POLITIQUE DE CERTIFICATION

AUTORITE DE CERTIFICATION

Chaabi eSign - Certs CA

Version V1.2

MODIFICATIONS

Date	Etat	Version	Commentaires
16/12/2023	Draft	V1.0	Initiation

REFERENCES

Référence	Version	Titre des documents

TABLE DES MATIERES

1. INTRODUCTION

Groupe Banque Populaires, s'est dotée d'une IGC avec plusieurs autorités de certifications (AC) pour délivrer des certificats électroniques à des personnes physiques et des personnes morales.

La présente Politique de Certification (PC) encadre les pratiques de certification appliquées dont GBP s'engage à respecter dans le cadre de la fourniture de son service de certification électronique. La PC identifie également les obligations et exigences portant sur les autres intervenants, les utilisateurs de certificat.

Ce document constitue la Politiques de Certification qui supporte les certificats de signature électronique sous format logiciel et délivrés par l'AC « **Chaabi eSign - Certs CA** » placée sous l'AC Racine «Chaabi eSign – Root CA ».
Les certificats concernés par ce document peuvent être fournis, soit à des particuliers, soit à des professionnels.
Les autres familles de certificat gérés par la plateforme IGC d'Groupe Banque Populaires et les Autorités de Certification correspondantes ne sont pas traitées par la présente PC.

Les certificats et les clés privées associées sont fournis sous format logiciel PKCS12 ou sur dispositif physique qualifié pour les certificats avancés.

1.1 Presentation Générale

La PC encadre la gestion des certificats qui comprend l'ensemble de son cycles de vie allant de la demande d'attribution du certificat jusqu'à sa fin de vie (expiration du certificat ou révocation).

La politique de certification ne décrit pas les détails de l'environnement utilisé pour la mise en œuvre de la plateforme IGC mais elle est complétée par la Déclaration des Pratiques de certification qui gère ce volet.

1.2 Identification du document

La présente PC est dénommé «GBP - Politique de Certification de Génération des certificats de signature électronique". Elle est identifiée par son numéro d'identifiant d'objet (1.2.504.1.1.2.1.3.10.1)
D'autres éléments, plus explicites, comme par exemple le nom, numéro de version, date de mise à jour permettent également de l'identifier

1.3 Définitions et acronymes

1.3.1 Acronymes

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

AC	Autorité de Certification
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information (autorité nationale d'agrément et de surveillance de la certification électronique)

AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
DSA	Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés.
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
SP	Service de Publication
IETF	Internet Engineering Task Force
FIPS	Federal Information Processing Standards Publications
NIST	National Institute of Standards and Technology
ITU	International Telecommunication Union
TS	Technical Specifications
AES	Advanced Encryption Standard
DES	Data Encryption Standard
UTC	Coordinated Universal Time

1.3.2 Définitions

Les termes utilisés dans la présente PC sont les suivants

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

Abonné - Entité ayant souscrit au service de certification à la volée de l'IGC et a accepté les conditions d'utilisation de ses services.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins 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 (AE) - Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.
Autorité d'horodatage (AH) - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage de GBP L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.
L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

Autorité de certification (AC) - Au sein d'un Prestataire de Service de Certification Electronique (PSCE), une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et le terme d'AC est le seul utilisé.

Authentification - Processus permettant de vérifier l'identité déclarée d'une personne ou de tout autre entité, ou de garantir l'origine de données reçues.

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

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.

Certificat d'AC - Certificat d'une autorité de certification.

Chaîne de confiance - Ensemble des certificats nécessaires pour valider la généalogie d'un certificat final.
Dans l'architecture la plus simple, la chaîne se compose d'un Certificat d'Autorité de Certification et du certificat final.

Clé privée – partie secrète d'une bi-clé détenue par son propriétaire. Cette partie de la clé ne doit pas être divulguée.

Clé publique – partie publique d'une bi-clé mise à la disposition des tierces parties pour pouvoir valider l'utilisation d'un certificat.

Common Name (CN) - Identité réelle ou pseudonyme d'un Porteur, d'un Serveur ou d'une AC.
Compromission - Divulgation, modification, substitution ou utilisation sans autorisation de données confidentielles (y compris les clés cryptographiques et d'autres paramètres de sécurité fondamentaux).

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

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

Dispositif sécurisé de création de signature électronique (SSCD) - Matériel ou logiciel, destinés à mettre en application les données de création de signature électronique, qui satisfait aux exigences définies par la règlementation.

Distinguished Name (DN) - Nom distinctif X.500 du Porteur, du Serveur ou de l'AC pour lequel le certificat est émis.

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.

Famille de certificats - Ensemble des certificats émis et gérés suivant une Politique de Certification particulière de l'AC.

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 ou du responsable du certificat.

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 ou au responsable du certificat. De tels éléments secrets peuvent être, par exemple, directement la bi-clé, les codes (activation / déblocage) liés au dispositif de stockage de la clé privée ou encore des codes ou clés temporaires permettant 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 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).

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

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

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

Liste des Autorités Révoquées (LAR) - Liste contenant les identifiants des certificats d'autorités subordonnées révoquées ou invalides.

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

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

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

Système d'information – Tout ensemble de moyen destiné 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 elles-mêmes.

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

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

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Subordonnées). 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.

Qualification d'un prestataire de services de certification électronique - 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.

Référencement - Opération réalisée par l'Administration qui atteste que l'offre de certification électronique du PSCE est utilisable avec tous les systèmes d'information qui requièrent ce type d'offre et exigent le niveau de sécurité correspondant. Une offre référencée par rapport à un service donné et un niveau de sécurité donné d'une PC peut être utilisée dans toutes les applications d'échanges dématérialisés requérant ce service et ce niveau de sécurité ou un niveau inférieur. Pour les usagers, le référencement permet de connaître quelles offres de certificats électroniques ils peuvent utiliser pour quels échanges dématérialisés.

Renouvellement d'un Certificat - Opération effectuée à la demande d'un Porteur ou d'un Responsable de Certificat ou en fin de période de validité d'un Certificat et qui consiste à générer un nouveau Certificat.

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

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.

Validation de certificat - Opération de contrôle du statut d'un Certificat ou d'une chaîne de certification.

Vérification de signature - Opération de contrôle d'une signature numérique.

1.4 Entités intervenant dans l'IGC

1.4.1 Autorité de certification

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, ...) et s'appuie pour cela sur une infrastructure technique : une IGC. L'AC est responsable de la mise en application de la PC à l'ensemble de l'IGC qu'elle a mise en place.

Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :

- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de génération d'éléments secrets ;
- Fonction de publication des conditions générales, de la PC, des certificats d'AC et des
- Formulaires de demande de certificat ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LCR)
- Mise à jour à intervalles réguliers et selon un mode requête/réponse en temps réel
- (OCSP)
-

L'AC assure ces fonctions directement et s'engage à respecter les obligations décrites dans la présente PC. Elle s'engage également à ce que les composants de l'IGC à l'AC, auxquels elles incombent les respectent aussi.

Les fonctions ci-dessus sont les fonctions minimales que doit obligatoirement mettre en œuvre une IGC gérant des certificats de signature, à l'exception de la fonction de génération des éléments secrets du porteur qui est optionnelle et qui dépend des prestations effectivement offertes par l'AC. Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

1.4.2 Autorité d'enregistrement

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

- La prise en compte et la vérification des informations du futur Responsable de Certificat (RC) ou Porteur ainsi que son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- La prise en compte et la vérification des informations, la constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur (notamment, elle respecte la législation relative à
- La protection des données personnelles)
- La vérification des demandes de révocation de certificat.

Dans ce cas précis, l'entité cliente qui est le Abonné a l'entière responsabilité d'effectuer toutes les opérations de vérification des informations du futur porteur et des pièces justificatives. le Abonné doit s'assurer que les demandes sont complètes et exactes avant de les transmettre à l'AE, ce dernier est chargé de s'assurer de l'identité du Abonné Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'abonnée Abonné.

1.4.3 Porteurs de certificats

1.4.3.1 Clients

Le Porteur de certificat est une personne physique, agissant pour son compte, client des partenaires et filiales et désirant signer électroniquement des données.
Il obtient dans ce contexte précis sa clé privée et le certificat correspondant généré à la volée pour son propre compte et valable uniquement pour le besoin d'une transaction.

1.4.4 Utilisateurs de certificats

Un utilisateur de certificat signature peut être notamment :

- Un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la Signature électronique apposée sur des données ou un message par le porteur du certificat ;
- Un usager qui signe électroniquement un document ou un message ;
- Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données.

Les utilisateurs de certificats doivent prendre toutes les précautions décrites dans la présente PC ainsi que dans les CGU.

1.4.5 Autres participants

1.4.5.1 Composants de l'IGC

La décomposition en fonction de l'IGC est présentée au chapitre 1.4.1 ci-dessus.
Les composantes de l'IGC mettant en œuvre ces fonctions devront être présentées dans le DPC de l'AC.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

L'AC « **Chaabi eSign - Certs CA** » délivre des certificats de signature.

1.5.1.1 Certificat Porteur

La PC traite des bi-clés et des certificats à destination de personnes physiques que ces derniers puissent signer électroniquement des données (documents ou messages) dans le cadre d'échanges. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données. Domaines utilisation interdits
Ces certificats ne peuvent pas être utilisés pour un usage à titre personnel, vers des domaines d'usage non explicitement autorisés.

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

La bi-clé d'AC racine est utilisée pour la signature des certificats d'AC intermédiaires et des Listes de certificats d'AC Révoqués (LAR).
La bi-clé d'AC intermédiaire est utilisée pour la signature des certificats finaux et des Listes de Certificats Révoqués (LCR)

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

Groupe Banque Populaires est responsable de la validation et de la gestion de la PC répondant aux
exigences de la présente PC représenté par le Responsable de la certification électronique (Responsable d'AC).

1.6.2 Point de contact

Les demandes d'informations ou commentaires sur cette Politique de Certification doivent être adressés au responsable de l'IGC à l'adresse suivante :

responsablepki@cpm.co.ma
Banque Centrale Populaire
Angle Mohamed El Bakri & Angle Mohamed Diouri
Casablanca Maroc

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

L'approbation de la conformité de la DPC vis-à-vis de la PC est prononcée par le responsable de l'AC.

1.6.4 Procédure d'approbation de la conformité de la DPC vis-à-vis de la PC

L'approbation suit une procédure bien précise. La DPC est revue régulièrement, au minimum une fois par an, par le comité de pilotage de la gouvernance de l'IGC.

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

2.1 Entités chargée de la mise à disposition des informations

L'AC met à disposition des utilisateurs et des applications utilisatrices des certificats qu'elle émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC.
La liste des certificats révoqués (LCR) est publiée automatiquement par la plate-forme IGC.

2.2 Information devant être publiées

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

- La présente politique de certification ;
- Les certificats de l'Autorité de Certification « Chaabi eSign - Certs CA »;
- La liste des certificats révoqués (LCR) ;
- La liste des autorités révoquées (LAR) ;

Compte tenu de la complexité de lecture d'une PC pour des porteurs ou des utilisateurs de certificats non spécialistes du domaine, il est obligatoire que l'AC publie également des conditions générales d'utilisation (CGU).

2.2.1 Publication de la Politique de Certification

La présente PC est accessible à partir des URL suivantes :

- http://www.gbp.ma/Documents/PC_Chaabi_eSign_Certs_CA.pdf

2.2.2 Publication du certificat de l'Autorité de Certification

Le certificat de l'AC est accessible à partir des URL suivantes :

- http://www.gbp.ma/certificats/Chaabbi_eSign_Certs_CA.cer

2.2.3 Publication de la liste des certificats/autorités révoqués

La liste des certificats révoqués (LCR) et la liste des autorités révoquées (LAR) sont accessibles à partir des URI suivantes :

- http://crl.gbp.ma/crldp/chaabi_esign.crl
- http://crl.gbp.ma/crldp/chaabi_eSign_Certs_CA.crl

2.3 Délais et fréquences de publication

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

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants et les systèmes les publiant ont une disponibilité de 24h/24 et 7j/7.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites à la section 4.9.7 Fréquence d'établissement des LCR

Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

2.4 Contrôle d'accès aux informations publiées

L'accès aux informations publiées à destination des utilisateurs est libre. L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Dans chaque certificat conforme à la norme X.509, l'AC émettrice (correspondant au champ « issuer ») et la personne physique ou la personne morale (champ « subject ») sont identifiés par un « Distinguished Name » (DN) répondant aux exigences de la norme X.501

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 Certificat Porteur

Les noms choisis pour désigner les porteurs de certificats sont explicites.
L'identité du porteur est construite à partir du nom et prénom de son état civil tel que porté sur le formulaire d'inscription lors de son enregistrement.

3.1.3 Pseudonymisation des porteurs

Les noms utilisés dans un certificat ne peuvent pas comporter de pseudonymes ou des données anonymes.

3.1.4 Règles d'interprétation des différentes formes de noms

Les règles d'interprétation des différentes formes de nom sont explicitées dans la section 7 décrivant le profil des Certificats et des LCR.

3.1.5 Unicités des noms

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

De plus, l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC et du SerialNumber où est inscrit le N° CIN du futur porteur.

3.1.6 Identification, authentification et rôle des marques déposées

Sans Objet

3.2 Validation initiale de l'identité

L'enregistrement d'un utilisateur se fait directement au moment de la souscription auprès du Abonné qui est le partenaire de GBP ; client du service de certification à la volée ou de délivrance de certificat avancé sur dispositif qualifié.
Les seuls éléments d'identité qui doivent être transmis à l'AC dans la requête de Certificat sont les nom, prénom, adresse mail, numéro de téléphone, et numéro de carte d'identité du porteur.

Lors de la demande de certificat, l'adresse email du porteur est vérifiée au travers de l'envoi d'un code unique par mail.

3.2.1 Méthode pour prouver la possession de la clé privée

3.2.1.1 PKCS12

Les clés des porteurs sont générées directement sous format PKCS12. S'il s'agit d'une première demande de certificat ou pour un renouvellement de certificat, le certificat est envoyé à l'abonné et le pin par mail au client de l'abonné.

3.2.1.2 Dispositif physique

Pour les certificats avancés sur un dispositif de création de signature, cette génération est effectuée dans un dispositif certifié CC répondant aux exigences de la présente PC. L'AC s'assure que la clé publique exportée réside effectivement dans le dispositif de protection des éléments secrets du porteur.

3.2.2 Validation de l'identité d'un organisme

Sans objet

3.2.3 Validation de l'identité d'un individu

La validation de l'identité d'un Porteur est à la charge de l'abonné

3.2.4 Informations non vérifiées du porteur

Le choix de la vérification ou non des informations fournies par le porteur est à la discrétion de l'abonné

3.2.5 Validation de l'autorité du demandeur

Tous abonnés du service est habilité à recevoir les certificats de signature.

3.2.6 Critères d'interopérabilité

La présente PC ne formule pas d'exigences spécifiques sur le sujet.

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

Le contenu de cette section est sans objet pour les certificats à usage unique car ces certificats ne sont pas renouvelables étant donné leur objet.

3.3.1 Identification et validation pour un renouvellement courant

Sans objet

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet

3.4 Identification et validation d'une demande de révocation

3.4.1 Demande faite via les moyens informatiques

3.4.1.1 Par le Porteur

Le Porteur peut demander la révocation de son certificat, s'il ne valide pas les informations contenues dans son certificat (cf. §4.4.1 « Démarche d'acceptation du certificat »).

3.4.1.2 Par le responsable du service de certification

Sans objet

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Un certificat peut être demandé par un Abonné pour un porteur.

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

L'établissement de la demande de Certificat est effectué au niveau de la plateforme de l'Abonné, l'Abonné se charge par la suite de transmettre la demande à l'IGC, pour la génération du certificat à courte durée.

Les informations qui servent à construire la demande de certificat sont les suivantes :
Nom et prénom du Client tel que portés sur la pièce d'identité en cours de validité tel qu'enregistrés par l'abonné.
L'information permettant de contacter et d'authentifier le Porteur (adresse de courrier électronique, numéro de téléphone,).

4.2 Traitement d'une demande de certificat

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

La demande est authentifiée et validée par l'abonné.
L'abonné identifie et authentifie le Porteur
L'abonné s'assure que le porteur a pris connaissance des conditions générales d'utilisation.
L'Abonné conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement

4.2.2 Acceptation ou rejet de la demande

A la réception du flux de demande de certificat provenant de la plateforme de l'abonné, « Chaabi eSign - Certs CA » :
- vérifie que la plateforme ou l'application utilisatrice est enregistrée et habilitée à émettre des demandes,
- les éléments fournis sont complets et intègres, et en cas de succès, transmet la demande de Certificat proprement dite à la fonction de l'AC chargée de la génération des clés et des certificats des Utilisateurs.

4.2.3 Durée d'établissement du certificat

La durée du traitement est liée au processus de génération de certificat à la volée et est immédiate suite à l'acceptation de la demande de certificat par l'abonné, l'AC vise une durée d'établissement la plus courte possible pour les demandes de certificat logiciel et de X ans maximum 3 ans pour les certificats avancé sur dispositif.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

4.3.1.1 PKCS12

Suite à l'authentification de la provenance et à la vérification de l'intégrité de la demande provenant de l'abonné, l'AC déclenche le processus de génération de la Bi-clé et du Certificat de signature du porteur. Le Certificat est à usage unique (durée de vie limitée maximum de 24h). cf. chapitre 7.2 « Certificats des Porteurs » détaille le format utilisé par l'AC pour ce type de Certificats.
Le certificat est envoyé au format PKCS12 à l'abonné et le PIN au client du Abonné. Cf section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques » précise les caractéristiques des modules utilisés pour générer et stocker la Bi-clé de signature.

4.3.1.2 Dipositif Physique

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande, l'AE ou le responsable local déclenchent les processus de génération et de préparation des différents éléments destinés au porteur (au minimum le certificat, son dispositif de création de signature, les codes d'activation, …).

Une notification est envoyée au porteur et à l'AE pour indiquer que la génération est terminée.
Si la demande provient du RSSI, une notification lui parvient également pour le prévenir de la génération des bi-clés.

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

4.3.2.1 PKCS12

Le certificat est mis à disposition de l'abonné immédiatement suite à sa génération.

4.3.2.2 Dipositif Physique

La remise du certificat se fait en mains propres auprès de l'AE, le porteur ou MC sera également tributaire des modalités d'accueil de l'AE.

4.4 Acceptation du certificate

4.4.1 Démarche acceptation du certificat

4.4.1.1 PKCS12

L'acceptation du certificat est effectuée par le porteur au travers l'utilisation du certificat sur la plateforme ou l'application utilisatrice de l'abonné, le porteur peut récupérer les données signés et vérifier le contenu du certificat (notamment les informations qui composent son identité). Si Le porteur n'informe pas l'abonné d'une anomalie dans le certificat, alors le certificat est considéré comme accepté, autrement, le certificat du porteur est révoqué suite à la demande de l'abonné auprès de l'IGC

4.4.1.2 Dispositif physique

Un certificat délivré par l'AC «Chaabi eSign – Certs CA» est considéré comme accepté par le Porteur à la première utilisation opérationnelle de celui-ci.

4.4.2 Publication du certificat

Les certificats de signature ne sont pas publiés après leur délivrance.

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

L'AC «Chaabi eSign - Certs CA » informe l'abonné de la délivrance du Certificat. Cf. section 4.3.2 « Notification par l'AC de la délivrance du certificat ».

4.5 Usage 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 du porteur et du Certificat associé est strictement limitée au service de signature (cf. section 1.5 « Usage des certificats »).
Les porteurs doivent respecter strictement les usages autorisés des Bi-clés et des certificats.
Dans le cas contraire, leur responsabilité serait engagée.

4.5.2 Utilisation de la clé publique et du certificat par le porteur du certificat

L'utilisation des certificats par les porteurs est décrite dans les paragraphes 1.5.

4.6 Renouvellement d'un certificat

Le renouvellement d'un Certificat qui consiste à la délivrance d'un nouveau Certificat pour lequel seules les dates de validité changent, toutes les autres informations restantes identiques au certificat précédent (y compris la clé publique du Porteur), n'est pas autorisé dans le cadre de la présente PC.

4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

Le contenu de cette partie est sans objet pour les certificats de courte durée à usage unique car ces certificats ne sont pas renouvelables étant donné leur objet.

4.7.1 Causes de renouvellement d'un certificat

Sans objet

4.7.2 Origine d'une demande de renouvellement

Sans objet

4.7.3 Procédure de traitement d'une demande de renouvellement

Sans objet

4.7.4 Livraison du nouveau certificat

Sans objet

4.7.5 Processus d'acception du nouveau certificat

Sans objet

4.7.6 Démarche de publication du nouveau certificat

Sans objet

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

Sans objet

4.8 MODIFICATION DU CERTIFICAT

La modification de certificat n'est pas autorisée dans le cadre de la présente PC.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation Procédure de traitement de la demande de modification

4.9.1.1 Certificats de Porteurs

Les circonstances ci-dessus peuvent être à l'origine de la révocation du certificat de signature du Porteur :
- les informations du Porteur figurant dans son certificat ne sont pas en conformité avec son identité,
- le Certificat de signature de l'AC « Chaabi eSign - Certs CA » est révoquée (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante).

Lorsqu'une des conditions ci-dessus se réalise et que l'AC «Chaabi eSign - Certs CA » en a connaissance, les Certificats concernés sont révoqués.

4.9.1.2 Certificats d'une composante de l'IGC

Les cas suivants peuvent entrainer la révocation d'un Certificat d'une composante de l'IGC (y compris un certificat de l'AC «Chaabi eSign - Certs CA » pour la génération de Certificats, de LCR :
- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante ;
- révocation du certificat de l'ACR ;

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de Porteurs

Les personnes / entités qui peuvent demander la révocation d'un Certificat Porteur sont les suivantes :
- le Porteur (via l'abonné), s'il constate que les données de son certificat ne sont pas conformes à son identité,
- l'AC « Chaabi eSign - Certs CA », émettrice du Certificat.

4.9.2.2 Certificat d'une composante de l'IGC

Les demandes de révocation des certificats émis par l'ACR sont réalisées en face-à-face avec l'AE de l'ACR sur présentation d'un formulaire signé par l'entité responsable de l'AC subordonnée.

La validation de l'identité et de l'autorité de la personne physique à l'origine de la demande sont vérifiées par l'AE. La révocation d'un certificat d'AC subordonnée émis par l'ACR peut être aussi déclenchée par l'entité responsable de l'ACR dans le cas de non-respect des exigences de l'IGC par cette AC subordonnée. L'entité responsable de l'AC subordonnée est ensuite prévenue dans les plus brefs délais de cette décision.
La révocation d'un certificat d'AC subordonnée nécessite une cérémonie des clés. L'ACR vérifie l'origine et l'intégrité de la demande de révocation du certificat. Si la demande est correcte, L'AC met à jour le dossier du porteur dans sa propre base de données et ajoute le numéro de série du certificat à la Liste des Certificats Révoqués (CRL).

4.10Procédure de traitement d'une demande de révocation

4.10.1.1 Révocation d'un certificat de Porteur

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre 3.4 « Identification et validation d'une demande de révocation ».
A l'initiative du Porteur (cf. §4.9.2 « Origine d'une demande de révocation »).
La demande de révocation de certificat comprend au minimum :
- l'identification du certificat concerné via au minimum :
- son numéro de série,
- l'identification de l'émetteur (champ DN de l'émetteur du certificat),
- la raison de révocation.

4.10.1.2 Révocation d'un certificat d'une composante de l'IGC

La DPC de l'AC «Chaabi eSign - Certs CA » précise les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.
En cas de révocation d'un des Certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des Porteurs concernés que leur Certificat n'est plus valide.

4.10.2 Délai accordé au porteur pour formuler la demande de révocation

Dès qu'une entité autorisée (cf 4.9.2 « Origine d'une demande de révocation ») a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.10.3 Délai de traitement par l'AC d'une demande de révocation

4.10.3.1 Révocation d'un certificat de Porteur

Par nature une demande de révocation doit être traitée en urgence. La fonction de gestion des révocations est disponible aux heures ouvrées. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) et une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	Durée
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	2h (jours ouvrés)
Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	16h (jours ouvrés)

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 24h. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.10.3.2 Révocation d'un certificat d'une composante de l'IGC

Il n'y a pas de période de grâce dans le cas d'une révocation d'une AC.
L'entité autorisée demande la révocation d'un certificat dès lors qu'elle en identifie une cause de révocation.

4.10.4 Exigences de vérification de la révocation par les Applications utilisatrices de certificats

L'application utilisatrice d'un certificat de Porteur, est tenue de vérifier avant son utilisation, l'état des Certificats de l'ensemble de la chaîne de certification correspondante, y compris le Certificat du Porteur lui-même.

4.10.5 Fréquence d'établissement des LCR

- Configuration des LCR :
  - Période de publication : 1 jours ;
  - Overlap : 0 jours ;
  - Durée de validité :1 jours ;

4.10.6 Délai maximum de publication d'une LCR

Suite à sa génération, une LCR doit être publiée dans le délai maximum de 30 minutes.

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

En complément de la publication des LCR, l'AC met à disposition un répondeur OCSP conforme à la RFC 6960. Le répondeur OCSP répond aux exigences d'intégrité, de disponibilité et de délai pour la publication décrite dans cette PC. Les réponses OCSP sont signées par un répondeur OCSP dont le certificat est signé par l'AC qui délivre le certificat dont l'état de révocation est vérifié.

4.10.8 Exigences de vérification en ligne de la révocation des certificats par les applications utilisatrices de certificats

Cf. section 4.9.6 « Exigences de vérification de la révocation par les Applications utilisatrices de certificats » ci-dessus.

4.10.9 Autres moyens disponibles d'information sur les révocations

Sans objet

4.10.10 Exigences spécifiques en cas de compromission de la clé privée

Pour les Certificats d'AC, outre les exigences du chapitre 4.9.3.2, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le Portail internet du groupe ou des partenaires et filiales qui utilise l'AC.

4.10.11 Causes possibles d'une suspension

Sans objet

4.10.12 Origine d'une demande de suspension

Sans objet

4.10.13 Procédure de traitement d'une demande de suspension

Sans objet

4.10.14 Limites de la période de suspension d'un certificat

Sans objet

4.11 Fonction d'information sur l'état des certificats

4.11.1 Caractéristiques opérationnelles

L'AC fournit aux applications utilisatrices de certificats de signature les moyens de vérifier et valider préalablement à son utilisation, le statut d'un certificat et de sa chaîne de certification, c'est-à-dire de vérifier également les signatures des Certificats de la chaîne et les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état des Certificats de l'ACR.

4.11.2 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) et une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	Durée
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats	4h (jours ouvrés)
Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats	32h (jours ouvrés)

4.11.3 Dispositifs optionnels

Sans objet

4.12 FIN DE LA RELATION ENTRE LE PORTEUR ET L'AC

Compte tenu de la durée de vie des certificats, cette section est sans objet dans le cadre présente PC.

4.13 SEQUESTRE DE CLE ET RECOUVREMENT

Le séquestre de clé et le recouvrement sont interdits dans le cadre de la présente PC.

4.13.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet

4.13.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet

5. MESURE DE SÉCURITÉ NON TECHNIQUES

Ce chapitre traite des mesures de sécurité non techniques (c. à d. concernant la sécurité physique, les procédures et la gestion du personnel) appliquées dans le but de sécuriser les fonctions de génération de clé, de délivrance des certificats, de révocation des certificats, d'audit et d'archivage.

Suite à une analyse de risque menée par GBP , différents contrôles sont mis en place afin d'assurer un haut niveau de confiance dans le fonctionnement de l'AC.

Les exigences définies dans la suite de ce chapitre sont les exigences minimales que l'AC «Chaabi eSign - Certs CA ». Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement de travail et des résultats de l'analyse de risque pour garantir un niveau de sécurité homogène.

5.1 Mesures de sécurité physique

GBP s'engage à mettre en œuvre et à maintenir un niveau de sécurité physique conforme aux règles de bonne pratique concernant les locaux d'exploitation des composantes de l'ensemble de son IGC

5.1.1 Situation géographique et construction des sites

La situation géographique est conforme aux pratiques du Groupe.

La construction des sites respecte les règlements et normes en vigueur ainsi que les résultats de l'analyse de risque réalisée. Les sites d'hébergement de l'IGC couvrent les risques inhérents aux tremblements de terre ou explosion.

Les plateformes d'hébergement de l'IGC sont situées hors zone sismique et hors zone inondable.

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC «Chaabi eSign - Certs CA », les accès aux locaux des différentes composantes de l'infrastructure de l'IGC sont contrôlés.

Ces éléments se trouvent dans une zone à accès restreint, avec mise en œuvre des moyens de contrôle et de traçabilité associés.

En dehors des heures ouvrées, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Par ailleurs, l'accès physique aux machines de l'IGC est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.
On entend par ressources l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisé pour la mise en œuvre de l'infrastructure IGC.

5.1.3 Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique (opéré par des groupes électrogènes) et de génération d'air conditionné sont mis en œuvre afin d'assurer la disponibilité et la continuité des services délivrés, en particulier le service de gestion des révocations et le service d'information sur l'état des certificats.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC, ainsi que les engagements pris, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.
De faux planchers ainsi que des détecteurs d'humidité sont mis en place dans les locaux de l'IGC afin de protéger la salle.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC, ainsi que les engagements pris, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.
Des détecteurs d'incendies ainsi que des systèmes d'extinction basée sur le gaz sont mis en place dans les locaux de l'IGC afin de prévenir les incendies et de protéger la sale.

5.1.6 Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).
Les supports (papier, disque dur, clé USB, CD, etc.) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.

5.1.7 Mise hors service des supports

En fin de vie, les supports seront détruits.
Les procédures et moyens de destruction sont conformes au niveau de confidentialité des informations correspondantes.
A l'occasion du comité de pilotage de l'IGC, des tests des clés des porteurs de secrets sont réalisés. Une procédure est également appliquée pour la destruction du matériel obsolescent.

5.1.8 Sauvegarde hors site

En complément de sauvegardes sur site, les composantes de l'infrastructure de l'IGC mettent en œuvre des sauvegardes hors site de leurs applications et de leurs informations.
Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC après incident respectant les engagements de service tels que définis dans la présente PC.
Ces sauvegardes sont chiffrées afin de garantir la sécurité des données. Les informations sauvegardées sont redirigées vers le site de backup.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiances suivants sont identifiés au sein du Groupe pour l'IGC :

- **Responsable de l'AC** - Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats. L'Autorité de Certification est nommée et définie par l'Autorité de Certification Racine représentée par le Responsable Sécurité.
- **Responsable d'AE -** Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- **Ingénieur système** - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur -** Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation au quotidien des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. Ces audits sont organisés de manière périodique sur chacune des branches ;

Ces rôles de confiances ont la possibilité d'être redondés. Les porteurs de secrets sont titulaires des rôles de confiance.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.
Toutes les opérations techniques sensibles nécessitent l'utilisation d'une carte d'administration du module cryptographique qui est délivré au moment de l'initialisation aux administrateurs de l'AC.

5.2.3 Identification et authentification pour chaque rôle

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

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

- Éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

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

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.
Pour les rôles de confiance, les cumuls suivants sont interdits :

- Responsable de sécurité et ingénieur système / opérateur / contrôleur ;
- Ingénieur système, opérateur et contrôleur.

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

5.3 Mesures de sécurité vis-à-vis du personnel

Les contrôles de sécurité vis-à-vis du personnel s'appliquent à l'ensemble du personnel lié à l'activité de l'IGC d 'GBP , qu'il s'agisse du personnel interne de GBP ou du personnel d'entités sous-traitantes exploitant certaines composantes de l'IGC.
En fonction de la sensibilité des tâches affectées, ces mesures concernent :

- Les mesures de formations ;
- La procédure de vérification des antécédents ;
- Les exigences en matière de formation initiale ;
- Les exigences et fréquence en matière de formation continue ;
- La fréquence et séquence de rotation entre différentes attributions ;
- Les sanctions en cas d'actions non autorisées ;
- Les exigences vis-à-vis du personnel des prestataires externes ;
- La documentation fournie au personnel.

5.3.1 Qualifications, compétences et habilitations requises

Toutes les personnes amenées à travailler sur les composantes de l'IGC sont soumises à une clause de secret professionnel.

Chaque entité opérant une composante de l'IGC s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.
Le personnel d'encadrement possède l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.
Toute personne intervenant dans des rôles de confiance de l'IGC est informée :

- de ses responsabilités relatives aux services de l'IGC ;
- des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

Le personnel est soumis aux procédures de recrutements internes du groupe qui inclut une vérification des antécédents.
Ces personnels n'ont pas de condamnation de justice en contradiction avec leurs attributions. Ils remettent à leur employeur une copie du bulletin n°3 de leur casier judiciaire. Les personnes ayant un rôle de confiance ne souffrent pas de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

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

5.3.3 Exigences en matière de formation initiale

Le personnel intervenant sur l'IGC est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il respecte.

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

5.3.4 Exigences et fréquences en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution de l'IGC et les systèmes sous-jacents.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

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

5.3.6 Sanctions en cas d'actions non autorisées

Des sanctions d'ordre légal ou disciplinaire sont applicables en cas d'abus de droit. GBP ne saurait être responsable des actions non autorisées menées.

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

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

5.3.8 La documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques de l'IGC qu'il utilise et met en œuvre.

5.4 Procédures de constitution des données d'audit

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

5.4.1 Type d'événement à enregistrer

Toute opération sensible, c'est à dire manipulant des biens protégés, fait l'objet d'une trace fiable et auditable. La journalisation des événements est sous la responsabilité de chaque composante de l'IGC de GBP pour les évènements qui la concernent.

Les évènements sont journalisés soit automatiquement, sous forme électronique, soit manuellement, sous forme électronique ou papier :

- opération sur les certificats (création, renouvellement, révocation) ;
- connexion / déconnexion des opérateurs d'enregistrement ;
- événements systèmes des différentes composantes de l'IGC (arrêt/démarrage des serveurs, accès réseau, …) ;

- Utilisation des secrets de l'AC ;
- événements techniques des applications composant l'IGC ;
- événements fonctionnels des applications composant l'IGC (demande de certificats, validation, révocation, rejet…) ;
- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- accès physiques aux locaux ;
- publication et mise à jour des informations liées à l'AC (PC, LCR et certificats d'AC) ;
- génération puis publication des LCR ;
- actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,..) ;
- Changements apportés au personnel.

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

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

5.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8 ci-dessous.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènement sont conservés sur site pendant au moins un mois. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous un mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.4 Protection des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements.
Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux. Ces mécanismes seront implémentés suite à la mise en production de l'IGC.
Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).
Le système de datation des évènements respecte les exigences du chapitre 6.8.
La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'événements

Les différents journaux d'évènements sont sauvegardés. Ces différents journaux sont créés au fur et à mesure. Ils sont conservés pendant 5 ans.

5.4.6 Système de collecte des journaux d'événements

La collecte des journaux d'évènements est de la responsabilité de chaque composante de l'IGC du pour les journaux qui la concerne.

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

La notification de l'enregistrement d'un évènement est faite par email au responsable.

5.4.8 Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC de GBP est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.
Les journaux d'évènements sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.
Les journaux d'évènements sont analysés dans leur totalité au minimum 1 fois toutes les 2 semaines et dès la détection d'une anomalie.
Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.
Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre-elles (autorité d'enregistrement et fonction de génération, fonction des révocations et fonction d'information sur l'état des certificats, etc.) est effectué 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont également prises par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.
Il est également conservé des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.
Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configurations des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les CGU ;
- Les accords contractuels avec d'autres AC ;
- Les récépissés ou notifications (à titre informatif) ;
- Les engagements signés des Abonnés;
- Les justificatifs 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

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire, et pendant au moins sept ans, pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.
Les facteurs à prendre en compte dans la détermination de la "loi applicable" sont la loi du pays dans lequel l'AC est établie.
Lorsque les porteurs sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays.
Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat est présenté par l'AC lors de toute sollicitation par les autorités habilitées.
Ce dossier, complété par les mentions consignées par l'AE, permet de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

Certificats, LCR

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins cinq années après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 seront archivés pendant sept années après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offriront le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements sera assurée tout au long de leur cycle de vie.

Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre 5.4, aucune exigence n'est stipulée. L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver ces journaux

5.5.3 Protection des archives

Les archives sont dûment protégées contre les risques d'accès illicite, de modification et de destruction ou d'altération. Les moyens de protection mis en œuvre sont conformes au niveau de classification des données archivées. La gestion des archives sera effective après la mise en production de l'IGC.
Pendant tout le temps de leur conservation, les archives sont :

- Protégées en intégrité ;
- Protégées contre la destruction ;
- Protégées contre les accès illicites ;
- Peuvent être relues et exploitées.

La DPC précise les moyens mis en œuvre.

5.5.4 Procédure de sauvegarde des archives

Les archives sont sauvegardées selon la procédure de sauvegarde en vigueur chez GBP . Une sauvegarde incrémentale est réalisée chaque soir et une sauvegarde complète chaque week-end.

5.5.5 Exigences d'horodatage des données

Les pratiques d'horodatage des données sont précisées dans la DPC.

5.5.6 Système de collecte des archives

Les archives sont centralisées. Le système de collecte est décrit dans la DPC.

5.5.7 Procédure de récupération et de vérification des archives

Les archives ne sont accessibles qu'aux entités en charge de la gestion de l'IGC. L'accès aux archives est contrôlé suivant le rôle demandant l'accès aux archives et le composant associé.
Le temps de récupération des archives est inférieur à deux jours ouvrés.

5.6 Changement de clés d'AC

Une AC ne peut pas générer des certificats pour les AC subordonnées ou les porteurs dont les dates de fin seraient postérieures à la date d'expiration du certificat de l'AC «Chaabi eSign - Certs CA ».
De ce fait, la période de validité du certificat de l'AC est supérieure à celle des certificats des AC subordonnées ou des porteurs.
Lorsqu'un nouveau certificat d'AC « Chaabi eSign - Certs CA » est émis, le certificat de l'AC « Chaabi eSign - Certs CA » précédent peut toujours être utilisé pour vérifier l'authenticité des certificats d'AC subordonnées ou des porteurs émis sous cet ancien certificat, et ce jusqu'à ce que ces certificats d'AC subordonnées ou des porteurs aient expiré.

5.7 Reprise suite à compromission et sinistre

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

Les différentes composantes de l'IGC disposent des procédures permettant de traiter de manière graduelle et adéquate tout incident.
Dans le cas d'incident majeur tel que la suspicion de compromission, le vol de la clé privée de l'AC «Chaabi eSign - Certs CA », l'évènement déclencheur est la constatation de l'incident au niveau de la composante concernée.
Une information au niveau de la direction du Groupe est immédiatement menée.
En cas de révocation du certificat de l'AC «Chaabi eSign - Certs CA », l'information est publiée dans l'urgence.

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

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

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante en tant que sinistre.
Dans les cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué : cf. chapitre 4.9.
En outre, l'AC respecte les engagements suivants :

- Informer les entités suivantes de la compromission : tous les porteurs, Abonné et les autres entités avec lesquelles l'AC a passé des accords ou à d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autre AC. En complément, cette information est mise à disposition des autres tiers utilisateurs ;

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

5.7.4 Capacités de continuité d'activités suite à un sinistre

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.
Ce plan est testé au minimum suivant une fréquence d'une fois par an.

5.8 Fin de vie de l'IGC

En cas d'interruption de ses activités, GBP s'engage à en aviser immédiatement les porteurs et à prendre des dispositions pour que les certificats et les informations de ses subordonnées continuent d'être archivés selon les indications et la période stipulée dans la présente PC.
En outre, GBP s'engage à :

- communiquer suivant un préavis correspondant à un mois, son intention de cesser son activité IGC ;
- informer les autorités compétentes ;
- mettre en œuvre tous les moyens dont il dispose pour informer ses partenaires ;
- révoquer ses certificats d'AC Subordonnées et ses porteurs ;
- révoquer tous les certificats émis ;
- assurer la pérennité des LARs émises.

En cas de transfert de l'activité à un tiers, GBP s'engage à transférer son activité IGC à un tiers à même de fournir le même niveau de service et de sécurité que celui défini dans la présente PC.
GBP mesurera les impacts 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.
L'AC maintient les archives de l'IGC en cas d'arrêt d'activité définitif.

6. MESURES DE SÉCURITÉ TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5).
Les clés de signature d'AC sont générées lors d'une cérémonie des clés à l'aide d'une ressource cryptographique matérielle.
Les rôles des personnes impliquées dans les cérémonies de clés sont précisés dans la DPC.
Suite à leur génération, les parts de secrets (données d'activation) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets est mise en œuvre par son porteur.

6.1.1.2 Clés porteurs générées pas l'AC

La réception de la requête de Certificat et de signature provenant de la plateforme de contractualisation en ligne au nom d'un utilisateur déclenche le processus de génération du Bi-clé.
La génération et le stockage de la Bi-clé de signature se fait au sein d'un module cryptographique matériel certifié CC EAL4+. Ce module est hébergé dans les locaux à accès très restreint de GBP .
Les bi-clés à usage unique sont détruites dans un intervalle de temps très court, une fois que la Transaction de signature est achevée.

6.1.1.3 Clés porteurs générées par le porteur

Les Utilisateurs, Porteurs des Bi-clés de signature, ne génèrent pas leurs Bi-clés.

6.1.2 Transmission de la clé privée à son propriétaire

6.1.2.1 PKCS12

Le certificat est généré sous format PKCS12 est transmise à l'abonnée, qui le met à la disposition de son client final

6.1.2.2 Dispositif physique

Le certificat et la clé privé sont générés directement sur le dispositif est remis directement au MC de l'abonnée, et qui le met à la disposition du porteur final.

6.1.3 Transmission de clé publique à l'AC

La clé publique est transmise à l'AC « Chaabi eSign – Certs CA » lors de la génération de la bi-clé, sous un format PKCS#10, et lors d'une connexion sécurisée de manière à garantir l'intégrité et la confidentialité de la communication et l'authentification entre l'AC et l'AE.

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

L'ensemble des certificats de la chaîne de confiance de l'AC est contenu dans le contrat signé par Le porteur.

6.1.5 Tailles des clés

- 4096 bits pour la taille des clés de l'AC «Chaabi eSign - Certs CA » ;
- 3072 pour les porteurs ;

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.
Les équipements utilisés sont des ressources cryptographiques matérielles évaluées certifiées critère commun EAL 4+.

6.1.7 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de signature, de plus les cas d'usage possible sont inscrits dans le champ « key usage » du certificat

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques (HSM), utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature sont certifiés CC EAL 4 + ET FIPS 140-2 LEVEL 3

6.2.1.2 Dispositifs de protection des éléments secrets des porteurs

Les dispositifs de protection des éléments secrets des porteurs, pour la mise en œuvre de leurs clés privées de personnes, respectent les exigences de la présente PC.
L'AC s'assure que :

- La préparation des dispositifs de protection des éléments secrets est contrôlée de façon sécurisée par le prestataire de service ;
- Les dispositifs de protection des éléments secrets sont stockés et distribués de façon sécurisée ; les désactivations et réactivations des dispositifs de protection des éléments secrets sont contrôlées de façon sécurisée.

6.2.2 Contrôle de la clé privée par plusieurs personnes

6.2.2.1 Clé privée AC

Le secret de l'AC est contrôlé par un secret partagé. Chaque part du secret est distribué à un porteur de secret sous la forme d'une carte à puce cryptographique.
Le porteur de secret s'engage à protéger et à ne pas divulguer cette carte.

6.2.2.2 Bi-clés Porteur

6.2.2.3 PKCS12

Le certificat porteur est généré sous format PKCS12, L'authentification est mise en œuvre suivant la cinématique d'activation choisie par l'Abonné et décrite dans la politique de signature

6.2.2.4 Dispositif physique

La clé privée du porteur est activée suite à la saisie du code PIN du porteur.

6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des Utilisateurs ne sont séquestrées.

6.2.4 Copie de secours de clé privée

6.2.4.1 Bi-clés AC

Les bi-clés d'AC sont sauvegardées à des fins de disponibilité sous le contrôle de plusieurs personnes (porteur de secret) afin de respecter les conditions initiales de contrôle de la clé privée.
Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles (HSM Backup) identiques à celles utilisées pour générer les bi-clés d'AC et stockées dans les locaux de GBP .

6.2.4.2 Bi-clés Porteur

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

6.2.5 Archivage de la clé privée

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

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

Les Bi-clés AC sont générées, et stockées dans des ressources cryptographiques matérielles.
Les sauvegardes de ces clés privées sont réalisées à l'aide de ressources cryptographiques matérielles comme décrit dans le chapitre (6.2.4.1). Elles sont transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC.

6.2.7 Stockage de la clé privée dans un module cryptographique

cf. section 6.2.1 « Standards et mesures de sécurité pour les modules cryptographiques ».

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées de l'AC

Les clés privées d'AC ne peuvent être activées dans le module cryptographique qu'avec des porteurs de secrets ayant des rôles de confiance et détenant des données d'activation de l'AC en question.

6.2.8.2 Clé privée des porteurs

Les bi-clés des Porteurs sont activées par le porteur avec le PIN reçu par mail.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées de l'AC

Sans objet.

6.2.9.2 Clé privée des porteurs

Les clés privées des porteurs ne peuvent être utilisées que dans le cadre de la signature de données (document ou messages).

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées de l'AC

Les clés privées sont utilisées par le processus autorisé lorsqu'elles sont « en lignes ».
En fin de vie ou une décision de fin d'utilisation anticipée (révocation) d'une clé privée d'AC dans une ressource cryptographique matérielle « en lignes », les clés sont supprimées. Les sauvegardes sont aussi détruites.

6.2.10.2 Clé privée des porteurs

Sans Objet

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC «Chaabi eSign - Certs CA » sont archivées par archivage des certificats correspondants et ce dans le cadre de la politique d'archivage.

6.3.2 Durée de vie des bi-clés et des certificats

6.3.2.1 Bi-clé et certificat d'AC

La durée de vie du certificat de l'AC est de 10 ans.

6.3.2.2 Bi-clé et certificat Utilisateur

Les bi-clés et certificats Utilisateurs couverts par la présente PC ont une durée de vie de 01 heures.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activations

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

Les données d'activation des clés privées d'AC sont générées durant la cérémonie de clés.
Les données d'activation sont générées automatiquement selon un schéma de type M of N. Les données d'activation sont remises à leurs porteurs après génération pendant la cérémonie des clés.
Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.
Génération et installation des données d'activation correspondant à la clé privée du porteur.
Génération et installation des données d'activation correspondant à la clé privée du porteur
Le type de données d'activation qu'utilise le porteur est décrit dans la politique de signature. Les données d'activation sont générées par l'AE et distribuées de manière sécurisée au Client de façon à avoir l'assurance que seul le Client pourra signer un contrat à l'aide de la donnée d'activation.

6.4.2 Protection des données d'activation

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

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique jusqu'à la remise à leur destinataire. Les porteurs de données d'activation sont responsables de leur gestion et de leur protection.

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

Les données d'activation correspondant aux clés privées des porteurs est le code PIN envoyé directement au porteur.

6.4.3 Autres aspects liés aux données d'activation

6.4.3.1 Clés privées de l'AC

Les données d'activation ne sont en aucun cas transmissibles sauf dans le cadre de la transmission éventuelle du rôle de détenteur de données d'activation à une autre personne, échange effectué sous le contrôle de l'Autorité de gestion des politiques.

6.4.3.2 Porteur

En cas de compromission de sa donnée d'activation, le porteur alerte l'Abonné qui en informe l'AC

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une IGC comprend les fonctions suivantes :

- Identification et Authentification forte des rôles de confiance (accès physique et logique) ;
- Gestion des droits d'accès basée sur des profils respectant le principe du moindre privilège ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, gestion droits d'accès aux fichiers) ;
- Interdiction de la réutilisation d'objets ;
- Exige l'utilisation de la cryptographie lors des communications ;
- Assure la séparation rigoureuse des tâches ;
- Protection contre les virus informatiques ;
- Protection du réseau contre toute intrusion illicite ;
- Fournit une autoprotection du système d'exploitation ;
- Fonction d'audits.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Les développements des systèmes sont contrôlés par les mesures suivantes :

- Achat des matériels et des logiciels afin à réduire les possibilités qu'un composant particulier soit altéré ;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;
- Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation ;
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'IGC. Seules les applications nécessaires à l'exécution des activités IGC sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite ;
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et sont installées par des personnels de confiance et formés selon les procédures en vigueur.

6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système d'AC, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC.
Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'IGC. Lors de son premier chargement, une vérification est faite que le logiciel de l'IGC correspond à celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

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

Sans objet

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées qui n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.
Les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).
Une analyse de risque relative à l'interconnexion a été menée afin d'établir les objectifs et les solutions de sécurité adaptées. A défaut le dispositif cryptographique dans lequel les clés de l'AC du Groupe sont activées est isolé.

6.8 Horodatage / système de datation

Sans Objet.

7. PROFILS DES CERTIFICATS ET CRLS

7.1 Profil Certficat AC

Elément		Valeur	
Version		V3	
Numéro de série		Numéro unique Nombre aléatoire à longueur fixe.	
Algorithme de signature		Sha512RSA	
Algorithme de hachage de la signature		Sha512	
Emetteur		CN= « Chaabi eSign - Root CA » O= «Groupe Banques Populaires » C= MA	
Valide à partir de		Date de création	
Valide jusqu'au		Date création +10 ans	
Objet		CN	Chaabi eSign. - Certs CA
		O	Groupe Banque Populaires
		C	MA
Clé publique		RSA (4096 bits)	

Extension	Critique	
Identificateur de la clé du sujet		Empreinte SHA-1 de la clé publique de l'issuer
Stratégie de certificat		Identificateur de la stratégie= 1.2.504.1.1.2.1.3.10.1
Identificateur de la clé de l'autorité		Empreinte SHA-1 de la clé publique de l'issuer
Accès aux informations de l'autorité		1.3.6.1.5.5.7.48.2 http://www.gbp.ma/certificats/Chaabbi_eSign_Root_CA.cer
Point de distribution CRL		http://crl.gbp.ma/crldp/chaabi_esign.crl
Utilisation de clé	**oui**	Signature du certificat, Signature de la liste de révocation des certificats hors connexion, Signature de la liste de révocation des certificats
Contrainte de base	**oui**	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=Aucun(e)
Algorithme d'empreinte numérique		SHA-1

7.2 Certificats des porteurs

7.2.1 Porteur

Le tableau suivant renseigne les valeurs par défaut des attributs d'un Certificat porteur émis par l'AC Chaabi eSign - Certs CA
Le format de ce Certificat ainsi que ses attributs respectent le profil X.509v3 décrit dans la RFC 5280 « Internet
X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

7.2.1.1 PKCS12

Elément		Valeur
Version		V3
Numéro de série		Numéro unique, Nombre aléatoire à longueur fixe.
Algorithme de signature		SHA-512
Algorithme de hachage de la signature		SHA-512

Emetteur		CN= « Chaabi eSign – Certs CA » O= «Groupe Banques Populaires » C= MA	
Valide à partir de		Date de génération du certificat	
Valide jusqu'au		Date de génération +X jours	
		SerialNumber	N°CIN ou autres Document d'identité
		Givename	Prenom du porteur
		Surname	Nom du porteur
		CN	Prenom Nom du porteur
		O	«Groupe Banques Populaires »
		organizationIdentifier	Numéro d'immatriculation officiel de l'entité titulaire du certificat, conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …) Exemple « NTRMA-Numéro registre de commerce » si le porteur est en relation avec son entité
		C	MA
Clé publique		RSA (3072 bits)	
Extension	**Critique**		
Identificateur de la clé du sujet		Empreinte SHA-1 de la clé publique de l'issuer	
Stratégie de certificat		Identificateur de la stratégie= 1.2.504.1.1.2.1.3.10.1	
Identificateur de la clé de l'autorité		Empreinte SHA-1 de la clé publique de l'issuer	
Accès aux informations de l'autorité		http://www.gbp.ma/certificats/Chaabbi_eSign_Certs_CA.cer	
Point de distribution CRL		http://crl.gbp.ma/crldp/chaabi_eSign_Certs_CA.crl	

Utilisation de la clé		Non répudiation

7.2.1.2 SmartCard

Elément		**Valeur**	
Version		V3	
Numéro de série		Numéro unique, Nombre aléatoire à longueur fixe.	
Algorithme de signature		SHA-512	
Algorithme de hachage de la signature		SHA-512	
Emetteur		CN= « Chaabi eSign – Certs CA » O= «Groupe Banques Populaires » C= MA	
Valide à partir de		Date de génération du certificat	
Valide jusqu'au		Date de génération +X jours	
		SerialNumber	N°CIN ou autres Document d'identité
		Givename	Prenom du porteur
		Surname	Nom du porteur
		CN	Prenom Nom du porteur
		O	«Groupe Banques Populaires »
		organizationIdentifier	Numéro d'immatriculation officiel de l'entité titulaire du certificat, conformément à [EN_319_412-1] Clause 5.1.4 (ICE, numéro d'inscription au registre du commerce, …) Exemple « NTRMA-Numéro registre de commerce » si le porteur est en relation avec son entité
		C	MA
Clé publique		RSA (3072 bits)	
Extension	**Critique**		

Identificateur de la clé du sujet		Empreinte SHA-1 de la clé publique de l'issuer
Stratégie de certificat		Identificateur de la stratégie= 1.2.504.1.1.2.1.3.10.1
Identificateur de la clé de l'autorité		Empreinte SHA-1 de la clé publique de l'issuer
qcStatements		esi4-qcStatement-4 : Valeur " id-etsi-qcs-QcSSCD". Indication que la clé privée correspondante est Stockée dans un dispositif qualifié de création de cachet électronique.
Accès aux informations de l'autorité		http://www.gbp.ma/certificats/Chaabbi_eSign_Certs_CA.cer
Point de distribution CRL		http://crl.gbp.ma/crldp/chaabi_eSign_Certs_CA.crl
Utilisation de la clé		Non répudiation

7.3 Profil des listes de certificats révoqués

Le tableau suivant fournit les valeurs par défaut des attributs de la Liste de Certificats Révoqués (LCR) émise par l'AC « Chaabi eSign - Certs CA ».
Le format de cette LCR ainsi que ses attributs respectent le profil X.509v2 décrit dans la RFC 5280 « Internet
X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », réf. [RFC5280].

Elément		**Valeur**
Version		V2
Emetteur		CN= « Chaabi eSign - Certs CA» O= «Groupe Banques Populaires » C= MA
Date d'effet		Date d'émission de la CRL
Prochaine mise à jour		Date d'émission de la CRL +1 jours
Algorithme de signature		SHA-512
Certificat Révoqués		n° de série du certificat révoqué date de révocation du certificat
Extension	**Critique**	
Algorithme de hachage de la signature		SHA-512
Numéro de la liste de révocation		Numéro de séquence de la LCR (incrémental simple)

Identificateur de la clé de l'autorité		Empreinte SHA-1 de la clé publique de l'issuer

7.4 Profil OCSP

Il n'y a pas d'exigence spécifique. Le service doit être conforme au RFC [6960]

8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Les audits et évaluations ont pour objectif de s'assurer que l'implémentation faite de l'IGC est conforme aux dispositions écrites dans la présente PC et dans la DPC associée.

8.1 Fréquences et/ou circonstances des évaluations

Un contrôle de conformité à la PC est réalisé tous les 3 ans. Toute évolution majeure de l'IGC donne lieu à un nouvel audit de conformité.
Les audits sont axés sur la base des éléments suivants :

- Les orientations stratégiques de GBP ;
- L'analyse des risques, par l'exploitation, notamment de la cartographie des risques et de la base incidents ;
- Les doléances formulées par le Comité Directeur et le Comité d'Audit - GBP ;
- La couverture suffisante de l'univers d'audit (Missions thématiques, Audit de processus, Audit de fonctions) ;
- Le champ d'intervention des auditeurs externes ou consultants et le cas échéant, des autorités de contrôle et de supervision.

8.2 Identités / qualification des évaluateurs

Les responsables ainsi que le personnel des fonctions d'Audit Interne de GBP sont tenus de se conformer aux :

- valeurs d'éthiques et règles de conduite associées à l'exercice de leur mission et présentées comme suit :
  - Impartialité et Objectivité
    - L'affectation des auditeurs aux missions respecte le principe de la rotation périodique ;
    - Les auditeurs recrutés en interne ne peuvent pas auditer les entités dont ils faisaient partie qu'après écoulement d'une période de 12 mois ;
    - les Auditeurs ne prennent pas part à des activités ou établir des relations qui pourraient compromettre ou risquer de compromettre le caractère impartial de leur jugement ou créer un conflit d'intérêt ;
    - la fonction Audit Interne n'est pas impliquée ni dans la conduite des opérations, ni dans la conception ou l'implémentation du processus de

Contrôle interne au jour le jour (contrôle des premiers niveaux) et de la gestion des risques.

- Compétence, les Auditeurs doivent :
  - réaliser leurs travaux d'audit dans le respect des normes édictées par la présente charte ainsi que des procédures et règles internes traitant de l'activité d'audit ;
  - s'efforcer d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux.
- Conduite : les auditeurs doivent :
  - faire preuve d'un comportement professionnel et ne pas subordonner leur jugement à celui des autres ;
  - respecter les règles de bonne conduite prévues dans le statut du personnel et le règlement intérieur de l'entité auditée (horaires de travail, etc.) ;
  - veiller à ne pas perturber le bon fonctionnement de l'entité qu'ils auditent.
  - refuser toute invitation ou cadeaux offerts par le personnel ou la Direction de l'entité auditée et ce à quelque titre que ce soit. Lorsqu'il s'agit d'invitation officielle, l'accord express de la hiérarchie est nécessaire.
  - être attentifs aux réclamations des clients qui se seraient présentés à eux, en dehors des locaux de l'entité auditée et des horaires du travail. Ils doivent inviter ces clients à se présenter aux locaux des entités auditées aux heures de travail, pour que leurs réclamations soient recueillies en bonne et due forme. Ils doivent également procéder aux investigations nécessaires pour vérifier le bien-fondé de ces réclamations.

8.3 Relations entre évaluateurs et entités évaluées

Au sein des organismes de GBP et de leurs filiales, ces missions en matière de contrôle interne sont confiées aux comités d'audit, composées de :

- du comité d'audit de GBP ;
- des comités d'audit des filiales.

8.3.1 Le comité d'audit GBP

Le Comité d'audit de GBP et son Président sont désignés par le Conseil d'administration de GBP . D'autres personnes notamment, les Commissaires aux comptes et certains responsables, pour fournir les explications nécessaires, peuvent prendre part aux réunions du Comité d'audit.

8.3.2 Les comités d'audits régionaux

Sans Objet

8.4 Sujets couverts par les évaluations

Les sujets couverts par les évaluations sont l'ensemble des éléments suivants :

- Les Missions d'Audit

Il s'agit de la réalisation des missions d'appréciation et d'évaluation du dispositif de Contrôle Interne, thématiques ou spéciales, afin d'aider GBP et ses partenaires à atteindre leurs objectifs en évaluant les systèmes de management des risques, de contrôle, de conformité et de PCA et en faisant des propositions pour renforcer leur efficacité.

- Les Missions d'Inspection

Elles recouvrent les enquêtes et les investigations sur les opérations de fraude et de détournement et tout incident pouvant avoir un impact négatif sur l'atteinte des objectifs en matière de Contrôle interne.

- Missions de prestations de conseil ou spéciales

Elles concernent les prestations de conseil, dénommées également missions spéciales, en réponse à des demandes de l'entité de rattachement ou du Comité d'Audit. Il peut s'agir notamment de :

  - Prestations courantes : participation à des Comités, échanges d'informations avec d'autres entités sollicitant un avis sur une thématique quelconque…etc. ;
  - Prestations occasionnelles : participation à des projets de durée déterminée (fusion, projet de changement de système, participation à une équipe en situation de crise dans le cadre du PCA…etc.).

8.5 Actions prises suite aux conclusions des évaluations

Pour chaque non-conformité observée, l'auditeur estimera le risque résiduel mineur, majeur ou critique pour la sécurité des ressources de l'AC racine GBP .
Si des risques critiques sont constatés la demande de délivrance de certificat est refusée.
Selon les non-conformités observées, l'AC racine GBP peut accepter la délivrance du certificat sous réserve de l'engagement de GBP à corriger les non-conformités dans le délai prescrit par l'auditeur.
Si lors d'une visite de contrôle, les non-conformités indiquées comme devant être corrigées persistent au-delà des délais prescrits, L'auditeur peut prendre la décision de révoquer le certificat émis pour cette AC.

Il n'y a pas d'assurance financière particulière dans le cadre de la délivrance des certificats.

9. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1 Tarifs

9.2 Responsabilité financière

Il n'y a pas d'assurance financière particulière dans le cadre de la délivrance des certificats.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations classifiées de l'IGC de GBP sont au minimum les suivantes :

- l'ensemble des informations liées aux clés privées des AC ;
- les données d'activation des clés des AC ;
- la DPC expliquant la déclinaison de la PC ;
- les spécifications de l'IGC telle que mise en œuvre ;
- les journaux d'évènements ;
- les rôles des différents opérateurs.

9.3.2 Information hors du périmètre des informations confidentielles

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

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.
De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.
L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire marocain. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement de porteurs à des tiers dans le cadre de procédures légales. Elle donne également l'accès à ces informations au Abonné

9.4 Protection des données à caractère personnel

9.4.1 Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par GBP et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire marocain.

9.4.2 Données à caractère personnel

Les informations considérées comme personnelles sont les dossiers d'enregistrement des porteurs pour l'initialisation de l'infrastructure IGC ainsi que l'ensemble des informations relatives aux porteurs.

9.4.3 Données à caractères non personnel

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

9.4.4 Responsabilité en termes de protection des données à caractère personnel

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

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

Conformément à la législation et réglementation en vigueur sur le territoire marocain, les informations personnelles remises par les porteurs à GBP ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.
La propriété intellectuelle et le savoir-faire des différentes composantes de l'Autorité de Certification et des certificats produits appartiennent à l'Autorité de Certification. La délivrance de certificat n'implique pas de transfert de propriété intellectuelle entre l'Autorité de Certification et le porteur.

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

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

9.4.7 Autres circonstances de divulgation de données à caractère personnel

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

9.5 Droits de propriété intellectuelle

GBP est et demeure titulaire des droits de propriété intellectuelle sur les outils de sécurisation d'infrastructure et sur leur documentation associée, dans toutes les versions existantes ou à venir et dans tous les environnements existants ou à venir, conformément aux dispositions du Code de la propriété intellectuelle. Par conséquent la fourniture par GBP de ces outils dans le cadre de sa politique de certification ne saurait être interprétée comme entraînant la cession d'un quelconque droit de propriété intellectuelle.
La propriété intellectuelle et le savoir-faire des différentes composantes de l'Autorité de Certification et des certificats produits appartiennent à l'Autorité de Certification. La délivrance de certificat n'implique pas de transfert de propriété intellectuelle entre l'Autorité de Certification et le porteur.

9.6 Interprétations contractuelles et garanties

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent ;
- respecter et appliquer la partie de la DPC leur incombant ;

- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC et l'organisme de qualification ;
- respecter les accords ou contrats qui les lient entre elles ou aux porteurs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaire à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de certification

L'AC a pour obligation de :

- pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre 4.4 ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligation 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 un lien contractuel/ hiérarchique/ réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification avec les exigences émises dans la présente PC. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC, par elle-même ou l'une de ses composantes. Elle prend 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 donnée 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, quand 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 est approuvée par les instances de haut niveau de l'AC.
En cas de non-respect ponctuel des obligations décrites dans la présente PC, l'administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

9.6.2 Service d'enregistrement

Cf. les obligations pertinentes du chapitre 9.6.1.

9.6.3 Porteurs de certificats

Le porteur a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande du certificat ;

- Protéger sa clé privée par des moyens appropriés à son environnement ;
- Protéger ses données d'activations et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à sa base de certificats ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- Faire, sans délai, une demande de révocation de son certificat auprès de l'AE, et ce à travers le Abonné en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

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

9.6.4 Utilisateurs de certificats

Le porteur a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger sa clé privée par des moyens appropriés à son environnement ;
- Protéger ses données d'activations et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à sa base de certificats ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- Faire, sans délai, une demande de révocation de son certificat auprès de l'AE, et ce à travers le Abonné en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

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

9.6.5 Autres participants

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

9.7 Limites de garanties

Sans objet.

9.8 Limites de responsabilités

Sans Objet

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de la PC.
La durée de validité de la DPC associée peut être indépendante de la durée de vie de la PC, si la DPC a pris en compte les exigences de plusieurs PC ; dans ce cas elle reste valide jusqu'à la fin de validité des derniers certificats émis selon les PC auxquelles elle se rapporte.

9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, GBP 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.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'AC contrôle que tout projet de modification de sa PC reste conforme aux exigences de la présente PC. En cas de changement important, l'AC fait appel à une expertise technique pour en contrôler l'impact ;

9.12.2 Mécanisme et période d'information sur les amendements

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

9.12.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduit par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.
En particulier, l'OID de la PC de l'AC évolue dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC) intervient dans les exigences de la présente PC applicable à la famille de certificats considérée

9.13 Dispositions concernant la résolution de conflits

Lors de la survenance d'un conflit et préalablement à toute procédure judiciaire, les Parties s'engagent à mettre en œuvre la procédure amiable suivante :

- dans un premier temps, à tenter de résoudre le litige à l'amiable ;
- dans un second temps et en cas d'échec de la tentative de règlement amiable, un expert pourra être désigné dans les conditions suivantes :
-
    - la volonté de saisir un expert sera notifiée par la partie la plus diligente à l'autre partie par lettre recommandée avec accusé de réception. A compter de la réception de ladite lettre, les parties disposent d'un délai de 15 jours calendaires afin de procéder, d'un commun accord, à la désignation d'un

expert amiable. A défaut d'accord dans le délai précité, une procédure judiciaire pourra être déclenchée ;

- les modalités de financement de l'intervention de l'expert devront être acceptées par les deux Parties avant le commencement de l'expertise. A défaut d'accord sur ce point, une procédure judiciaire pourra être déclenchée ;

- les Parties s'attacheront à se conformer à la position qui sera exprimée par l'expert. En cas de conciliation, les Parties signeront, s'il y a lieu un accord transactionnel. A défaut d'accord amiable entre les Parties, l'expert établira un procès-verbal de non conciliation en trois exemplaires datés et signés. Un exemplaire sera remis à chacune des Parties. Aucune action contentieuse ne pourra être introduite avant l'expiration d'un délai d'un jour franc à compter de la date figurant sur le procès-verbal de non-conciliation.

9.14 Juridictions compétentes

Les éventuels litiges seront traités par le tribunal compétent.

9.15 Obligations aux législations et réglementations

9.16 Dispositions diverses

9.16.1 – Accord global

La présente PC ne formule pas d'exigences spécifiques sur le sujet.

9.16.2 – Transfert d'activités

Cf. chapitre 5.8.1.1

9.16.3 Conséquences d'une clause non valide

La présente PC ne formule pas d'exigences spécifiques sur le sujet.

9.16.4 Application et renonciation

La présente PC ne formule pas d'exigences spécifiques sur le sujet.

9.16.5 – Force majeure

Les cas de force majeurs habituellement appliqués sont ceux définis au niveau du Dahir formant le code des obligations et des contrats.

9.16.6 – Autres dispositions

Sans objet.