification (OSC)

L'Opérateur de Service de Certification est chargé de la délivrance du service technique correspondant aux fonctions de l'Autorité de Certification.

- Il héberge, exploite et maintient en conditions opérationnelles les composants d'infrastructure et les interfaces de gestion.
- Il s'engage sur le niveau de service de l'Autorité de Certification.
- Il joue un rôle d'Autorité d'Enregistrement Déléguée (voir paragraphe 1.3.2.2).

L'Opérateur de Service de Certification est Atos Worldline.

Le contrat établi entre SG Trust Services et Atos Worldline définit précisément les rôles et les obligations de chacune des parties.

Le personnel de l'OSC, en-dehors de l'AE Déléguée, peut être amené à utiliser des certificats d'authentification ou de signature sur les composantes de l'IGC. Ces certificats sont émis par une Autorité de Certification propre à l'OSC. La présente Politique de Certification ne s'applique pas à ces certificats.

3) Mandataire de certification (ou Gestionnaire de Certificats)

Remarque : on désigne dans la présente PC un Mandataire de Certification par l'expression « Gestionnaire de Certificats ».

Le Gestionnaire de Certificats est une personne physique, dûment identifiée et habilitée par l'AE, désignée pour effectuer la vérification de l'identité et de l'habilitation du demandeur, à disposer de certificat électronique, au titre de l'une de ses fonctions ou mandats.

- Le Gestionnaire de Certificats appartient à l'organisation des Porteurs. Il est mandaté par le Représentant Légal du Client. A ce titre, il représente son organisation d'appartenance vis-à-vis de l'Autorité de Certification.
- Le Gestionnaire de Certificats est garant de la fiabilité des informations concernant les Porteurs contenues dans les dossiers d'enregistrement.
- Le Gestionnaire de Certificats transmet les demandes d'enregistrement à l'AE Déléguée. Il peut également faire des demandes de révocation pour des certificats de Porteurs dont il a la charge.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

1) Bi-clés et certificats des Porteurs

Les certificats concernés par cette PC sont des certificats de signature. Ils répondent aux besoins de signature électronique et de non répudiation des personnes physiques qui agissent pour le compte de clients Entreprises ou Professionnels du Groupe Société Générale vis-à-vis de :

- Services de l'Administration accessible par voie électronique : il s'agit des applications qui s'appuient sur des PSCE, historiquement désignées comme applications « référencées PRIS V1 ».
- Services du Groupe Société Générale accessible par voie électronique (application Sogecash NET, EBICS…).

L'usage des certificats est rappelé dans les Conditions Générales d'Utilisation, qui font partie du formulaire de demande DIP, et que le Porteur approuve et signe lors de l'enregistrement (voir paragraphe 4.1.2).

Les bi-clés associées aux certificats sont stockées dans des supports physiques (de type clé cryptographique avec port USB ou carte à puce) remis personnellement à chacun des Porteurs.

Les supports physiques sont certifiés selon les Critères Communs EAL4+ et sont qualifiés au niveau renforcé.

2) Bi-clés et certificats d'AC et composantes

Le certificat de l'AC SG TS 2 ETOILES est signé par l'AC Racine et est utilisable exclusivement pour :

- Signer des certificats Porteurs.
- Signer des LCRs.

1.4.2. Domaines d'utilisation interdits

L'AC décline toute responsabilité dans l'usage que ferait un Porteur ou un Client d'un Certificat dans le cadre d'une application non mentionnée au paragraphe 1.4.1, et pour toute opération illicite.

En cas de violation de cette obligation par le Porteur ou le Client, SG Trust Services ne pourra voir sa responsabilité engagée vis-à-vis de quiconque.

Les actions résultant de l'utilisation du Certificat ne peuvent être considérées comme ayant une valeur probante au sens de la directive européenne 1999/93/CE et des articles 1316 et suivants du Code civil.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

La présente PC est gérée par le Responsable de l'Offre de Certificats électroniques de SG Trust Services.

1.5.2. Point de contact

Les demandes d'informations ou questions concernant l'Autorité de Certification doivent être adressées à :

Responsable de l'Offre Certificats électroniques

SG Trust Services

Les Miroirs – 18, avenue d'Alsace

92 400 Courbevoie

France

Les questions concernant l'Autorité d'Enregistrement Déléguée doivent être adressées aux contacts ci-dessous :

- Par mail :
  - Pour les Clients francophones : support@sgtrustservices.com
  - Pour les Clients anglophones : hotline@sgtrustservices.com
- Par téléphone :
  - SVP clients en France : 0892 70 75 80
  - SVP clients étrangers : +33 (0)2 54 44 71 07

Ces points de contact sont disponibles et à jour sur le site de publication de l'Autorité de Certification (voir le paragraphe 2.2).

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

Le Comité de Pilotage de l'Autorité de Certification décide et pilote la mise en œuvre des opérations de contrôle de conformité la DPC à la PC.

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

L'approbation de conformité de la DPC à la PC est prononcée par le Responsable de l'Autorité de Certification.

1.6. Définitions et acronymes

1.6.1. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

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

CSR	Certificate Signing Request
DGME	Direction Générale de la Modernisation de l'Etat
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
GC	Gestionnaire de Certificats
IGC	Infrastructure de Gestion de Clés
KC	Key Ceremony
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
OSC	Opérateur de Service de Certification
OID	Object Identifier
OSC	Opérateur de Service de Certification
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
RSA	Rivest Shamir Adelman
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

1.6.2. Définitions

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

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.

Autorités administratives – Ce terme générique désigne les administrations de l'État, 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 1.3.2.

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 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 une personne physique et portant sur une bi-clé de signature, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Client – Personne morale ou professionnel personne physique signataire du Contrat d'Abonnement qui habilite les Porteurs à utiliser des Certificats et qui donne mandat au Gestionnaire de Certificats de le représenter pour la gestion des certificats.

Comité de Pilotage de l'Autorité de Certification – instance de pilotage de l'Autorité de Certification. Elle comprend notamment le Responsable de l'Autorité de Certification et le Président de SG Trust Services. Elle se réunit sur une base annuelle. Le comité de pilotage prend notamment les décisions de mener des analyses de risque et des audits.

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.

Conditions Générales d'Utilisation (CGU) - Récapitulatif de l'usage autorisé d'un certificat et des obligations du Porteur, conformément à la Politique de Certification de l'AC. Les CGU doivent être connues du Porteur. Elles sont intégrées dans le formulaire de Demande Individuelle Porteur (DIP).

Contrat d'Abonnement – Contrat de fourniture des services de Certification devant être signé par le Client souhaitant habiliter des Porteurs à utiliser des certificats.

Contrat de Vente Kit de Connexion – Contrat, joint au Dossier De Souscription le cas échéant, précisant les modalités de la mise à disposition d'un kit de connexion permettant la lecture du Support Physique.

CSR (Certificate Signing Request) – Message envoyé à l'Autorité de Certification pour demander la génération d'un certificat. Ce message contient des informations d'identification du demandeur ainsi que sa clé publique, le tout étant signé par sa clé privée. Dans le cas de la présente Politique de Certification, les CSR sont conformes au standard PKCS#10.

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

Dispositif de création de signature – Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée de signature.

Dossier d'enregistrement – Ensemble de documents permettant au Chargé de Clientèle et à l'AE Déléguée de valider la demande d'enregistrement d'un futur Porteur. Il est composé d'un formulaire de Demande Individuelle Porteur (DIP) et d'une copie « certifiée conforme à l'original » du titre d'identité du Porteur.

Dossier de souscription (DDS) – Le dossier de souscription englobe le dossier d'enregistrement. Il contient des pièces supplémentaires nécessaires à la fourniture du service de certification par SG Trust Services pour un Porteur rattaché à un Client. Le DDS est constitué de :

- Une partie dite « Client » servant à l'enregistrement d'un nouveau Client. Elle est constituée de :
  - Un contrat d'abonnement (signé par le Représentant Légal du Client).
  - Un justificatif attestant de l'existence de l'entreprise du Client. Ce justificatif peut être soit :
    - Un Extrait K-BIS de l'entreprise (ou tout autre registre national similaire pour les entités de droit étranger) ou
    - Un Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou
    - Pour les associations, une copie du JO contenant l'insertion relative à l'association, copie de ses statuts et délibération de la dernière assemblée générale nommant un dirigeant
  - Remarque : Dans le cas où le Représentant légal ayant signé le contrat d'abonnement ne correspond pas à celui identifié dans l'extrait K-BIS ou équivalent, il devra alors fournir une attestation de sa qualité de Représentant Légal.
- Une partie dite « Gestionnaire de Certificats » servant à l'enregistrement d'un nouveau Gestionnaire de Certificats. Elle est constituée de :
  - Une fiche d'Identification Gestionnaire de Certificats (signée par le Représentant Légal du Client et par le Gestionnaire de Certificats).
  - Un titre d'identité du Gestionnaire de Certificats (également signée par le Représentant Légal du Client et par le Gestionnaire de Certificats).
- Une partie dite « Porteur » servant à l'enregistrement d'un nouveau Porteur. Cette partie est dénommée **dossier d'enregistrement**. Elle est constituée de :
  - Une Demande Individuelle Porteur (signée par le Gestionnaire de Certificats et par le Porteur).
  - Un titre d'identité du Porteur de Certificats (également signé par le Gestionnaire de Certificats et par le Porteur).

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 – 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 porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère la bi-clé du porteur.

Fonction de génération des éléments secrets du porteur – Cette fonction génère les éléments secrets à destination du porteur, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur (par exemple, personnalisation de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du porteur, les codes (activation / déblocage) liés au dispositif de stockage de la clé privée du porteur ou encore des codes ou clés temporaires permettant au porteur de mener à distance le processus de génération / récupération de son certificat.

Fonction de gestion des révocations – Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction de publication – Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs 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 de ses porteurs.

Fonction de remise au porteur – Cette fonction remet au porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur, clé privée du porteur, codes d'activation,…).

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).

Gestionnaire de Certificats (GC) – voir Mandataire de Certification.

Infrastructure de gestion de clés (IGC) – Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de Gestionnaire de Certificats, d'une entité d'archivage, d'une entité de publication, etc.

***Key Ceremony* (ou Cérémonie de Clés) –** Une *Key Ceremony* est une cérémonie notariée (réalisée en effectif restreints devant témoins, éventuellement filmée…) au cours de laquelle sont réalisées des opérations relatives au cycle de vie des clés d'AC. Par exemple la *Key Ceremony* associée à la création d'un certificat d'AC regroupera les procédures de génération de la bi-clé, de génération du certificat d'AC, de génération et de partage des parts de secrets liés à l'activation de la clé privée… On réalisera une *Key Ceremony* notamment pour la création, la révocation et le renouvellement d'un certificat d'AC racine ou d'AC fille.

Kit de connexion – Kit de connexion mis à disposition du Porteur composé d'un lecteur pour le support physique et d'un logiciel d'interface permettant la lecture du Support Physique.

Mandataire de Certification – Il est appelé Gestionnaire de Certificats (GC) dans la présente PC. Le Gestionnaire de Certificats est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec le Chargé de Clientèle. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des Porteurs lorsque celui-ci est requis).

Opérateur d'Enregistrement – Un Opérateur d'Enregistrement est une personne physique appartenant au back office Atos Worldline, Il est en charge d'effectuer toutes les actions liées à la gestion du cycle de vie des certificats. Un Opérateur d'Enregistrement peut jouer le rôle d'Opérateur de saisie ou d'Opérateur de validation, ces deux rôles ne pouvant être cumulés par le même Opérateur pour une même demande de certificats.

Opérateur de saisie – Opérateur d'Enregistrement ayant pour rôle de vérifier la complétude des dossiers d'enregistrement puis de saisir les demandes de certificats au niveau des interfaces techniques de l'Autorité d'Enregistrement Déléguée.

Opérateur de validation – Opérateur d'Enregistrement ayant pout rôle de valider techniquement les demandes de certificats saisies par un Opérateur de saisie. Pour cela, l'Opérateur de validation doit vérifier que les informations saisies par l'Opérateur de saisie sont conformes à celles figurant dans le dossier d'enregistrement.

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

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

Porteur – La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.

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 porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

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

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 opérationnel – membre du comité de pilotage de l'AC, il est en charge d'exécuter les fonctions incombant au Responsable de Certification. C'est le responsable du service de certification, dont la composante technique est fournie par l'OSC.

Support physique – Support matériel cryptographique sur lequel sont stockés le Certificat et la Clé Privée d'un Porteur. Il peut s'agir d'une clé cryptographique avec prise USB, ou d'une carte à puce. Le type de support physique utilisé pour un Certificat donné est précisé dans le formulaire de Demande Individuelle Porteur.

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

Titre d'identité – Carte d'identité nationale, passeport, ou carte de séjour pour les étrangers.

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 – L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du porteur du certificat.

2. RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

2.1. Entités chargées de la mise à disposition des informations

L'Autorité de Certification est chargée de la mise à disposition des informations devant être publiées.

L'Opérateur de Service de Certification s'engage à fournir les informations devant être publiées dans les délais réglementaires, pour publication au niveau du site Internet de SG Trust Services.

Le service d'exploitation du site Internet de SG Trust Services est chargé de la mise en ligne dans les délais réglementaires de ces informations.

2.2. Informations devant être publiées

Les informations publiées par l'AC SG TS 2 ETOILES sont les suivantes :

- La présente Politique de Certification.
- Les formulaires nécessaires à la gestion des certificats :
  - Contrat d'abonnement Certificat Électronique pour Téléprocédures administratives ou applications de Banque Électronique.
  - Fiche d'Identification Gestionnaire de Certificats.
  - Formulaire de Demande Individuelle Porteur (DIP) pour l'enregistrement.
  - Formulaire de révocation.
- Les Conditions Générales d'Utilisation (incluses dans le formulaire de Demande Individuelle Porteur - DIP).
- Les points de contacts (adresses email, numéros de téléphone) avec l'Autorité de Certification et l'Autorité d'Enregistrement Déléguée.
- La liste des certificats révoqués (LCR).
- Les certificats de l'AC SG TS 2 ETOILES et de l'AC Racine.
- L'empreinte du certificat de l'AC SG TS 2 ETOILES.

Toutes ces informations sont publiées sur le site de publication : http://www.sgts.rgs2e.sgtrustservices.com. En particulier :

- Politique de Certification :

  http://www.sgts.rgs2e.sgtrustservices.com/entreprise/pc/SGTS-2Etoiles/signature/index.htm

- Liste des Certificats Révoqués (LCR) : http://crl.sgtrustservices.com/SGTS-2Etoiles/LatestCRL
- Certificats de l'AC SG TS 2 ETOILES et de l'AC Racine :

  http://www.sgts.rgs2e.sgtrustservices.com/sgts/digitalidCenter.htm

Remarque : ces URL figurent dans les certificats des Porteurs (voir paragraphe 7).

2.3. Délais et fréquences de publication

Le site de publication a une disponibilité de 24h/24 7j/7.

La disponibilité, les délais et fréquence de publication des LCR sont précisés au paragraphe 4.9.

Le site de publication garantit l'intégrité des informations publiées.

2.4. Contrôle d'accès aux informations publiées

Les informations publiées sont mises à disposition en lecture à l'ensemble des accédants au site de publication (ouvert sur Internet).

Les ajouts, suppressions et modifications sont limités aux personnes autorisées de l'AC.

- Le personnel de l'OSC a accès aux informations y compris les informations d'état des certificats (ajout, suppression, modification), via une authentification par certificat, et selon une politique d'habilitation.
- Le personnel d'exploitation du site de publication a accès aux informations y compris les informations d'état des certificats (ajout, suppression, modification), via une authentification à deux facteurs, et selon une politique d'habilitation.

Le transfert des informations devant être publiées de l'OSC vers le personnel d'exploitation du site de publication se fait de manière sécurisée de manière à garantir l'intégrité des données.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de noms

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

Dans chaque certificat X509v3 l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" (DN) de type X.501.

Le paragraphe 7 précise le format du DN.

3.1.2. Nécessité d'utilisation de noms explicites

La décomposition du DN est la suivante :

- Champ CN (Common Name) : contient le prénom suivi du nom du Porteur, tels qu'inscrit sur le titre d'identité présenté lors de l'enregistrement.
  - Remarque : en cas d'homonymie, un deuxième prénom, tel que figurant sur le titre d'identité présenté, pourra être ajouté dans le champ CN.
- Champ E (Email) : contient l'adresse email professionnelle du Porteur au sein de son organisation d'appartenance.
- Champ OU (Organizational Unit) : contient le numéro de SIREN ou SIRET de l'organisation d'appartenance du Porteur, tel que renseigné sur le Contrat d'Abonnement.
- Champ O (Organization) : contient le libellé de l'organisation d'appartenance du Porteur.
- Champ C (Country) : contient le pays où est basé le siège social de l'organisation d'appartenance du Porteur.

Ces informations sont recueillies par le Gestionnaire de Certificats, lors de la phase de validation de l'identité du porteur.

Le Gestionnaire de Certificats s'assure du caractère explicite du nom du Porteur.

Le paragraphe 7 précise le format du DN.

3.1.3. Pseudonymisation des porteurs

Les pseudonymes ne sont pas autorisés par la présente Politique de Certification.

Remarque : les certificats anonymes ne sont pas non plus autorisés.

3.1.4. Règles d'interprétation des différentes formes de nom

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Objet" des Certificats.

Ces informations sont établies par l'AC et reposent essentiellement sur les règles suivantes :

- Tous les caractères sont au format printableString, i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501.
- Les prénoms et noms composés sont séparés par des tirets " - ".

Les certificats respectent les exigences formulées dans le document « Profils de Certificats » de l'Annexe A du RGS [RGS_A_14].

3.1.5. Unicité des noms

Les certificats des Porteurs de l'Autorité de Certification « SG TS 2 ETOILES » pour le profil Signature sont identifiés de manière unique par la combinaison :

- Du DN du certificat.
  - Le DN contient le prénom, le nom et l'organisation du Porteur.
  - L'AE Déléguée inscrira le deuxième prénom du Porteur dans le champ CN (entre le premier prénom et le nom) en cas d'homonymie avec un Porteur existant. L'AE Déléguée est responsable de vérifier les cas d'homonymie.
- Du champ « Subject Alternative Name ».
  - Ce champ contient l'adresse email professionnelle du Porteur qui est unique au sein de son organisation.
- Du champ « Key Usage ».
  - Ce champ permet de distinguer le certificat d'un même Porteur pour des profils différents (Authentification ou Signature).

3.1.6. Identification, authentification et rôle des marques déposées

Sans objet.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

L'AC SG Trust Services exige des Porteurs, au moment de la requête du certificat, la preuve de possession de la clé privée.

Pour cela, la requête de certificat est conforme au standard PKCS#10. De plus, la qualification du support physique utilisé garantit la sécurité des échanges entre le support (où se trouve la clé privée) et le middleware s'exécutant sur le poste de travail.

3.2.2. Validation de l'identité d'un organisme

Cf. paragraphe 3.2.3.

3.2.3. Validation de l'identité d'un individu

1) Enregistrement d'un porteur [particulier]

Sans objet.

2) Enregistrement d'un porteur [Entreprise]/[Administration] sans Mandataire de Certification

Sans objet. Ce processus n'est pas prévu dans la présente Politique de Certification.

3) Enregistrement d'un Mandataire de Certification (ou Gestionnaire de Certificats)

Le processus d'enregistrement (ou de nomination) du Gestionnaire de Certificats est le suivant :

- Le futur Gestionnaire de Certificats remplit et signe la « fiche d'Identification Gestionnaire de Certificats ».
  - Remarque : la fiche d'Identification Gestionnaire de Certificats précise les engagements que prend le futur Gestionnaire à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs et à signaler au Chargé de Clientèle son départ de l'entreprise.
- Le futur Gestionnaire de Certificats fait signer la « fiche d'Identification Gestionnaire de Certificats » par son Représentant Légal.
- De plus, le Représentant Légal signe le contrat d'abonnement entre son organisation d'appartenance (le Client) et SG Trust Services.
- Le Représentant Légal doit également fournir au futur Gestionnaire un Extrait K-BIS de l'entreprise (ou tout autre registre national similaire pour les entités de droit étranger) ou un certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou, pour les associations, une copie du JO contenant l'insertion relative à l'association, ainsi qu'une copie de ses statuts et délibération de la dernière assemblée générale nommant un dirigeant.
  - Remarque : Dans le cas où le Représentant légal ayant signé la fiche d'identification du Gestionnaire de Certificats ne correspond pas à celui identifié dans l'extrait K-BIS ou équivalent, il devra alors fournir une attestation de sa qualité de Représentant Légal.
- Le futur Gestionnaire de Certificats se déplace auprès du Chargé de Clientèle afin d'obtenir la validation de sa nomination.
- Le Chargé de Clientèle vérifie l'identité du futur GC en face-à-face sur présentation d'un titre d'identité.
- Le Chargé de Clientèle photocopie le titre d'identité y ajoute la mention « Certifié conforme à l'original » et le signe. Le futur GC y ajoute sa signature.
- Le Chargé de Clientèle récupère l'ensemble du dossier d'enregistrement qui comprend :
  - La fiche d'Identification Gestionnaire de Certificats signée par le Gestionnaire et par le Représentant Légal.
    - Remarque : ce document doit être daté de moins de 3 mois.
  - Le contrat d'abonnement signé par le Représentant Légal.

- L'extrait K-BIS de l'entreprise (ou tout autre registre national similaire pour les entités de droit étranger) ou un certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou, pour les associations, une copie du JO contenant l'insertion relative à l'association, ainsi qu'une copie de ses statuts et délibération de la dernière assemblée générale nommant un dirigeant.
- La photocopie signée du titre d'identité.

- Le Chargé de Clientèle valide la nomination du Gestionnaire de Certificats en vérifiant les points suivants :
  - La complétude du Dossier d'Enregistrement.
  - La signature du Représentant Légal sur la fiche d'Identification Gestionnaire de Certificats et le contrat d'abonnement.
  - La signature du futur Gestionnaire de Certificats sur la fiche d'Identification Gestionnaire de Certificats.
  - La cohérence entre les informations remplies dans la fiche d'Identification Gestionnaire de Certificats et le titre d'identité fourni d'une part (pour les informations d'identité personnelle), et le contrat d'abonnement (pour les informations concernant l'organisation) d'autre part.
- Le Chargé de Clientèle transmet le dossier d'enregistrement au Back Office Atos World Line pour archivage.
  - Remarque : L'agence ou le Service Banque / Pôle Service Clients doit posséder et conserver une copie du dossier d'enregistrement du Gestionnaire de Certificats. Les extraits originaux étant archivés par le Back Office Atos Worldline.

4) Enregistrement d'un porteur [Entreprise/Administration] via un Mandataire de Certification (ou Gestionnaire de Certificats)

Le présent paragraphe porte sur l'étape de validation de l'identité d'un futur Porteur dans le cadre de la procédure d'enregistrement de sa demande de certificat.

Le Client par l'intermédiaire de son Gestionnaire de Certificats se porte garant de la véracité des informations d'identité du Porteur. Les obligations du Gestionnaire de Certificats concernant l'étape de validation de l'identité sont décrites pour chaque Client dans le contrat d'abonnement et dans la Fiche d'Identification Gestionnaire de Certificats.

Dans tous les cas, le processus est le suivant :

- Le futur Porteur doit se déplacer auprès de son Gestionnaire de Certificats, muni d'un titre d'identité.
- Le Gestionnaire de Certificats vérifie en face-à-face l'identité du Porteur sur la base du titre d'identité présenté.
- Le Gestionnaire de Certificats photocopie le titre d'identité, y ajoute la mention « Certifié conforme à l'original » et le signe. Le Porteur doit également ajouter sa signature sur la photocopie du titre d'identité.
- Le Gestionnaire de Certificats s'assure que le futur Porteur est autorisé à utiliser des certificats pour le compte du Client.
- Le Gestionnaire de Certificats fait remplir au Porteur et signer le formulaire de Demande Individuelle Porteur. Il s'assure que les informations d'identité remplies sont conformes au titre d'identité présenté.
- Le Gestionnaire de Certificats transmet le dossier d'enregistrement au Chargé de Clientèle. Le dossier d'enregistrement d'un nouveau Porteur contient :

- Le formulaire de Demande Individuelle Porteur (DIP) daté de moins de 3 mois, rempli et signé à la fois par le futur Porteur et le GC.
  - Le formulaire de DIP contient les informations personnelles sur le futur Porteur nécessaires à la création du certificat (voir paragraphe 4.1.2).
  - Le formulaire DIP inclut les Conditions Générales d'Utilisation.
- La photocopie du titre d'identité du Porteur de Certificats, signé par le Gestionnaire de Certificats et par le Porteur.

3.2.4. Informations non vérifiées du porteur

Sans objet.

3.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée dans le cadre de la validation de l'identité du Porteur par le Gestionnaire de Certificats : le Gestionnaire de Certificats s'assure que le futur Porteur est autorisé à utiliser des certificats pour le compte du Client.

Cette vérification dépend entièrement du Client.

SG Trust Services vérifiera que la demande concerne l'un de ses Clients tel que décrit au paragraphe 1.3.3.

3.2.6. Certification croisée d'AC

L'AC SG TS 2 Etoiles ne fait l'objet d'aucune certification croisée avec une autre AC.

Le comité de pilotage de l'AC est chargé d'examiner les besoins éventuels de certification croisée avec d'autres AC, notamment dans le cadre du CFONB (Comité Français d'Organisation et de Normalisation Bancaire). L'AC qui pourra faire l'objet d'une certification croisée devra présenter un niveau de sécurité au moins équivalent à l'AC SG TS 2 Etoiles.

Le cas échéant, le comité de pilotage décidera et pilotera la réalisation de cette certification croisée.

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

Remarque : un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante.

3.3.1. Identification et validation pour un renouvellement courant

1) Cas du premier renouvellement

Le Porteur reçoit des notifications l'informant de l'arrivée à expiration de son certificat, 100 jours, 60 jours, 30 jours puis 15 jours avant la date de fin de validité de son certificat.

Remarque : le Gestionnaire de Certificats est en copie de la notification à 60 jours.

Ces notifications demandent au Porteur de signaler tout changement dans les informations d'identité ou d'organisation le concernant, et qu'il avait fournies lors de l'enregistrement initial (voir paragraphe 3.2.3.4).

Si ces informations n'ont pas changé, le dossier d'enregistrement est toujours valable, et la demande de renouvellement est validée par l'Autorité d'Enregistrement Déléguée.

Sinon, une nouvelle demande doit être faite par le Porteur, conformément à la procédure décrite au paragraphe 3.2.3.4).

2) Cas du second renouvellement

Le Porteur reçoit des notifications l'informant de l'arrivée à expiration de son certificat, 100 jours, 60 jours, 30 jours puis 15 jours avant la date de fin de validité de son certificat.

Remarque : le Gestionnaire de Certificats est en copie de la notification à 60 jours.

Ces notifications précisent la procédure à suivre pour le renouvellement du certificat : elle est identique à celle de l'enregistrement initial (voir paragraphe 3.2.3.4).

Le Porteur ainsi que le GC reçoivent un mail les informant de la procédure à suivre pour le renouvellement.

3.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial (voir paragraphe 3.2.3.4)

3.4. Identification et validation d'une demande de révocation

Toute demande de révocation est authentifiée et validée.

Les acteurs suivants peuvent être à l'origine d'une demande de révocation :

- Le Porteur via la révocation en ligne.
- Le Porteur, le Gestionnaire de Certificats ou le Représentant Légal via un formulaire papier.
- Les Opérateurs d'Enregistrement via les interfaces du Back Office.

3.4.1. Cas d'une révocation en ligne

Dans le cas d'une révocation en ligne par le Porteur, l'identification et la validation de la demande de révocation se déroulent de la manière suivante :

- Le Porteur se connecte au site web de SG Trust Services.
- Le Porteur accède à la fonction de révocation.
- Il s'authentifie via un jeu de 3 questions/réponses. Ces questions/réponses ont été configurées par le Porteur au moment du retrait du certificat (voir paragraphe 4.3).

L'Autorité de Certification vérifie la validité de ces questions / réponses et déclenche le cas échéant la suite du processus de révocation (voir paragraphe 4.9).

3.4.2. Cas d'une révocation via un formulaire papier

Dans ce paragraphe, on désigne par demandeur le Porteur, le Gestionnaire de Certificats ou le Représentant Légal.

Dans le cas d'une révocation par formulaire papier, le demandeur doit télécharger le formulaire de révocation au niveau du site de publication de SG Trust Services.

Le demandeur remplit et signe ce formulaire.

Le demandeur transmet le formulaire à l'AE Déléguée par courrier ou télécopie.

Un Opérateur d'Enregistrement au sein du Back Office Atos Worldline doit valider cette demande. Pour cela :

- L'Opérateur d'Enregistrement vérifie que le formulaire de révocation est entièrement rempli (il permet d'identifier le certificat à révoquer).
- L'Opérateur d'Enregistrement vérifie que le Porteur concerné existe.
- L'Opérateur d'Enregistrement vérifie la signature du demandeur, sur la base de signatures préalablement fournies (dans les dossiers d'enregistrement). Le demandeur doit être soit le Porteur, soit le Gestionnaire de Certificats, soit le Représentant Légal.

Le cas échéant, la validation de la demande déclenche la suite du processus de révocation (voir paragraphe 4.9).

3.4.3. Cas d'une révocation par un Opérateur d'Enregistrement

Un Opérateur d'Enregistrement du Back Office Atos World Line peut révoquer un certificat d'un Porteur dont il a la charge via une interface technique du Back Office.

Dans ce cas, l'Opérateur d'Enregistrement est authentifié fortement à l'aide d'un certificat sur support physique (délivré au sein de l'OSC).

4. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Une demande de certificat pour un Porteur doit émaner d'un Gestionnaire de Certificats.

Cette demande fait suite à l'étape de validation d'identité faisant intervenir le Porteur telle que décrite au paragraphe 3.2.

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

La demande de certificat pour un Porteur s'appuie sur un dossier d'enregistrement. Il comporte :

- Le formulaire de Demande Individuelle Porteur (DIP) daté de moins de 3 mois, complété et signé à la fois par le futur Porteur et le Gestionnaire de Certificats.
- La photocopie du titre d'identité du Porteur de Certificats, « certifiée conforme à l'original », et signée par le Gestionnaire de Certificats et par le Porteur.

Le formulaire de Demande Individuelle porteur (DIP) comporte les informations suivantes :

- Des données personnelles d'identification du Porteur :
  - Nom.
  - Prénom.
  - Adresse email.
  - Adresse postale.
  - Numéro de téléphone.
- Des données d'identification de l'organisation d'appartenance du Porteur
  - Nom de l'organisation (dénomination sociale).
  - Numéro de SIREN ou SIRET de l'organisation.

Remarque : le formulaire de Demande Individuelle porteur (DIP) contient les Conditions Générales d'Utilisation du certificat. La signature de ce formulaire vaut également signature des Conditions Générales d'Utilisation.

Le dossier d'enregistrement doit être transmis au Back Office Atos Worldline pour validation.

4.2. Traitement d'une demande de certificat

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

Le Chargé de Clientèle reçoit le dossier d'enregistrement de la part du Gestionnaire de Certificats. Ensuite, il procède à l'identification et à la validation de la demande de la manière suivante :

- Il vérifie la complétude du dossier d'enregistrement.
- Il vérifie l'origine de la demande. Le Gestionnaire de Certificats doit avoir été nommé conformément au processus décrit au paragraphe 3.2.3.3).
- Il vérifie la cohérence de la demande avec le titre d'identité présenté.

Si le dossier d'enregistrement est validé, le Chargé de Clientèle appose sa signature sur le formulaire DIP avant de transmettre le dossier d'enregistrement au Back Office Atos Worldline pour traitement. Sinon, il fait un retour au Gestionnaire de Certificats concernant la non-conformité de la demande.

Le Back Office Atos Worldline reçoit le dossier d'enregistrement validé de la part du Chargé de Clientèle.

- Un Opérateur de saisie vérifie l'authenticité de la signature du Chargé de Clientèle. Puis il saisit la demande au niveau des interfaces techniques.

  Remarque : l'accès aux interfaces techniques est authentifié par certificats. Les certificats utilisés proviennent de l'AC « SG TS 2 ETOILES ».

- Un Opérateur de validation, vérifie la cohérence des informations saisies par l'Opérateur de saisie avec celles figurant dans le dossier d'enregistrement avant de valider techniquement la demande.

La validation technique de la demande déclenche la génération d'une URL de retrait personnalisée pour le Porteur, ainsi que d'un code de retrait généré aléatoirement permettant l'authentification du Porteur lors de l'accès à cette URL. Le Porteur reçoit dans deux mails distincts :

- D'abord le code de retrait
  - Remarque : le mail précise la procédure à suivre pour le retrait du certificat.
- Ensuite l'URL de retrait
  - Le mail contenant l'URL de retrait est envoyé au moins 4 heures après l'envoi du code de retrait, afin d'éviter les risques d'interception par un tiers à la fois de l'URL et du code de retrait.
  - L'accès à cette URL est sécurisé via le protocole HTTPS.

Un Opérateur d'Enregistrement doit ensuite envoyer un support physique au Porteur, à l'adresse qui a été renseignée dans le formulaire DIP.

4.2.2. Acceptation ou rejet de la demande

L'étape de validation décrite au paragraphe précédent (paragraphe 4.2.1) peut conduire à l'acceptation ou au rejet de la demande.

En cas de rejet de la demande, le Chargé de Clientèle fait un retour au Gestionnaire de Certificats concernant la non-conformité de la demande.

4.2.3. Durée d'établissement du certificat

À partir de la réception d'un dossier d'enregistrement pour un Porteur par le Back Office Atos World Line, le traitement de la demande se fait dans un délai maximum de 48h.

À l'issue de ce traitement, un support physique ainsi que les deux mails contenant l'URL de retrait et le code de retrait sont envoyés dans un délai de 24h.

Suite à la réception de ces deux mails et du support physique, la durée d'établissement du certificat dépend essentiellement du porteur qui est à l'origine du retrait de ce certificat. Le temps nécessaire au retrait du certificat (paragraphe 4.3) ainsi qu'à l'acceptation (paragraphe 4.4) est d'environ dix minutes.

Il est à noter que l'URL de retrait envoyée au Porteur a une durée de validité limitée à 30 jours calendaires. A l'issue de ce délai, SG Trust Services supprimera les Certificats correspondants sans préavis.

4.3. Délivrance du certificat

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

Ce paragraphe fait suite au paragraphe 3.2 qui présente l'étape de validation de l'identité et l'enregistrement d'un futur Porteur et au paragraphe 4.2 qui présente le traitement de la demande par l'Autorité d'Enregistrement Déléguée.

L'étape de délivrance du certificat par l'AC (ou de retrait du certificat par le Porteur) se déroule de la manière suivante :

- Le Porteur reçoit par courrier le support physique. Le support physique est associé à un code PIN initial par défaut.
- Le Porteur change le code PIN de son support physique.
  - Remarque 1 : le certificat ne peut pas être retiré si le code PIN initial par défaut n'a pas été changé par le Porteur.
  - Remarque 2 : le code PIN doit être conforme à la politique de code PIN qui lui est rappelée par l'outil (voir paragraphe 4.3.1).
- Le Porteur se connecte à l'URL de retrait et s'authentifie à l'aide de son code de retrait.
- Le Porteur configure une liste de 3 questions secrètes à partir d'une liste de questions pré-définies.
  - Ces questions secrètes serviront à authentifier le Porteur lors d'une demande de révocation.
- Le Porteur génère une bi-clé dans son support physique (c'est la personnalisation électrique du support physique).
- Le Porteur envoie une demande de certificat au format PKCS#10 à l'Autorité de Certification, sur la base de la clé publique qu'il vient de générer.
- L'Autorité de Certification génère le certificat et le signe.
- Le Porteur récupère son certificat et l'insère au niveau de son support physique.
- Le Porteur est dirigé vers une page de test de son certificat (voir paragraphe 4.4).

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

Après la délivrance du certificat par l'Autorité de Certification, le Porteur reçoit un mail de confirmation du retrait.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat par le Porteur est explicite. Elle prend la forme d'un test cryptographique consistant en une signature.

Le Porteur, après avoir retiré son certificat, est invité à effectuer un test de signature sur le site de SG Trust Services. Ce test vaut acceptation du certificat et une trace en sera conservée par l'AE Déléguée.

Le Porteur est averti qu'en l'absence d'une trace de test au-delà d'un délai de 7 jours, l'AE Déléguée en déduira que le certificat n'a pas été accepté. Dans ce cas, l'AE Déléguée contactera le Porteur afin de vérifier sa situation. Si le Porteur refuse son Certificat, ou s'il ne donne pas de réponse, l'AE Déléguée révoquera son certificat.

4.4.2. Publication du certificat

Les certificats ne sont pas publiés après leur délivrance.

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

Suite à la délivrance du certificat, le Chargé de Clientèle et le Gestionnaire de Certificats sont automatiquement notifiés par mail.

4.5. Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée et du certificat doit être conforme aux usages prévus au paragraphe 1.4.

Les Conditions Générales d'Utilisation incluses dans le formulaire DIP rappellent ces usages.

De plus, le certificat les mentionne explicitement dans des champs dédiés (voir le paragraphe 7).

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

Les utilisateurs de certificats doivent respecter les usages autorisés des certificats tels que prévus au paragraphe 1.4.

4.6. Renouvellement d'un certificat

La RFC 3647 définit l'opération de renouvellement d'un certificat comme la génération d'un certificat dont seules les dates de validité ont changé par rapport au certificat précédent.

Si des données ont changé concernant l'identité du Porteur ou son organisation, une nouvelle demande de certificat doit être réalisée (voir le paragraphe 4.1).

Par ailleurs, conformément à la Politique de Certification type pour le profil « Signature » de l'Annexe A du RGS, le renouvellement d'un certificat doit s'accompagner d'un renouvellement de la bi-clé correspondante.

La présente Politique de Certification traite donc du renouvellement des certificats au paragraphe 4.7 « Délivrance d'un nouveau certificat suite à changement de la bi-clé ».

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2. Origine d'une demande de renouvellement

Sans objet.

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

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

Sans objet.

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6. Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

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

Les bi-clés émises pour les certificats des porteurs, par l'AC SG TS 2 ETOILES, ont une durée de validité de 3 ans.

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

- L'arrivée à expiration du certificat, 30 jours avant la date de fin de validité du certificat.
- Une nouvelle demande suite à la révocation du certificat.

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

Le Porteur reçoit des notifications l'avertissant de l'arrivée à expiration de son certificat 100 jours, 60 jours, 30 jours et 15 jours avant la date de fin de validité du certificat.

Une fois le renouvellement effectué, les notifications s'arrêtent.

Les notifications rappellent la procédure à suivre. Elle est différente dans le cas d'un premier ou d'un second renouvellement (voir le paragraphe 4.7.3).

Si la demande de nouveau certificat fait suite à une révocation, la procédure de demande de nouveau certificat est identique à la procédure de demande initiale (voir le paragraphe 4.1).

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

La procédure de traitement d'une demande d'un nouveau certificat est différente entre un premier et un second renouvellement.

Dans tous les cas, la demande d'un nouveau certificat s'accompagne du changement de support physique.

Dans le cas d'un second renouvellement (six ans après l'émission du certificat), la demande d'un nouveau certificat se déroule de manière identique à la demande initiale (voir les paragraphes 4.1, 4.2, et 4.3).

Dans le cas d'un premier renouvellement, le processus de demande d'un nouveau certificat se déroule de la manière suivante.

- L'Autorité d'Enregistrement Déléguée envoie des notifications au Porteur et au Gestionnaire de Certificats, les informant de l'arrivée à expiration du certificat.
  - Une notification est envoyée par mail au Gestionnaire de Certificats 100 jours avant la date d'expiration, pour information.
  - Une notification est envoyée par mail au Gestionnaire de Certificats ainsi qu'au Porteur 60 jours avant la date d'expiration.
    - Cette notification demande au Porteur de communiquer les informations d'identité ou d'organisation qui auraient changé. Si c'est le cas, le Porteur doit faire une nouvelle demande (voir paragraphe 4.1).
  - Deux mails consécutifs sont envoyés au Porteur 30 jours avant la date d'expiration.
    - Un premier mail contient un code de retrait généré aléatoirement.
    - Un second mail, envoyé quatre heures après, contient une URL de retrait personnalisée et sécurisée.
  - Une dernière notification est envoyée par mail au Porteur 15 jours avant la date d'expiration.
- Le Porteur reçoit par courrier un nouveau support physique (avant réception de l'URL de retrait).
- Le Porteur doit modifier le code PIN de son nouveau support physique.
- Le Porteur se connecte à l'URL de retrait et saisit son code de retrait pour s'authentifier.
- Le Porteur réalise la personnalisation électrique du nouveau support physique et retire son certificat.
- Le Porteur accepte son certificat de manière explicite (voir paragraphe 4.6.5).

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

Identique à la demande initiale (voir paragraphe 4.3.2).

4.7.5. Démarche d'acceptation du nouveau certificat

La démarche d'acceptation du nouveau certificat est explicite. Elle est identique à l'acceptation lors de la demande initiale (voir paragraphe 4.4.1).

4.7.6. Publication du nouveau certificat

Identique à la demande initiale (voir paragraphe 4.4.2).

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

Identique à la demande initiale (voir paragraphe 4.4.3).

4.8. Modification du certificat

La modification de certificat n'est pas autorisée dans la présente Politique de Certification.

4.8.1. Causes possibles de modification d'un certificat

Sans objet.

4.8.2. Origine d'une demande de modification d'un certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.8.5. Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6. Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

1) Certificats de Porteurs

Un certificat Porteur doit être révoqué dans les cas suivants :

- Violation du Contrat d'Abonnement (ou de tout autre contrat joint au dossier d'enregistrement) par un Porteur, un Gestionnaire de Certificats ou le Client.
- La résiliation du contrat d'abonnement dans le cadre duquel le certificat a été émis.
- Non-respect de la PC et des Conditions Générales d'Utilisation.

- Les informations relatives à l'identité du Porteur figurant dans le certificat ou dans le dossier d'enregistrement ne sont plus exactes.
- Le décès du Porteur, son départ de l'entité du Client ou la perte de son habilitation, donnée par le Client, d'utiliser des certificats.
- La clé privée du Porteur est suspectée de compromission ou est compromise.
- La perte ou vol des données confidentielles (clés privées et données d'activation).
- La perte ou vol du support physique sur lequel est stocké le certificat.
- La cessation d'activité du Client ou celle de l'entité du Porteur.
- Le certificat de l'AC est révoqué (ce qui entraîne la Révocation de tous les Certificats signés par la Clé Privée correspondante).
- Le Porteur, le Gestionnaire de Certificat, le Représentant Légal du Client, ou l'Autorité d'Enregistrement Déléguée fait une demande de révocation du certificat Porteur.

2) Certificats d'une composante de l'IGC

Un certificat de composante de l'IGC doit être révoqué dans les cas suivants :

- 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 elle suite à un audit de qualification ou de conformité négatif).
- Cessation d'activité de l'entité opérant la composante.

4.9.2. Origine d'une demande de révocation

1) Certificats de Porteurs

Les personnes ou entités qui peuvent demander la révocation d'un certificat de Porteur sont les suivantes :

- Le Porteur au nom duquel le certificat a été émis.
- Le Gestionnaire de Certificats.
- Un Représentant légal du Client.
- L'AC émettrice du certificat.
- L'Autorité d'Enregistrement Déléguée.

Le Porteur est informé des personnes ou entités susceptibles d'effectuer une demande de révocation pour son certificat, via les Conditions Générales d'Utilisation.

2) Certificats d'une composante de l'IGC

La révocation du certificat de l'AC SG TS 2 ETOILES ne peut être décidée que par le responsable de l'AC ou par des autorités judiciaires via une décision de justice.

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

4.9.3. Procédure de traitement d'une demande de révocation

1) Révocation d'un certificat Porteur

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

La révocation d'un certificat Porteur peut être réalisée selon les processus suivants :

- En self-service par le Porteur.
- Via un formulaire papier par le Porteur, le Gestionnaire de Certificats ou le Représentant Légal.
- Via une interface technique du Back Office par les Opérateurs d'Enregistrement.

Le processus de révocation en self-service par le Porteur se déroule de la manière suivante :

- Le Porteur se connecte au site web de SG Trust Services et accède à la fonction de révocation. Voir le paragraphe 3.4.1 pour la validation de son identité.
- Le Porteur sélectionne son certificat.
- Le Porteur saisit un motif de révocation de manière optionnelle.
- Le Porteur envoie la demande.
- L'Autorité de Certification révoque le certificat et met à jour la CRL correspondante.
- Une notification par mail est envoyée au Porteur ainsi qu'au Chargé de Clientèle après la révocation du certificat concerné.

Le processus de révocation via un formulaire papier par le Porteur, le Gestionnaire de Certificats ou le Représentant Légal se déroule de la manière suivante :

- Le demandeur remplit le formulaire de révocation et le transmet à l'Autorité d'Enregistrement Déléguée tel que décrit au paragraphe 3.4.2.
- L'Opérateur d'Enregistrement qui a validé l'identité du demandeur accède à une interface technique pour saisir la demande.
- L'Opérateur d'Enregistrement sélectionne le certificat (en le recherchant sur l'adresse email du Porteur).
- L'Opérateur d'Enregistrement saisit un motif de révocation de manière optionnelle.
- L'Opérateur d'Enregistrement envoie la demande.
- L'Autorité de Certification révoque le certificat et met à jour la CRL correspondante.
- Une notification par mail est envoyée au Porteur ainsi qu'à l'Autorité d'Enregistrement (Back Office Atos World Line) après la révocation du certificat concerné.

Le processus de révocation par l'Autorité d'Enregistrement Déléguée via une interface technique se déroule de la manière suivante :

- L'Opérateur d'Enregistrement se connecte à l'interface technique et accède à la fonction de révocation. Son identité est validée comme décrit au paragraphe 3.4.3.
- L'Opérateur d'Enregistrement sélectionne le certificat (en le recherchant sur l'adresse email du Porteur).

- L'Opérateur d'Enregistrement saisit un motif de révocation de manière optionnelle.
- L'Opérateur d'Enregistrement envoie la demande.
- L'Autorité de Certification révoque le certificat et met à jour la CRL correspondante.
- Une notification par mail est envoyée au Porteur ainsi qu'au Chargé de Clientèle après la révocation du certificat concerné.

L'opération est enregistrée dans les journaux d'événement de l'AC.

2) Révocation d'un certificat d'une composante de l'IGC

La décision de révocation d'un certificat d'AC sera prise par le responsable de l'Autorité de Certification. Il en informera aussitôt les Chargés de Clientèle et l'OSC.

L'Autorité d'Enregistrement Déléguée en informera les Porteurs et les Gestionnaires de Certificats.

Le responsable de l'Autorité de Certification en informera également la DGME le cas échéant (à partir du référencement de l'AC par la DGME).

La décision de révoquer un certificat d'une autre composante de l'IGC (sous la responsabilité de l'OSC) devra être soumise par l'OSC au Responsable de l'Autorité de Certification au préalable. Les impacts de cette révocation seront étudiés, et des mesures prises en conséquence.

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

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

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

1) Révocation d'un certificat Porteur

La fonction de révocation en self-service par le Porteur est disponible en 24h/24 7j/7 et permet de prendre en charge et traiter de manière urgente les demandes de révocation. L'information de révocation sera publiée aux utilisateurs dans un délai de 24h.

Par ailleurs cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée maximale totale d'indisponibilité par mois de 8h.

Les autres demandes de révocation sont traitées en fonction de la disponibilité du Back Office Atos World Line.

- Disponibilité de l'équipe en jours et heures ouvrés.
- Délai total de prise en charge des demandes et de traitement à partir de leur prise en charge (incluant la publication de la CRL) : 24h.

Les Porteurs n'utilisant leurs certificats généralement qu'en jours et heures ouvrés, la disponibilité de la fonction de révocation via le Back office convient bien à ce contexte d'utilisation.

Les interfaces techniques du Back Office Atos World Line permettant de traiter ces autres demandes de révocation ont les propriétés suivantes :

- Taux de disponibilité : 24h/24, 7j/7.
- Durée maximale d'indisponibilité par interruption de service : 2h.
- Durée maximale totale d'indisponibilité par mois : 8h.

2) Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'AC ou d'une composante de l'IGC est effectuée immédiatement par l'OSC dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat (voir paragraphe 4.9.2.2) et suite à la prise de décision du Responsable d'AC.

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.

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

Les utilisateurs des certificats délivrés par l'AC SG TS 2 ETOILES tels que définis au paragraphe 1.3.4 doivent vérifier l'état du certificat de l'Autorité de Certification, et des certificats constituant la chaîne de certification.

La méthode utilisée est à l'appréciation de l'utilisateur selon ses besoins de disponibilité ou les contraintes liées à son application.

L'accès aux listes des certificats révoqués est possible via le serveur de publication de la CRL (voir paragraphe 2.2).

4.9.7. Fréquence d'établissement des LCR

Les LCR sont établies et publiées toutes les 24 heures.

4.9.8. Délai maximum de publication d'une LCR

Après sa génération, la LCR est publiée dans un délai maximum de 30 minutes.

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

Aucun service OSCP n'est mis en œuvre.

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

Sans objet.

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

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

Pour les certificats de Porteurs, les entités autorisées à effectuer une demande de révocation l'effectuent dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée sur le site Internet de l'AC.

4.9.13. Causes possibles d'une suspension

La présente Politique de Certification n'autorise pas la suspension de certificats.

4.9.14. Origine d'une demande de suspension

Sans objet.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

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

Sans objet.

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

4.10.1. Caractéristiques opérationnelles

Les LCR / LAR sont des LCR au format V2 et sont publiées sur le serveur web HTTP de publication.

Les accès en lecture aux LCR / LAR sont publics.

4.10.2. Disponibilité de la fonction

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

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4h et une durée maximale totale d'indisponibilité par mois de 16h.

4.10.3. Dispositifs optionnels

Sans objet.

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

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

4.12. Séquestre de clé et recouvrement

Il n'est pas procédé à un séquestre de clé.

4.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5. MESURES DE SÉCURITÉ NON TECHNIQUES

Ce chapitre présente un ensemble de mesures non techniques concernant la sécurité de l'IGC. Des précisions et des compléments sur la mise en œuvre de ces mesures sont donnés dans la DPC.

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

La construction des sites respecte les règlements et normes en vigueur.

La localisation géographique des sites ne présente pas de risque concernant les tremblements de terre, les explosions ou les inondations.

5.1.2. Accès physique

Un système de contrôle d'accès nominatif est mis en place. Il est strictement limité aux seules personnes autorisées, en présence d'une autre personne autorisée. Il garantit en outre la traçabilité des accès.

Il contrôle :

- L'accès physique aux fonctions de génération des certificats, génération des éléments secrets du porteur et de gestion des révocations
- L'accès physique aux données sensibles : HSM contenant les clés d'AC, coffres-forts contenant les données d'activation, journaux d'événements.

En dehors des heures ouvrables, des mesures de détection d'intrusion physique et logique sont mises en œuvre.

5.1.3. Alimentation électrique et climatisation

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

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

Pour cela, des installations de secours sont prévues concernant l'alimentation électrique et la climatisation.

5.1.4. Vulnérabilité aux dégâts des eaux

La vulnérabilité aux dégâts des eaux a été prise en compte pour l'élaboration des mesures de sécurité. Elles permettent de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

Des moyens de protection contre les dégâts des eaux sont prévus.

5.1.5. Prévention et protection incendie

Les risques d'incendie ont été pris en compte pour l'élaboration des mesures de sécurité. Elles permettent de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

Des moyens de prévention et de lutte contre les incendies sont prévus.

5.1.6. Conservation des supports

Les informations nécessaires aux activités de l'IGC sont listées. Elles sont classifiées selon leurs besoins en intégrité, confidentialité, disponibilité et traçabilité. Leurs supports de conservation sont identifiés.

En fonction de leur place dans la classification et en fonction du type de support, des moyens sont mis en place pour garantir l'intégrité et la confidentialité des informations.

Des moyens spécifiques sont mis en place pour la conservation dans le temps de ces supports.

5.1.7. Mise hors service des supports

Des moyens sont prévus pour détruire ou réinitialiser de manière sécurisée les supports des informations de l'IGC, lorsque ces informations ne doivent plus être conservées.

La destruction ou la réinitialisation dépendra du niveau des informations dans la classification.

5.1.8. Sauvegardes hors site

Un site de secours est utilisé pour la sauvegarde des informations.

Des procédures de sauvegarde sont définies. Elles permettent les reprises suite à un incident, en respectant les exigences de disponibilité de la présente PC (notamment concernant les fonctions de gestion des révocations et d'information sur l'état des certificats).

Les procédures de sauvegarde sont réalisées par des rôles de confiance dans le but de protéger l'intégrité et la confidentialité des informations.

La DPC donne plus de détails sur ces sauvegardes.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Les opérations réalisées au sein de l'OSC sont classées selon leur niveau de sensibilité. Les opérations sensibles suivent des procédures définies qui s'appuient sur les rôles de confiance. Ces procédures respectent les principes de séparation des responsabilités et du moindre privilège.

La DPC décrit les rôles de confiance propres à l'OSC.

De plus, l'Autorité de Certification compte les rôles de confiance suivants :

- Responsable de l'Autorité de Certification : voir paragraphe **Erreur ! Source du renvoi introuvable.**. Le Responsable de l'Autorité de Certification décide de la création de l'Autorité de Certification, ou a été désigné par le précédent Responsable de l'Autorité de Certification.
  - Un document désignant nominativement le nouveau Responsable de l'Autorité de Certification et signé par le précédent Responsable de l'Autorité de Certification est conservé par le Responsable de l'Autorité de Certification en poste.
- Chargé de clientèle : voir paragraphe **Erreur ! Source du renvoi introuvable.**. Le Chargé de Clientèle a une fonction métier au sein du Groupe Société Générale.
  - Le document d'« instruction pour le réseau Certificats électroniques » établit ses attributions concernant les certificats. Le Chargé de Clientèle signe ce document et le retourne à l'AE Déléguée.
  - L'AE Déléguée détient la liste nominative des Chargés de Clientèle gérant des certificats.

Remarque : l'Autorité de Certification est régie par un comité de pilotage présidé par le Responsable de l'Autorité de Certification.

Ce comité de pilotage, tenu sur une base annuelle (revue de direction), décide des orientations fonctionnelles concernant le fonctionnement de l'Autorité de Certification. Il pilote la prestation de l'OSC en charge de délivrer les services techniques répondant aux missions de l'Autorité de Certification.

5.2.2. Nombre de personnes requises par tâches

En fonction des opérations réalisées, une ou plusieurs personnes avec des rôles différents seront requises.

La DPC précise pour chaque type d'opération le nombre de personnes et de rôles requis.

5.2.3. Identification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement de l'IGC doit avoir préalablement reçu le rôle correspondant.

La procédure d'habilitation correspondante est définie. Elle est détaillée dans la DPC.

L'affectation d'un rôle est tracée.

Le rôle peut donner les habilitations suivantes :

- Accès physique aux locaux et jusqu'aux systèmes.

- Accès logique aux services techniques, à l'aide d'un compte et d'un authentifiant (le cas échéant, un certificat).

5.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être affectés à une même personne, quand la définition du rôle le permet.

Les cumuls de rôles de confiance suivants sont interdits :

- Responsable de sécurité et ingénieur système ou opérateur.
- Contrôleur et tout autre rôle.
- Ingénieur système et opérateur.

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

5.3.1. Qualifications, compétences et habilitations requises

Le personnel travaillant pour l'une des composantes de l'IGC est soumis à une clause de confidentialité vis-à-vis de son employeur.

Les fonctions demandées à chaque membre du personnel doivent être compatibles avec ses compétences. Notamment, le personnel d'encadrement doit avoir l'expertise nécessaire et être familier des procédures de sécurité.

L'Autorité de Certification informe chaque personne disposant d'un rôle de confiance :

- De ses responsabilités relatives aux services de l'IGC.
- Des procédures qu'elle doit respecter, concernant la sécurité du système et le contrôle du personnel.

Les rôles de confiance sont affectés par des personnes exerçant elles-mêmes une fonction de sécurité. Elles sont précisées dans la procédure d'habilitation décrite par la DPC.

5.3.2. Procédures de vérification des antécédents

Le personnel travaillant pour l'une des composantes de l'IGC est soumis à une procédure de vérification de ses antécédents lors de leur prise de fonction.

Pour les rôles de confiance, des vérifications sont menées en plus tous les 3 ans.

Les vérifications porteront sur les points suivants :

- Les éventuelles condamnations en justice de la personne ne devront pas être contraires à ses fonctions.
- Les rôles de confiance ne devront pas se trouver dans un conflit d'intérêt préjudiciable à l'impartialité de leurs tâches.

A cet effet, les membres du personnel devront fournir le bulletin n°3 de leur casier judiciaire.

5.3.3. Exigences en matière de formation initiale

Le personnel travaillant pour l'une des composantes de l'IGC sera préalablement formé. Cette formation lui permettra notamment de prendre conscience des enjeux de sécurité liés à sa fonction.

5.3.4. Exigences et fréquence en matière de formation continue

En fonction des évolutions apportées au fonctionnement de l'IGC (concernant les systèmes techniques ou les procédures), le personnel recevra une formation, ou les informations nécessaires à la bonne réalisation de ses activités.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Des changements dans les affectations de rôles pourront avoir lieu soit en cas de départ, ou de mutation d'un membre du personnel, soit suite à un audit.

5.3.6. Sanctions en cas d'actions non autorisées

La DPC précise ou fait référence aux sanctions prévues en cas d'actions non autorisées. Elles sont communiquées au personnel avant la prise de fonction.

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

Les exigences du paragraphe 5.3 sont applicables aux prestataires externes. Ces exigences sont explicitées dans les contrats avec les prestataires.

5.3.8. Documentation fournie au personnel

Le personnel a accès à la documentation concernant les procédures et les systèmes techniques qui le concernent dans le cadre de ses fonctions. Notamment il a accès à la politique de sécurité correspondante.

La DPC donne les moyens d'accéder à cette documentation.

5.4. Procédures de constitution des données d'audit

5.4.1. Type d'évènements à enregistrer

Les événements listés ci-dessous concernant l'ensemble des composantes de l'IGC.

Les événements suivants doivent être enregistrés de manière automatique :

- 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.

Les événements suivants doivent être enregistrés, de manière automatique ou manuelle :

- Accès physiques.
- Actions de maintenance et de changements de la configuration des systèmes
- Changements apportés au personnel.

- Actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

De plus, concernant la gestion du cycle de vie des certificats, les événements ci-dessous doivent être enregistrés de manière automatique ou manuelle :

- 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 (*Key Ceremony*), sauvegarde / récupération, révocation, renouvellement, destruction,...).
- Génération des éléments secrets du porteur (bi-clé, codes d'activation,…).
- Génération des certificats des porteurs.
- Transmission des certificats aux porteurs et acceptations / rejets explicites par les porteurs.
- Remise de son dispositif de création de signature au porteur.
- 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.

Pour chaque événement, les informations suivantes doivent être enregistrées :

- Type de l'évènement.
- Nom / identifiant 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).

De plus pour les événements concernant les certificats, les informations suivantes devront être enregistrées :

- Destinataire de l'opération (Porteur du certificat).
- 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.
- Autre information caractérisant l'évènement (notamment, pour la génération d'un certificat, le numéro de série de ce certificat).

Les événements à journaliser automatiquement sont enregistrés au cours du processus. Les événements qui sont journalisés manuellement doivent l'être le même jour ouvré que l'événement.

5.4.2. Fréquence de traitement des journaux d'évènements

Les journaux d'événement sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins une fois par semaine, et dès la détection d'une anomalie. Cette analyse donne lieu à un résumé qui fait apparaître les événements importants ainsi qu'une explication. Le résumé fait notamment apparaître les anomalies et les éventuelles falsifications.

Le rapprochement entre journaux d'événements de fonctions interagissant entre elles est réalisé une fois par mois. Il vise à vérifier la concordance et l'exactitude des informations fournies par les journaux d'événement. Ce rapprochement pourra donner lieu à la détection d'anomalie.

5.4.3. Période de conservation des journaux d'évènements

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

Ils sont archivés au plus tard un mois après leur génération.

5.4.4. Protection des journaux d'évènements

Le mode de conservation des journaux d'événements protège leur intégrité, et leur disponibilité.

De plus, un mécanisme de contrôle d'intégrité est mis en place.

Le niveau de confidentialité de chaque type d'événement a été classé. Les moyens de protection de la confidentialité des journaux sont adaptés à cette classification.

Le système de datation des événements respecte les exigences du paragraphe 6.8.

5.4.5. Procédure de sauvegarde des journaux d'évènements

Les journaux d'événements sont sauvegardés sur le site de secours.

5.4.6. Système de collecte des journaux d'évènements

Voir le paragraphe 5.4.1 pour les modes de collecte (manuel ou automatique) en fonction des types d'événements.

De plus un système de collecte des journaux d'événements sur chacun des systèmes permet de récupérer ces journaux pour la sauvegarde ou l'archivage.

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

Sans objet.

5.4.8. Évaluation des vulnérabilités

L'OSC met en œuvre des campagnes de détection des vulnérabilités sur ses systèmes, et notamment sur les journaux d'événements.

5.5. Archivage des données

5.5.1. Types de données à archiver

En plus des journaux d'événements, un certain nombre de données sont archivées par l'Autorité de Certification.

Les données archivées sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques.
- Les Politiques de Certification.
- Les DPC.
- Les éventuels accords contractuels avec d'autres AC.
- Les certificats et LCR tels qu'émis ou publiés.
- Les notifications (à titre informatif).
- Les engagements signés des Gestionnaires de Certificats.
- Les titres d'identité des Porteurs et, le cas échéant, de leur entité de rattachement.
- Les journaux d'évènements des différentes entités de l'IGC.

5.5.2. Période de conservation des archives

Les dossiers d'enregistrement sont conservés dans un local sécurisé à disposition du Back Office Atos Worldline. Ils sont archivés pendant toute la durée du contrat d'abonnement du Client. Après la résiliation de ce dernier les dossiers seront conservés pendant une durée de 5 ans.

Les autres type de données archivées tels que listés au paragraphe 5.5.1 sont conservés pendant cinq ans.

5.5.3. Protection des archives

Des moyens sont mis en place pour protéger les archives et leurs sauvegardes en intégrité et en confidentialité.

Par ailleurs, les archives et leurs sauvegardes peuvent être accédées par les personnes autorisées pour lecture et exploitation.

5.5.4. Procédure de sauvegarde des archives

Une procédure de sauvegarde des archives est définie. La DPC décrit les moyens mis en œuvre.

5.5.5. Exigences d'horodatage des données

Les journaux d'événements doivent être datés (voir le paragraphe 5.4.4).

Le paragraphe 6.8 précise les exigences relatives au système de datation des événements.

5.5.6. Système de collecte des archives

Un système de collecte des archives est mis en place. Il respecte les exigences du paragraphe 5.5.3.

5.5.7. Procédures de récupération et de vérification des archives

Seule l'AC peut accéder à l'ensemble des archives. Les composantes de l'IGC ne peuvent accéder qu'aux archives de la composante.

Le circuit de demande et validation d'accès à une archive est explicité dans la DPC.

Le délai de récupération d'une archive est inférieur à 2 jours ouvrés.

5.6. Changement de clé d'AC

L'Autorité de Certification a une durée de validité de 10 ans. Les certificats qu'elle émet ont une durée de vie de 3 ans.

Conformément à la Politique de Certification type de l'Annexe A du RGS pour le profil « Signature », l'AC ne peut pas émettre de certificat qui serait encore valide au moment de la date de fin de validité de l'AC.

Pour ce faire, le dernier certificat émis par l'AC le sera sept ans avant la date de fin de validité de l'AC.

Le certificat d'AC sera renouvelé. Tous les nouveaux certificats Porteurs devront être signés par le nouveau certificat d'AC.

L'ancien certificat d'AC servira pour valider les certificats précédemment émis, et pour signer les CRL.

5.7. Reprise suite à compromission et sinistre

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

Des procédures de remontée et de traitement des incidents sont mises en place par l'OSC. La DPC détaille le fonctionnement de ces procédures.

Ces procédures s'appuient notamment sur le personnel de l'OSC et sur les journaux d'événements.

Dans le cas d'un incident majeur tel que la compromission d'une clé d'AC, le responsable de l'Autorité de Certification en est informé dans les plus brefs délais. Les incidents majeurs sont traités en première urgence. Cela peut donner lieu à la révocation d'un certificat d'AC (voir paragraphes 4.9.3.2) et 4.9.5.2).

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

Le plan de reprise d'activité de l'OSC définit les modalités de reprise en cas de corruption des ressources informatiques. La DPC donne plus d'informations sur ces modalités.

Le plan de continuité d'activité de l'OSC est testé une fois tous les deux ans.

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

Le cas de compromission de la clé privée d'une composante est traité dans le cadre des plans de continuité et de reprise d'activité de l'OSC.

La compromission de la clé privée d'une composante donne lieu à la révocation du certificat (voir paragraphe 4.9.2.2).

Dans ce cas, l'AC communique auprès des personnes ou entités concernées (voir paragraphe 4.9.12.

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

La capacité de continuité d'activité suite à un sinistre est traitée dans le cadre du plan de continuité d'activité de l'OSC.

5.8. Fin de vie de l'IGC

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

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

Les dispositions présentées ci-dessous, quand elles concernent l'OSC, figurent dans le contrat entre l'AC et l'OSC.

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 affectant une composante de l'IGC

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

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

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

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

- Le cas échéant (référencement de l'AC par la DGME), l'AC communiquera au 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 communiquera 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 porteurs et les utilisateurs de certificats.
- Le cas échéant (référencement de l'AC par la DGME), l'AC tiendra 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 l'AC, ou une entité tierce qui reprend les activités, soit capable de reprendre les activités.

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

Le contrat entre l'AC et l'OSC stipule les dispositions prises en cas de cessation de service. Elles concernent notamment :

- La notification des entités affectées.
- Le transfert des obligations de l'OSC 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, une *Key Ceremony* aura lieu afin de désactiver les clés privées d'AC, révoquer les certificats d'AC et des Porteurs encore valides.

L'AC informera les Clients, les Gestionnaires de Certificats et les Porteurs de la fin de vie de l'AC.

6. MESURES DE SÉCURITÉ TECHNIQUES

Ce chapitre présente un ensemble de mesures techniques concernant la sécurité de l'IGC. Des précisions et des compléments sur la mise en œuvre de ces mesures sont donnés dans la DPC.

6.1. Génération et installation de bi-clés

6.1.1. Génération des bi-clés

1) Clés d'AC

La génération des clés de signature de l'AC SG TS 2 ETOILES a lieu lors d'une *Key Ceremony* (cérémonie de clés*).* Cette cérémonie se déroule sur le site de Vendôme sous le contrôle du maître de cérémonie et d'au moins deux membres du comité de pilotage de l'Autorité de Certification.

Remarque : les différents rôles participant à la *Key Ceremony* sont cités dans la DPC et sont nommés dans la documentation relative à la *Key Ceremony*.

Un auditeur externe sera présent lors de cette cérémonie et veillera à la bonne application des procédures et au respect des exigences de sécurité définies dans la présente Politique de Certification et dans la Déclaration des Pratiques de Certification.

La génération des clés de signature de l'AC doit être précédée de l'initialisation du HSM réalisée à l'aide d'une carte d'initialisation. Cette étape donne lieu à la création d'une carte d'administration.

- Cette carte est attribuée à un Porteur de secret.
- Elle est placée dans un coffre.
- Deux autres Porteurs de secrets ayant des rôles distincts sont nécessaires pour utiliser la carte d'administration.

Remarque : cette procédure fait partie du déroulement de la *Key Ceremony* et est documentée et les Porteurs de secrets y sont nommément identifiés.

2) Clés Porteurs générées par l'AC

Sans objet. Les clés des Porteurs sont générées par le Porteur sous son contrôle exclusif.

3) Clés Porteurs générées par le Porteur

La génération de la bi-clé du Porteur se fait par le Porteur dans un module cryptographique matériel (support physique, voir la définition au paragraphe 1.6.2).

Le support physique est sous le contrôle exclusif du Porteur qui en a la responsabilité. L'accès à ce support physique est protégé par un code PIN personnel au Porteur.

SG Trust Services exige des Porteurs le respect du Contrat d'Abonnement, notamment les conditions relatives à la conservation des Clés Privées. SG Trust Services décline toute responsabilité quant aux litiges liés à de mauvais modes de conservation des Clés Privées.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée de l'AC est générée directement dans le HSM, et y reste confinée. Elle ne peut être utilisée qu'à partir de ce HSM.

La clé privée du Porteur est générée directement dans le support physique appartenant au Porteur.

6.1.3. Transmission de la clé publique à l'AC

La transmission de la clé publique du Porteur à l'AC se fait au moment du retrait du certificat (voir paragraphe 4.3), suite à la personnalisation électrique du support physique. La demande de certificat est au format standard PKCS#10.

Le format PKCS#10 de la demande garantit que la clé publique est protégée en intégrité et que son origine en est authentifiée.

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

La clé publique de l'AC est mise à disposition des utilisateurs via le certificat de l'AC SG TS 2 ETOILES qui est téléchargeable publiquement tel que défini au paragraphe 2.2.

L'empreinte (*Thumbprint*) du certificat de la clé publique de l'AC qui est également publiée permet d'en établir l'authenticité.

6.1.5. Tailles des clés

La taille des clés de l'AC SG TS 2 ETOILES est de 4096 bits.

La taille des clés des Porteurs pour un certificat de signature est de 2048 bits.

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

Voir le paragraphe 7 pour les paramètres et les algorithmes liés à la génération des bi-clés.

6.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC SG TS 2 ETOILES et du certificat associé est strictement limitée à la signature de certificats de Porteurs et de LCR.

L'utilisation de la clé privée de Porteur et du certificat de signature associé est strictement limitée aux usages définis au paragraphe 1.4.1.1).

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

1) Modules cryptographiques de l'AC

Le module cryptographique utilisé par l'AC pour générer et mettre en œuvre sa clé de signature répond aux exigences de sécurité du RGS au niveau **. Il est qualifié au niveau renforcé et est certifié conforme vis-à-vis des critères communs EAL4+.

2) Dispositifs de création de signature des Porteurs

Le dispositif de création de signature des Porteurs est un support physique sous forme de clé USB ou de carte à puce. Il est envoyé par le Back Office Atos World Line par courrier à l'intention du Porteur (à l'adresse qu'il a renseignée lors de l'enregistrement).

La mise en œuvre de la clé privée de signature du Porteur nécessite l'utilisation d'une donnée d'activation (code PIN). Les Porteurs sont responsables de la confidentialité de cette donnée. Ce point figure dans le Contrat d'Abonnement signé par le Porteur.

Ce dispositif répond aux exigences de sécurité du RGS au niveau **. Il est qualifié au niveau standard et est certifié aux vis-à-vis des critères communs EAL4+.

6.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle de la clé privée de l'AC SG TS 2 ETOILES, pour les opérations d'export ou d'import hors ou dans un module cryptographique, est assuré par les Porteurs de secrets de l'AC (voir paragraphe 6.1.1.1) où la présence de trois Porteurs de secrets est nécessaire pour mettre en œuvre la clé privée de l'AC.

6.2.3. Séquestre de la clé privée

Il n'est procédé à aucun séquestre de clés privées, qu'il s'agisse de clé privée d'AC ou de porteur.

6.2.4. Copie de secours de la clé privée

La clé privée des Porteurs ne fait pas l'objet d'une copie de secours.

La clé privée de l'AC SG TS 2 ETOILES fait l'objet de deux copies de secours stockées chacune dans un module cryptographique (HSM) répondant aux même exigences en matière de sécurité qu'au paragraphe 6.2.1.1).

6.2.5. Archivage de la clé privée

Ni la clé privée de l'AC SG TS 2 ETOILES ni celles des Porteurs ne font l'objet d'un archivage.

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

La clé privée de l'AC SG TS 2 ETOILES est générée et stockée au sein du même module cryptographique.

Le transfert des copies de secours de cette clé vers les deux autres modules de secours se fait de manière chiffrée et conformément aux exigences du chapitre 6.2.4.

Les clés privées des Porteurs ne font l'objet d'aucun transfert.

6.2.7. Stockage de la clé privée dans un module cryptographique

La clé privée d'AC, les copies de secours de cette clé ainsi que les clés privées des Porteurs sont stockées dans des modules cryptographiques répondant aux exigences de sécurité du RGS au niveau ** (Voir paragraphes 6.2.1 et 6.2.4).

6.2.8. Méthode d'activation de la clé privée

1) Clé privée d'AC

L'activation des clés privées d'AC dans le module cryptographique est contrôlée via une carte d'administration et fait intervenir au moins trois Porteurs de secrets.

2) Clés privée des Porteurs

L'activation de la clé privée des Porteurs est contrôlée via une donnée d'activation (code PIN) définie par le Porteur lors du retrait (voir paragraphe 4.3).

Le Porteur est responsable de la confidentialité de cette donnée d'activation, tel qu'il s'y est engagé lors de la signature du Contrat d'Abonnement.

6.2.9. Méthode de désactivation de la clé privée

1) Clé privée d'AC

La désactivation de la clé privée de l'AC dans le module cryptographique est contrôlée via une carte d'administration et fait intervenir au moins trois Porteurs de secrets.

La clé privée d'AC pourra être désactivée manuellement dès l'apparition d'un incident lié à l'évolution de l'environnement du module cryptographique, notamment en cas d'arrêt ou de déconnexion du module.

2) Clés privées de Porteurs

Aucun mécanisme de désactivation de la clé privée des Porteurs n'est mis en place.

A noter qu'au bout de trois erreurs dans la saisie du code PIN, le support physique est bloqué et ne peut plus être utilisé. Bien que le certificat soit encore valide, l'utilisation de la clé privée associée n'est plus possible.

Dans ce cas, le Porteur doit révoquer son certificat puis faire une nouvelle demande.

6.2.10. Méthode de destruction des clés privées

1) Clé privée de l'AC

La destruction de la clé privée de l'AC ne peut être effectuée qu'à partir du module cryptographique (HSM).

2) Clés privées de Porteurs

La destruction de la clé privée d'un Porteur ne peut être effectuée qu'à partir du support physique stockant cette clé.

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

Voir paragraphes 6.2.1 et 6.2.4.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

Les clés publiques d'AC et les clés publiques de Porteurs sont archivées dans le cadre de la politique d'archivage des certificats (voir chapitre 5.5).

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

Les bi-clés et certificats des Porteurs couverts par la présente Politique de Certification ont une durée de vie de 3 ans.

La durée de vie de la bi-clé de signature de l'AC SG TS 2 ETOILES est de 10 ans.

l'AC SG TS 2 ETOILES veillera à n'émettre des certificats que si leur date de fin de validité est antérieure à la date de fin de validité du certificat de l'AC SG TS 2 ETOILES (cf. paragraphe 5.6).

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

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 des modules cryptographiques stockant la clé privée de l'AC ainsi que les copies de cette clé se font lors de la phase d'initialisation et de personnalisation de ces modules (lors de la *Key Ceremony*).

Les données d'activation d'un HSM correspondent à sa carte d'administration. La carte d'administration est sous le contrôle d'un Porteur de secret.

L'initialisation du module cryptographique (création de la carte d'administration) nécessite la mise en œuvre d'une carte d'initialisation tel que décrit en paragraphe 6.1.1.1).

Les Porteurs de secrets sont identifiés dans l'un des documents opérationnels de l'AC décrivant les rôles et l'organisation.

2) Génération et installation des données d'activation correspondant à la clé privée du Porteur

La donnée d'activation correspondant à la clé privée du Porteur est choisie par le Porteur avant la génération de sa bi-clé au moment de l'initialisation de son support physique (voir paragraphe 4.3.1).

La politique de ce code PIN est la suivante : il s'agit d'un code composé de 4 chiffres de 0 à 9. Les codes PIN triviaux sont interdits.

6.4.2. Protection des données d'activation

1) Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation générées par l'AC pour les modules cryptographiques ne sont connues que par les responsables des données d'activation, qui en assurent la confidentialité, l'intégrité et la disponibilité.

2) Protection des données d'activation correspondant à la clé privée du Porteur

La donnée d'activation correspondant à la clé privée du Porteur est connue uniquement de lui, et doit être gardée secrète.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques supportant les fonctions de l'Autorité de Certification et mis à disposition par l'OSC sont encadrés par les mesures de sécurité suivantes :

- 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).
- Gestion des reprises sur erreur.

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

La DPC décrit les moyens mis en œuvre pour implémenter chacune de ces mesures de sécurité. Ces mesures de sécurité sont explicitées dans des règles opérationnelles de sécurité et dans des documents d'exploitation utilisés par l'OSC.

6.5.2. Niveau de qualification des systèmes informatiques

Les systèmes informatiques mis à disposition par l'OSC sont qualifiés au regard du RGS qui s'appuie sur la norme CWA 14167-1.

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

6.6.1. Mesures de sécurité liées au développement des systèmes

La conception et le développement des systèmes informatiques supportant les fonctions de l'Autorité de Certification ont été réalisés dans le respect des normes et standards applicables.

Les aspects sécurité ont notamment été pris en compte.

La documentation existe et évolue en fonction des mises à jour.

Les systèmes informatiques sont testés dans un environnement de test dédié avant mise en production.

6.6.2. Mesures liées à la gestion de la sécurité

Le Comité de Pilotage de l'AC valide les évolutions à apporter aux systèmes afin de maintenir le niveau de sécurité de l'AC.

Ces évolutions donnent lieu à des tests et à une mise à jour de la documentation et des procédures d'exploitation.

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

Sans objet.

6.7. Mesures de sécurité réseau

L'architecture réseau des systèmes informatiques supportant les fonctions de l'Autorité de Certification respecte les bonnes pratiques en matière de sécurité réseau : cloisonnement, séparation des environnements (test / production), règles de filtrage, robustesse des équipements réseau, gestion de la haute disponibilité…

Des audits périodiques suivis d'actions correctrices sont menés pour lutter contre les vulnérabilités.

La DPC donne plus de détails sur les règles mises en œuvre pour chacun des composants de l'architecture technique.

6.8. Horodatage / Système de datation

L'Autorité de Certification date les journaux d'événements avant de les envoyer vers l'archivage (voir paragraphes 5.4.4 et 5.5.5).

Cette datation se base sur des serveurs de temps synchronisés sur une source de temps satellite et sur les Universités de Tours et de Lyon. Le mécanisme de synchronisation est basé sur des flux NTP. La précision est inférieure à 1 seconde

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1. Profil des certificats

Les certificats de l'IGC SGTS sont au format X509v3.

7.1.1. Certificat de l'AC SG TS 2 ETOILES

Le certificat de l'AC SG TS 2 ETOILES contient les informations suivantes.

1) Champs de base

Champ	Valeur
Version	2 (= V3)
Numéro de série	Défini par l'outil
DN Émetteur	CN = SG TRUST SERVICES RACINE OU = 0002 43525289500022 O = SG TRUST SERVICES C = FR
DN Objet	CN = SG TS 2 ETOILES OU = 0002 43525289500022 O = SG TRUST SERVICES C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 10 ans
Algorithme de clé publique	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Clé publique	<valeur de la clé publique RSA de 4096 bits>

2) Extensions de base

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Signature de certificat, Signature de Liste de Révocation de Certificats
Stratégies de certificat	O	N	Identificateur de politique = 1.2.250.1.124.7.1.1.1.1
Points de distribution des LCR	O	N	HTTP : URL=http://crl.sgtrustservices.com/racine-GroupeSG/LatestCRL
Contraintes de base	O	O	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=0

7.1.2. Certificat des Porteurs

Les certificats de signature des Porteurs contiennent les informations suivantes :

1) Champs de base

Champ	Valeur
Version	2 (= V3)
Numéro de série	Défini par l'outil

DN Émetteur	CN = SG TS 2 ETOILES OU = 0002 43525289500022 O = SG TRUST SERVICES C = FR
DN Objet	CN = Michel DURAND E = mdurand@societe.fr OU = 0002 < SIREN (9 chiffres) ou SIRET (14 chiffres) > O = CLIENT C = < FR ou pays du Client >
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 3 ans
Algorithme de clé publique	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Clé publique	<valeur de la clé publique RSA de 2048 bits>

Remarque : les contraintes sur le format du champ OU du DN sont compatibles avec le format des numéros SIREN ou équivalent étranger (pas de contrainte sur le nombre de caractères).

2) Extensions Standard

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Non répudiation (40)
Stratégies de certificat	O	N	Identificateur de politique = 1.2.250.1.124.7.1.2.3.1
Points de distribution des LCR	O	N	http= http://crl.sgtrustservices.com/SGTS-2Etoiles/LatestCRL
Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=N/A

3) Autres extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Extended Key Usage	N	N	*EmaiProtection*
Subject Alternative Name	N	N	mdurand@societe.fr

7.2. Profil des Listes de Certificats Révoqués (LCR)

Les LCR émises présentent les caractéristiques suivantes :

Durée et fréquence de mise à jour

- Durée de validité : 7 jours
- Périodicité de mise à jour : 24 heures

Informations et principes de base

La version de la LCR est v2.

L'émetteur de la liste de révocation a comme DN le nom de l'Autorité de Certification signataire de cette LCR (AC SG TS 2 ETOILES).

Les certificats révoqués sont listés.

Les certificats sont nommés par leur numéro de série.

La date de révocation est précisée.

Extensions

- Numéro de la LCR
- Authority Key Identifier : identifiant de la clé publique de l'AC SG TS 2 ETOILES

Lieux de publication

URL http de publication : http://crl.sgtrustservices.com/SGTS-2Etoiles/LatestCRL

8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Ce paragraphe concerne les audits commandités en interne par l'Autorité de Certification afin de vérifier la conformité de l'implémentation au regard de la Politique de Certification, dans une démarche de contrôle permanent.

Les audits de qualification liés au statut de PSCE ne sont pas traités ici.

8.1. Fréquences et / ou circonstances des évaluations

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

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

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

8.2. Identités / qualifications des évaluateurs

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

8.3. Relations entre évaluateurs et entités évaluées

L'AC veillera à ce que l'équipe d'audit n'appartienne pas à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et à ce qu'elle soit dûment autorisée à pratiquer les contrôles visés.

8.4. Sujets couverts par les évaluations

Le programme d'audit est établi sur un cycle de deux ans.

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).

Ils visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC, dans la DPC, et dans les autres documents (Politiques de Sécurité, procédures opérationnelles) cités par la DPC.

Le sujet et le périmètre de l'évaluation seront préalablement définis dans un protocole d'audit qui sera validé par le Comité de Pilotage de l'AC.

8.5. Actions prises suite aux conclusions des évaluations

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

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être :
  - La cessation (temporaire ou définitive) d'activité.
  - La révocation du certificat de la composante.
  - La révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc.

  Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées.

  Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

8.6. Communication des résultats

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

9. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Les tarifs des abonnements aux services de Certification sont stipulés dans le Contrat d'Abonnement.

Remarque : Les tarifs des kits nécessaires à l'installation du support physique sont mentionnés sur le Contrat de Vente Kit de Connexion.

SG Trust Services se réserve le droit à tout moment de modifier le montant de la redevance en avertissant le client moyennant un préavis de deux mois.

9.1.2. Tarifs pour accéder aux certificats

Pour les Porteurs, voir paragraphe 9.1.1. L'accès aux certificats est inclus dans la fourniture d'un certificat.

Les certificats des Porteurs ne sont pas publiés. Les certificats des Porteurs doivent être demandés par les applications dans le cadre du mécanisme technique de création et validation de signature. Cette opération n'est pas contrôlée par SG Trust Services, elle n'est soumise à aucune tarification.

Les Certificats de l'AC SG TS 2 ETOILES ainsi que celui de l'AC racine disponibles sur le site de publication (voir paragraphe 2.2) sont en téléchargement libre.

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

L'accès aux LCR est libre en lecture.

9.1.4. Tarifs pour d'autres services

SG Trust Services se réserve le droit de facturer tout autre service ne faisant pas partie des services cités ci-dessus.

9.1.5. Politique de remboursement

Toute demande de remboursement devra être adressée à :

SG TRUST SERVICES

SERVICE CLIENTS

17 cours Valmy

92972 PARIS LA DEFENSE CEDEX

France

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

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

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- Les Clés privées des Porteurs de Certificats.
- Les Données d'Activation des Porteurs.
- Les causes de révocation, sauf accord explicite du Porteur.
- La Demande Individuelle Porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les Certificats).
- Le Dossier d'Enregistrement et a fortiori le Dossier De Souscription rempli.
- Les clés privées des AC et des composantes de l'IGC.
- Les secrets et données d'activation de l'AC.
- La DPC et les documents opérationnels associés.
- Les journaux d'événements des composantes de l'IGC.
- Les rapports d'audit.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilités en termes de protection des informations confidentielles

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

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

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

L'Autorité de Certification veille à la protection des données personnelles conformément à la réglementation, en particulier de la loi CNIL.

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à tous les documents détenus ou transmis par l'AC ou par une des composantes de l'IGC (site de la CNIL http://www.cnil.fr).

En vertu de la loi, les personnes physiques disposent d'un droit d'accès, de rectification ou d'opposition des données à caractère personnel les concernant. Ce droit peut être exercé auprès de :

SG Trust Services

Service Clients

17 cours Valmy

92972 PARIS LA DEFENSE CEDEX

FRANCE

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les informations nominatives enregistrées pour chaque Porteur : nom, prénom, adresse email.
- Les causes de révocation, sauf accord explicite du Porteur.

9.4.3. Informations à caractère non personnel

Pas d'exigence particulière.

9.4.4. Responsabilité en termes de protection des données personnelles

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

9.4.5. Notification et consentement d'utilisation des données personnelles

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

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

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

Les informations nominatives recueillies dans le Dossier de Souscription de même que celles qui seront recueillies ultérieurement, sont destinées à SG Trust Services qui, de convention express, est autorisée à les conserver en mémoire informatique, à les utiliser, ainsi qu'à les communiquer aux mêmes fins aux personnes morales du Groupe Société Générale, ou à des tiers pour des besoins de gestion.

9.4.7. Autres circonstances de divulgation d'informations personnelles

Pas d'exigences spécifiques.

9.5. Droits sur la propriété intellectuelle et industrielle

Lors de l'exécution des prestations de services définies dans le Contrat d'Abonnement, l'AC peut fournir des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété de l'AC ou du détenteur des droits correspondants. Le Client aura le droit de reproduire ces éléments dans le seul cadre de l'utilisation des Certificats conformément au Contrat d'Abonnement. Il ne pourra en aucun cas, sans l'autorisation préalable de l'AC, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.

Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée au Client et/ou au Porteur par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant.

9.6. Interprétations contractuelles et garanties

Les obligations communes à toutes les composantes de l'AC et de l'AE ainsi qu'aux Chargés de Clientèle sont :

- 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.
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. paragraphe 8) et l'organisme de qualification.
- Respecter les accords ou contrats qui les lient entre elles ou aux porteurs.
- Documenter leurs procédures internes de fonctionnement.
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1. Autorités de Certification

L'AC s'engage à :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un Porteur donné et que ce Porteur a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus.
- Tenir à disposition des Porteurs, des Gestionnaires de Certificats, du Client et des Utilisateurs de Certificats la notification de Révocation du Certificat d'une composante de l'IGC ou d'un Porteur.
- Ne pas choisir ou imposer les données d'activation du Porteur.
- Diffuser publiquement la présente PC et les LCR.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant, notamment via le Client les ayant habilité à utiliser des Certificats, 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 porteur et l'AC est formalisée par le Contrat d'Abonnement du Client ainsi que les Conditions Générales d'Utilisation (intégrées dans le formulaire de demande) signés par le Porteur, précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

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

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

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

9.6.2. Service d'enregistrement

Les Chargés de Clientèle s'engagent à mettre en œuvre les moyens décrits dans la présente PC pour :

- Vérifier la validité des pièces justificatives et l'exactitude des mentions du Dossier De Souscription qui établissent l'identité du Client.

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

- Vérifier la validité des pièces justificatives et l'exactitude des mentions du Dossier De Souscription qui établissent l'identité du Client.
- Vérifier l'origine et l'exactitude de toute demande de révocation et mettre en œuvre les moyens permettant de les traiter.

- Respecter les politiques de contrôle d'accès aux composantes techniques de l'Autorité d'Enregistrement Déléguée.

9.6.3. Porteurs de certificats

Le Porteur a l'obligation de :

- Générer sa Bi-Clé sur le support physique fourni par SG Trust Services.
- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat (ainsi que toutes les pièces justificatives nécessaires) et informer immédiatement l'AE Déléguée de toute modification de celles-ci.
- Protéger sa Clé Privée par des moyens appropriés à l'environnement dans lequel se trouve cette clé.
- Protéger ses Données d'Activation.
- Protéger l'accès à sa base de certificats.
- Respecter les conditions d'utilisation de sa Clé privée et du Certificat correspondant.
- Faire sans délai, une demande de révocation de son certificat auprès de l'AC ou du Gestionnaire de Certificats en cas de compromission ou de suspicion de compromission de sa clé privée.

La relation entre le Porteur et l'AE Déléguée est formalisée par un engagement du Porteur visant à certifier l'exactitude des renseignements et des documents fournis (signature du formulaire de demande DIP).

Remarque : les obligations du Gestionnaire de Certificats sont décrites au paragraphe 9.6.5.1).

9.6.4. Utilisateurs de certificats

Les utilisateurs utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis.
- Pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation).
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.5. Autres participants

1) Le Gestionnaire de Certificats

Le Gestionnaire des Certificats s'engage à :

- Communiquer des informations complètes et à jour lors de la demande de Certificat (ainsi que toutes les pièces justificatives nécessaires) et informer immédiatement l'AC de toute modification de celles-ci.
- Vérifier que le Demandeur de Certificat est autorisé à utiliser des Certificats pour le compte du Client.
- Recueillir l'ensemble des pièces justificatives relatives au Porteur, vérifier son identité et en effectuer une photocopie. Il doit signer cette photocopie.

- Vérifier l'exactitude des mentions qui établissent l'identité du Porteur.
- Informer immédiatement le Distributeur ou l'AC de tout départ de la personne morale ou décès du Porteur.

Le Gestionnaire s'engage à faire respecter les obligations du Porteur telles que décrites au paragraphe 9.6.3.

9.7. Limite de garantie

Les responsabilités du Client et les garanties sont précisées dans le Contrat d'Abonnement. Le présent paragraphe reprend l'article 14 des Conditions Générales de ce contrat.

Le Client demeure à l'égard de SG Trust Services l'unique responsable du bon accomplissement par le Gestionnaire de Certificats ou par les Porteurs de leurs droits et obligations au titre des documents contractuels. Le Client garantit en outre SG Trust Services contre toute action, réclamation ou demande qui pourrait être introduite à son encontre par un Gestionnaire de Certificats, un Porteur ou un tiers, et tout dommage en résultant, ayant directement ou indirectement comme origine ou fondement le non-respect par le Client, un Gestionnaire de Certificats ou un Porteur de l'une quelconque des dispositions, des Conditions Générales, des Conditions Particulières, des Demandes Individuelles Porteur ou d'un Contrat de Vente Kit de Connexion.

9.8. Limite de responsabilité

Les limites de responsabilité de SG Trust Services sont précisées dans le Contrat d'Abonnement. Le présent paragraphe reprend l'article 15 des Conditions Générales de ce contrat.

La responsabilité de SG Trust Services est limitée aux dommages matériels directs à l'exclusion de tout dommage indirect et de toute perte de chiffre d'affaires, de bénéfice, de profit, d'exploitation, de renommée ou de réputation, de clientèle, du préjudice commercial, économique et autre perte de revenus, des conséquences liées à la révocation d'un Certificat et de la perte de données. La responsabilité totale cumulée de SG Trust Services au titre d'un service donné pendant toute sa durée, quelle que soit la cause ou la forme de l'action intentée, n'excédera pas le montant mentionné à l'article "Responsabilité" des Conditions Particulières s'appliquant au Service à l'origine du dommage.

SG Trust Services n'assume aucune responsabilité quant aux conséquences des retards, altérations ou pertes que pourrait subir le Client dans la transmission de tous messages électroniques, lettres ou documents.

SG Trust Services ne pourra voir sa responsabilité engagée en cas d'interruption, totale ou partielle, du Service.

Voir paragraphe 9.16.5 pour les cas de force majeure.

9.9. Indemnités

Pas d'exigences particulières.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

Le présent document est applicable jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2. Fin anticipée de validité

Sauf événement exceptionnel lié à la sécurité, les évolutions à venir du présent document n'imposeront pas la révocation des certificats déjà émis.

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

Pas d'exigences particulières.

9.11. Notifications individuelles et communications entre les participants

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

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

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

L'AC contrôlera que tout projet de modification de sa PC reste conforme aux exigences de la présente PC, dans le respect du RGS. En cas de changement important, l'AC pourra faire appel à une expertise technique pour en contrôler l'impact.

9.12.2. Mécanisme et période d'information sur les amendements

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

9.12.3. Circonstances selon lesquelles l'OID doit être changé

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

9.13. Dispositions concernant la résolution de conflits

Le règlement des litiges est précisé dans le Contrat d'Abonnement. Le présent paragraphe reprend l'article 23 des Conditions Générales de ce contrat.

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

9.14. Juridictions compétentes

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

9.15. Conformité aux législations et réglementations

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

9.16. Dispositions diverses

9.16.1. Accord global

Pas d'exigence particulière.

9.16.2. Transfert d'activités

Voir paragraphe 5.8.

9.16.3. Conséquences d'une clause non valide

Pas d'exigence particulière.

9.16.4. Application et renonciation

Pas d'exigence particulière.

9.16.5. Force majeure

Le présent paragraphe reprend l'article 15 des Conditions Générales du Contrat d'Abonnement.

SG Trust Services ne saurait être tenue responsable des pertes, dommages, retards ou manquement à l'exécution d'obligations résultant des Conditions Générales lorsque les circonstances y donnant lieu relèvent de la force majeure au sens de l'article 1148 du Code civil. Les Parties conviennent, en outre, que seront assimilables à un cas de force majeure: décisions d'une autorité publique, modifications législatives et/ou réglementaires, fait de tiers imprévisible ayant causé des dommages rendant impossible la fourniture du Service, blocage des réseaux de télécommunications pour quelque raison que ce soit. Dans l'hypothèse où le cas de force majeure empêche l'exécution par l'une des Parties de ses obligations pour une durée supérieure à 2 mois, chacune des Parties pourra résilier le Contrat d'abonnement, de plein droit et sans formalité judiciaire, sans que le Client ne puisse prétendre à aucune indemnité.

9.17. Autres dispositions

Pas d'exigence particulière.