POLITIQUE DE CERTIFICATION

AUTORITÉS DE CERTIFICATION

CHAABI ESIGN – Seals CA

Version 0.1

MODIFICATIONS

Date	Etat	Version	Commentaires
16/12/2023	Validé	0.1	Création du document.

REFERENCES

Référence	Version	Titre des documents

Table des matières

1 – INTRODUCTION

1.1 Présentation générale

Le Groupe Banque Populaire (GBP) a mis en place une Infrastructure à Gestion de Clés afin de délivrer des certificats cachets pour ses besoins internes ainsi que ses filiales et partenaires Cette infrastructure à Gestion de Clés est nommée IGC et est déclinée en plusieurs Autorités de Certification pour la délivrance des différents types de certificats.

Cette ICG est basée sur l'Autorité de Certification (nommée AC) « Chaabi eSign – Root CA».

Ce document constitue la politique de Certification (notée PC dans la suite du document). Elle définit comment le GBP met en œuvre les procédures et les exigences techniques relatives à l'AC « Chaabi eSign - Seals CA » qui sont détaillées dans le Politique de Certification (PC) de l'AC « Chaabi eSign - Seals CA » correspondante.

Le GBP a créé une hiérarchie de certification structurée sur la base :

- d'une Autorité de Certification Racine, l'AC « Chaabi eSign – Root CA », signant :
  - des certificats d'Autorité de Certification Subordonnée (ACS)

Chacune des AC émet plusieurs types de certificats, selon différents profils.
Dans le cadre de cette PC, l'Autorité de Certification est GBP dûment représenté par le Directeur Général adjoint qui est le responsable du pôle Système Informatique.

Dans le cadre de cette activité il peut, s'il le souhaite, déléguer cette fonction à une personne de son choix ayant le même périmètre fonctionnel tout en conservant une séparation hiérarchique et fonctionnelle avec le responsable AE.

L'AC est en charge de l'application de la présente PC. L'AC est responsable des certificats signés en son nom et de l'ensemble de l'infrastructure à clé publique (IGC) qu'elle a mise en place.

1.2 Identification du document

La présente PC est dénommée Politique de Certification de l'Autorité de Certification Chaabi eSign - Seals CA
Elle peut être identifiée par son numéro d'OID.
Le numéro d'OID du présent document est :
1.2.504.1.1.2.1.3.7.1

1.3 Entités intervenant dans l'IGC

1.3.1 Autorités 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 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) et(OCSP).

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.
L'AC « Chaabi eSign Seals CA » s'engage à respecter les obligations décrites dans la présente PC. Elle s'engage également à ce que les composants de l'IGC, internes ou externes à l'AC, auxquels elles incombent les respectent aussi.

1.3.2 Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur RCC et les informations liées au cachet

Pour cela, l'AE assure les tâches suivantes:

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

1.3.3 Responsables de certificats de cachets

Un RCC est une personne physique qui est responsable de l'utilisation du certificat de cachet du serveur informatique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat.
Le RCC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RCC respecte les conditions qui lui incombent définies dans la PC de l'AC, qui doit reprendre les conditions définies dans la présente PC.
Il est à noter que le certificat étant attaché au serveur informatique et non au RCC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RCC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.
L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RCC de ses fonctions et lui désigner un successeur. Une AC doit révoquer un certificat de cachet pour lequel il n'y a plus de RCC explicitement identifié.

1.3.4 Utilisateurs de certificats

La présente PC traitant de certificats de cachet (cf. chapitre I.4), un utilisateur de certificats peut être notamment :

- Un agent (personne physique) destinataire de données signées par un cachet informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager destinataire de données provenant d'un serveur informatique d'une autorité administrative et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.

1.3.5 Autres participants

I.3.5.1. Composantes de l'IGC

Sans objet

I.3.5.2. Mandataire de certification

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

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

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

- Effectuer correctement et de façon indépendante les contrôles d'identité et des éventuels attributs des futurs RCC et serveurs informatiques de l'entité pour laquelle il est MC,

- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent. L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

Le MC n'a en aucun cas accès aux moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat de cachet délivré au RCC.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

I.4.1.1. Bi-clés et certificats du serveur informatique

La présente PC traite des bi-clés et des certificats utilisés par des services applicatifs déployés sur des serveurs informatiques dont la fonction est de signer des données, afin que les catégories d'utilisateurs de certificats identifiées au chapitre I.3.4 ci-dessus puissent en vérifier la signature (le cachet).

Ceci correspond notamment aux relations suivantes :

- apposition d'un cachet sur des données par un serveur informatique d'une autorité administrative et vérification de ce cachet par un usager,
- apposition d'un cachet sur des données par un serveur informatique et vérification de ce cachet par un agent,
- apposition d'un cachet sur des données par un serveur informatique et vérification de ce cachet par un autre serveur informatique

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

Cette PC comporte également des exigences, lorsque nécessaire, concernant les bi-clés et certificats de l'AC (signature des certificats cachets serveurs, des LCR) ainsi que des clés, bi-clés et certificats des composantes de l'IGC.

L'AC génère et signe différents types d'objets : certificats, LCR

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

1.4.2 Domaines d'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 Gestion de la PC

1.5.1 Entité gérant la PC

La gestion de la PC est de la responsabilité de la DSI.

1.5.2 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@BCP.co.ma
Banque Centrale Populaire
Angle Mohamed El Bakri & Angle Mohamed Diouri
Casablanca Maroc

.

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

La conformité de la DPC avec la PC est assurée par le responsable de l'AC

1.5.4 Procédures 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 afin :

- D'assurer sa conformité aux normes de sécurité attendues par les applications qui référencent des familles de certificat porteur ;
- D'adapter aux évolutions technologiques

1.6 Définitions et acronymes

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
CEN	Comité Européen de Normalisation
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
RCC	Responsable du Certificat de Cachet
RSA	Rivest Shamir Adelman
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

1.6.2 Définitions

Les termes utilisés dans la présente PC sont les suivants :

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

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

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

Autorités administratives - Ce terme générique, désigne les administrations de l'Etat, les

collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

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

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage de GBP.

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge,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 du chapitre I.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

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

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

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

Dispositif de création de cachet - Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée pour la création de cachet.

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

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

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

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

Fonction de publication - Cf. chapitre I.3.1.

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

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

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de

certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Mandataire de certification - Cf. chapitre I.3.1.

Personne autorisée - Cf. chapitre I.3.1.

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 RCC et les utilisateurs de certificats.

Porteur - Cf. chapitre I.3.1.

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

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

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

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

Qualification d'un produit de sécurité - Acte par lequel la DGSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS].

Responsable du certificat de cachet - Cf. chapitre I.3.1.

Serveur informatique - Il s'agit d'un service applicatif (disposant d'un certificat fourni par l'AC) rattaché à l'entité, (identifiée dans le certificat) détenant le nom de domaine correspondant au service ou en charge de ce service.

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

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une

personne morale et procédant à des échanges électroniques avec des autorités administratives.

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

Utilisateur de certificat - Cf. chapitre I.3.1.

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

2.1 Entités chargées de la mise à disposition des informations

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

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

2.2 Informations devant être publiées

L'AC publie à destination des RCCS et utilisateurs de certificats :

- La PC;
- Les Conditions Générales d'Utilisation des services de certification Chaabi Cachet Serveur ;
- Les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, . . .) ;
- Le certificat d'AC « Chaabi eSign Root CA » et le certificat d'AC intermédiaire Chaabi eSign – Seals CA en cours de validité ;
- La liste des certificats révoqués (LAR / LCR) ;
- La DPC sur demande expresse auprès de BCP.

L'IGC 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 « Chaabi eSign Seals CA ». Ces informations sont publiées aux emplacements suivants :

http://www.gbp.ma/Documents/PC_Chaabi_eSign_Seals_CA.pdf

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

3. Identification et authentification

3.1 Nommage

3.1.1 Types de noms

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

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

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les services de création de cachet dans les certificats doivent être explicites.

L'identification de l'entité à laquelle ce service est rattaché est obligatoire.

Le DN a la forme suivante :

{

- C = Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée,
- CN = Identité et fonction du serveur informatique,
- O= Nom de l'entité à laquelle appartient le serveur informatique,
- OrrgId = identifiant de l'entité à laquelle appartient le serveur informatique.

}

3.1.3 Anonymisation ou pseudonymisation des services de création de cachet

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

3.1.4 Règles d'interprétation des différentes formes de nom

Les noms utilisés pour les certificats des AC du GBP sont suffisamment explicites, et ne nécessitent pas d'interprétation particulière.

3.1.5 Unicité des noms

L'AC est responsable de l'unicité des noms des serveurs utilisés dans ses certificats et de la résolution des litiges portant sur la revendication d'utilisation d'un nom. Cet engagement de responsabilité s'appuie sur le niveau de contrôle assuré lors du traitement des demandes de certificats et sur l'unicité du numéro de série.

3.1.6 Identification, authentification et rôle des marques

déposées La présente PC ne formule pas d'exigence spécifique

sur le sujet.

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

3.2 Validation initiale de l'identité

L'enregistrement d'un RCC se fait directement auprès de l'AE (AE ou AED).

L'enregistrement d'un service de création de cachet d'une entité auquel un certificat doit être délivré se fait via l'enregistrement du RCC correspondant.

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

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

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

- Enregistrement d'un RCC sans MC pour un certificat de cachet à émettre : validation par l'AE de l'identité "personne morale" d'entité de rattachement du RCC, de l'identité "personne physique" du futur RCC, de son habilitation à être RCC pour le service de création de cachet considérée et pour l'entité considérée.

- Enregistrement d'un nouveau RCC sans MC pour un certificat de cachet déjà émis : validation par l'AE de l'identité "personne physique" du futur RCC et de son habilitation à être RCC pour le service de création de cachet considéré et pour l'entité considérée.

3.2.1 Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par les composantes de l'IGC et par l'AC est réalisée par les procédures de génération de la bi-clé privée correspondante à la clé publique du certificat de l'AC.

3.2.2 Validation de l'identité d'un organisme

Cf. chapitre 3.2.3

3.2.3 Validation de l'identité d'un individu

IV.9.2.1. Enregistrement d'un RCC sans MC pour un certificat de cachet à émettre

L'enregistrement du futur RCC (personne physique) représentant une entité nécessite, l'identification de cette entité et l'identification de la personne physique. S'agissant d'un certificat de cachet, le RCC doit de plus être habilité en tant que RCC pour le service de création de cachet considéré.

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

- une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du service de création de cachet concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RCC comme étant habilité à être RCC pour le service de création de cachet pour lequel le certificat de cachet doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCC,
- [PARTENAIRE] toute pièce, valide lors de la demande de certificat, attestant de l'existence du partenaire notamment la raison sociale ou à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- [PARTENAIRE] tout document attestant de la qualité du signataire de la demande de certificat,
- un document officiel d'identité en cours de validité du futur RCC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- les conditions générales d'utilisation signées.

Le RCC est informé que les informations personnelles d'identité seront utilisées comme éléments d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

IV.9.2.2. Enregistrement d'un nouveau RCC sans MC pour un certificat de cachet déjà émis

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

L'enregistrement du nouveau RCC (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le service de création de cachet est rattaché et en tant que RCC pour ce service.

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

- un mandat, daté de moins de 3 mois, désignant le futur RCC comme étant habilité à être le nouveau RCC pour le service de création de cachet auquel le certificat a été délivré, en remplacement du RCC précédent. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCC,
- [PARTENAIRE] tout document attestant de la qualité du signataire du mandat,
- un document officiel d'identité en cours de validité du futur RCC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- les conditions générales d'utilisation signées.

Le RCC est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

3.2.4 Informations non vérifiées du RCC et/ou du serveur informatique

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

3.2.5 Validation de l'autorité du demandeur

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

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

3.3.1 Identification et validation pour un renouvellement courant

Le renouvellement de la bi-clé d'un serveur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat de cachet ne peut pas être fourni au RCC sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

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

3.3.2 Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement doit être identique à la procédure d'enregistrement initial.

3.4 Identification et validation d'une demande de révocation

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

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificate

4.1.1 Origine d'une demande de certificat

Un certificat peut être demandé par un représentant légal de l'entité, avec consentement préalable du futur RCC.

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

Les informations suivantes doivent faire partie de la demande de certificat (cf. chapitre 3.2 ci- dessus) :

- le nom du service de création de cachet à utiliser dans le certificat ;

- les données personnelles d'identification du RCC ;
- les données d'identification de l'entité.

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

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

4.2 Traitement d'une demande de certificate

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

Les identités "personne physique" et "personne morale" sont vérifiées conformément aux exigences du chapitre 3.2.

L'AE, doit effectuer les opérations suivantes :

- valider l'identité du futur RCC ;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le futur RCC a pris connaissance des modalités applicables pour l'utilisation du certificat (les conditions générales d'utilisation).

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

L'AE conserve ensuite une trace des justificatifs présentés :

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

4.2.2 Acceptation ou rejet de la demande

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

4.2.3 Durée d'établissement du certificat

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

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à la validation de l'identité du demandeur et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au RCC.

Le processus de génération du certificat doit être lié de manière sécurisée au processus de génération de la bi-clé : l'ordonnancement des opérations doit être assuré ainsi que, le cas échéant en fonction de l'architecture de l'IGC, l'intégrité et l'authentification des échanges entres les

composantes. Par ailleurs, la clé privée est transmise de façon sécurisée au RCC, en en garantissant l'intégrité et la confidentialité.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous.

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

Le certificat complet et exact est mis à la disposition du RCC.
La remise du certificat peut se faire en main propre auprès de l'AE ou bien par courrier postal avec accusé de réception. L'adresse utilisée est l'adresse du R.C. saisie lors du processus de demande.

4.4 Acceptation du certificat

L'acceptation est tacite à compter de la date d'envoi du certificat (ou des informations de téléchargement) au RC.

4.4.1 Démarche d'acceptation du certificat

L'acceptation est tacite à compter de la date de génération et de stockage de la Bi-clé et du certificat associé sous la présence du RC.

4.4.2 Publication du certificat

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

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

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

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le RCC

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service de cachet de données émises par le serveur. Les RCC doivent s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

Cf. chapitre précédent et chapitre I.4.

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

4.6 Renouvellement d'un certificat

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

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au RCC de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

Ce chapitre traite de la délivrance d'un nouveau certificat de cachet liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des serveurs, et les certificats correspondants, seront renouvelées au maximum à une fréquence de trois ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du serveur.

4.7.2 Origine d'une demande d'un nouveau certificat

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

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

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

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

Pour les actions de l'AC, cf. chapitre 4.3.1.

4.7.4 Notification au RCC de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8 Modification du certificat

La modification de certificat n'est pas autorisée dans la présente PC. En cas de nécessité de modification d'informations présentes dans le certificat, un nouveau certificat sera délivré après révocation de l'ancien certificat.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.8.4 Notification au RCC de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

IV.9.1.1. Certificats de cachet

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

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

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance, le certificat concerné est révoqué.

IV.9.1.2. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :

- 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.

4.9.2 Origine d'une demande de révocation

IV.9.2.3. Certificats de cachet

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

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

Le RCC est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité.

IV.9.2.4. Certificats d'une composante de l'IGC

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

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

4.9.3 Procédure de traitement d'une demande de révocation

IV.9.2.5. Révocation d'un certificat de cachet

La demande de révocation est opérée auprès de l'AE ou de l'AC

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

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

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via une LCR signée par une entité désignée par l'AC.

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

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

IV.9.2.6. 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 l'ensemble des RCC concernés que leurs certificats cachet correspondants ne sont plus valides.

Pour cela, l'IGC envoie des récépissés aux AE et aux MC. Ces derniers informe les RCC en leur indiquant explicitement que leurs certificats cachet ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

4.9.4 Délai accordé au RCC pour formuler la demande de révocation

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

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

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 de signature de jeton d'horodatage est traitée dans un délai inférieur à 72h. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

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

L'utilisateur d'un certificat de cachet est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR est la suivante :

- Configuration des LCR :
  - Période de publication : 1 jours ;
  - Overlap (marge): 0 jours ;

Durée de validité : 1 jours ;

4.9.8 Délai maximum de publication d'une LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de publication de LCR et, le cas échéant, de Delta LCR, celles-ci doivent être publiées et disponibles pour le téléchargement au maximum dans les 30 minutes suivant leur génération.

IV.9.2.7. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Sans Objet

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

Cf. chapitre 4.9.6 ci-dessus.

4.9.10 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.11 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de cachet, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la

compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre IV.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens.

Quant au R.C., l'A.C. impose par voie contractuelle qu'en cas de compromission de sa clé privée du R.C. ou de connaissance de la compromission de la clé privée de l'A.C. ayant émis son certificat, le R.C. s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.12 Causes possibles d'une suspension

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

4.9.13 Origine d'une demande de suspension

Sans objet.

4.9.14 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.15 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

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

La fonction d'information sur l'état des certificats mets à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR / LAR. Ces LCR / LAR sont des LCR au format V2, publiées dans un annuaire accessible en protocole LDAP V3.

4.10.2 Disponibilité de la fonction

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 2 heures et une durée maximale totale d'indisponibilité par mois de 8 heures.

4.10.3 Dispositifs optionnels

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

4.11 Fin de la relation entre le RCC et l'AC

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

De plus, l'AC doit révoquer un certificat de cachet pour lequel il n'y a plus de RCC explicitement identifié.

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des serveurs est interdit par la présente PC. Les clés privées d'AC ne doivent pas non plus être séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5. Mesures de sécurité non techniques

Ce chapitre 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 le 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 – Root CA » respecte.

5.1 Mesures de sécurité physique

Le 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 GBP.

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

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 – Root 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.

Les locaux de l'IGC sont cloisonnés dans une zone dite « core banking » et isolés avec sa propre porte et son accès physique dédié.

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 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.

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.

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 devront être détruits.
Les procédures et moyens de destruction sont conformes au niveau de confidentialité des informations correspondantes.

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.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiance suivants sont identifiés au sein du GBP 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 GBP.
- **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 du GBP ;
- Porteurs de secret : ces personnes portent les secrets d'initialisation des boitiers cryptographiques. Un Quorum de 3 porteurs différents parmi 6 est défini.

5.2.2 Nombre de personnes requises par tâche

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

Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur un nombre de 5 personnes. Les fonctions sont séparées comme suit :

- Officier Sécurité IGC (CMO)
- Maitre de Cérémonie / Administrateur IGC

- Administrateur Autorité de Certification
- Opérateur Autorité Certification
- Auditeur.

5.2.3 Rôles exigeant une séparation des attributions

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 interdis :

- 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 du GBP, qu'il s'agisse du personnel interne au 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 autorisée
- Les exigences vis-à-vis du personnel des prestataires externes,
- La documentation fournie à la personne

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 du GBP.
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 Procédure de vérification des antécédents

Le personnel est soumis aux procédures de recrutements internes du GBP qui inclut une vérification des antécédents.
Ces personnels n'ont pas de condamnation de justice en contradiction avec leurs attributions. Ils devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire. Les personnes ayant un rôle de confiance ne 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 ont connaissance et comprendre 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. Les sanctions sont précisées dans la DPC. Le 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 également 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 l'automatique. Les fichiers résultants, sous forme papier ou électronique, 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 du 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. Ces mécanismes seront implémentés suite à la mise en production de l'IGC.
Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.
Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).
Le système de datation des évènements respecte les exigences du chapitre 6.8
La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'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 GBP pour les journaux qui la concerne.

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

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 accords contractuels avec d'autres AC ;
- Les certificats, LCR ou réponses OCSP tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les justificatifs d'identité des RC 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.
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 et réponses OCSP émis par l'AC

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.
Les réponses OCSP produites sont archivées pendant au moins trois mois 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 devront offrir le même

niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre 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

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

Un AC Racine ne peut pas générer des certificats pour les AC subordonnées dont les dates de fin seraient postérieures à la date d'expiration du certificat de l'AC « Chaabi eSign – Root CA ».
De ce fait, la période de validité du certificat d'AC RACINE est supérieure à celle des certificats des AC subordonnées.
Lorsqu'un nouveau certificat d'AC « Chaabi eSign – Root CA » est émis, le certificat de l'AC « Chaabi eSign – Root CA » précédent peut toujours être utilisé pour vérifier l'authenticité des certificats d'AC subordonnées émis sous cet ancien certificat, et ce jusqu'à ce que ces certificats d'AC subordonnées 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 du GBP 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 – Root CA », l'évènement déclencheur est la constatation de l'incident au niveau de la composante concernée.
Une information au niveau de la direction du GBP est immédiatement menée.
En cas de révocation du certificat de l'AC « Chaabi eSign – Root CA », l'information est publiée dans l'urgence dans l'annuaire interne.

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 au minimum les engagements suivants :

- informer les entités suivantes de la compromission : tous les porteurs, MC 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.

5.8 Fin de vie de l'IGC

En cas d'interruption de ses activités, le 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, le GBP s'engage à :

- communiquer suivant un préavis correspondant son intention de cesser son activité IGC ;
- informer les autorités compétentes ;
- mettre en œuvre tous les moyens dont il dispose pour informer ses Seals ;

- révoquer ses certificats d'AC RACINE, AC Subordonnées ;
- révoquer tous les certificats émis ;
- assurer la pérennité des LARs émises.

En cas de transfert de l'activité à un tiers, le 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.
Le 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. Mesure de sécurité technique

6.1 Génération et installation de biclés

6.1.1 Génération des biclés

La génération des clés des serveurs est effectuée dans un environnement sécurisé (*cf.* chapitre V). Les biclés des serveurs sont générées dans un module cryptographique ou dans un autre dispositif de création de cachet conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de création de signature destiné au serveur sans que l'A.C. n'en garde aucune copie.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée générée par l'A.C. est transmise au serveur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission se fait directement dans le dispositif de création de cachet destiné au serveur.

Une fois remise, la clé privée est maintenue sous le seul contrôle du R.C. L'A.C. ne conserve ni ne duplique cette clé privée.

6.1.3 Transmission de la clé publique à l'AC

Sans objet

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

Sans objet

6.1.5 Tailles des clés

La taille des bi-clés des A.C. 4096 bits.

La taille des bi-clés des R.C. est de 3072 bits.

6.1.6 Vérification de la génération des paramètres des biclés et de leur qualité

L'équipement de génération de biclés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la biclé. Les paramètres et les algorithmes de signature sont documentés au chapitre VII

6.1.7 Objectifs d'usage de la clé

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

L'utilisation de la clé privée du R.C. et du certificat associé est strictement limitée au service de cachet.

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

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 Fips 140-2 niveau 3 et CC EAL4+

6.2.1.2 Dispositifs de création des cachets

Les dispositifs de création de signature cachet serveur et de protection de clés privées des serveurs, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre ci-dessous pour le niveau de sécurité considéré. Si l'AC ne fournit pas elle-même ce dispositif au RCC, elle doit s'assurer auprès du RCC de la conformité du dispositif mis en œuvre par le serveur, au minimum au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC. En revanche, lorsque l'AC fournit ce dispositif au RCC, directement ou indirectement, elle doit s'assurer que :

- La préparation des dispositifs de création de signature cachet serveur est contrôlée de façon sécurisée ;
- les dispositifs de création de signature cachet serveur sont stockés et distribués de façon sécurisée ;
- les désactivations et réactivations des dispositifs de création de signature cachet serveur sont contrôlées de façon sécurisée.

6.2.2 Contrôle de la clé privée par plusieurs personnes

6.2.2.1 Clé privée AC

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

6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des serveurs 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 la BCP.

6.2.4.2 Bi-clés serveur

Les clés privées des serveurs 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 serveurs 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 un minimum de 3 personnes (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 cachets

La méthode d'activation de la clé privée du serveur dépend du dispositif utilisé. L'activation de la clé privée du serveur doit au minimum être contrôlée via des données d'activation (cf. chapitre 6.4) et doit permettre de répondre aux exigences définies pour le niveau de sécurité considéré.

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 serveurs

Il n'y a pas de méthode de désactivation pour la clé privée des serveurs

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 serveurs

En fin de vie ou une décision de fin d'utilisation anticipée (révocation) d'une clé privée de signature cachet serveur dans un serveur, le certificat logiciel est complétement supprimé de ce serveur après sa révocation.

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 - Seals 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 des certificats de l'AC sont de 10 ans.

6.3.2.2 Bi-clé et certificat cachet

Les bi-clés et les certificats des serveurs couverts par la présente PC ont une durée de vie de 3 ans.

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.

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

L'AC génère la clé privée du serveur, et le transmet au RCC, et les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données. Ces données d'activation sont sous forme de mots de passe aléatoire généré par l'AC que le RCC pourra changer par la suite avant de le mettra à disposition du serveur.

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 clés privées d'AC ne peuvent être activées dans le module cryptographique qu'avec un minimum de 3 personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

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

Les données d'activation des clés privées des serveurs sont des codes PIN générés aléatoirement par l'AC, elles sont protégées en intégrité et en confidentialité jusqu'à la remise aux RCC.

Les clés privées des serveurs sont activées suite à la saisie du code PIN.

6.4.3 Autres aspects liés aux données d'activation

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

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

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 GBP sont activées est isolé.

6.8 Horodatage / système de datation

Les systèmes de datation sont synchronisés par rapport à une source fiable du temps universel (UTC) et un système de synchronisation temporelle (NTP) avec une précision au moins égale à une minute.

7. Profil des certificats et des LCR

7.1 Certificats cachet

Le tableau suivant renseigne les valeurs par défaut des attributs d'un Certificat de signature de cachet serveur émis par l'AC Chaabi eSign Seals CA
Le format de ce Certificat ainsi que ses attributs respectent le profil X.509v3 décrit dans la RFC 5280

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 – Seals CA » O= «Groupe Banques Populaires » C= MA

Valide à partir de		Date de génération du certificat	
Valide jusqu'au		Date de génération +3ans	
		CN	Nom significatif du service mettant en oeuvre le cachet
		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 »
		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= 1.2.504.1.1.2.1.3.7.1	
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_Seals_CA.cer	
Point de distribution CRL		http://crl.gbp.ma/crldp/chaabi_eSign_Seals_CA.crl	

Utilisation de clé	**oui**	Signature numérique, Non répudiation
Algorithme d'empreinte numérique		SHA-1

7.2 Liste de Certificats Révoqués

Elément		**Valeur**
Version		V2
Emetteur		CN= « Chaabi eSign - Seals 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

7.3 Certificat de l'A.C émettrice

Le tableau ci-dessous décrit les valeurs des attributs du Certificat de l'AC « Chaabi eSign - Seals CA » émis par
l'AC racine « Chaabi eSign Root 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].

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 - 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. - Seals 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= 1.2.504.1.1.2.1.3.7.1	
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	

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 du groupe ;
- 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 du Groupe sont tenus de se conformer aux :

- dispositions prévues par la circulaire CFD-403 « Code de Déontologie et d'Ethique du GBP » ;
- 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 doivent pas prendre 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 ;

- 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 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

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

Au sein des organismes du BCP 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 régionaux ;
- 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

Ils sont composés par :

- Le Président du conseil de surveillance ;
- Des membres du conseil de surveillance nommément désignés ;
- Le directeur de la fonction audit interne de la BPR en tant que secrétaire du Comité.

A noter qu'au même titre que le comité d'audit GBP, le président du comité d'audit régional peut inviter d'autres personnes à prendre part aux réunions dudit comité. Il s'agit notamment, des commissaires aux comptes, du président du directoire de la BPR et de certains responsables et ce pour fournir les explications nécessaires.

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 les organismes du BCP et leurs filiales 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 « Chaabi eSign - Seals CA ».

Si des risques critiques sont constatés la demande de délivrance de certificat est refusée.
Selon les non-conformités observées, l'AC «Chaabi eSign - Seals CA » 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.

8.6 Communication des résultats

La publication des résultats de l'évaluation est faite sous forme de rapports réglementaires. Ces rapports doivent suivre les règlements suivants :

- Rapport sur le Contrôle Interne au sein du BCP en application des dispositions des articles n°90 à 93 de la Circulaire n°40/G/2007 de Bank Al Maghrib, régissant le Contrôle Interne dans les établissements de crédit ;
- Rapport au Comité Directeur stipulé dans les articles n°31 et 32 de la loi 44-08 modifiant la loi 12-96 portant réforme du BCP et l'article n°10 du Règlement intérieur du Comité Directeur ;

Rapport aux Conseils de Surveillance ou aux Conseils d'Administration des BPR et filiales et Rapport au Comité d'Audit / GBP prévus par les dispositions de l'article n°33 de la loi 44-08 modifiant la loi 12-96 portant réforme du BCP.

9. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1 Tarifs

Les certificats seront facturés par le GBP pour les filiales (externes GBP).

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 porteur et au MC.

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 le 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 au GBP ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Le 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 le 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, du MC de son entreprise ou de l'AC 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 formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis. Ces informations s'appliquent également aux MC.

9.6.4 Utilisateurs de certificats

Les utilisateurs de la sphère publique utilisant les certificats :

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

L'AC n'émet dans sa propre PC d'obligations supplémentaires, par rapport aux obligations de la présente PC, à l'encontre des utilisateurs de la sphère publique.

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

Le GBP décline toute responsabilité en cas d'usage non-conforme des éléments de sécurité générés par son IGC.

Par ailleurs, le GBP s'exonère de toute responsabilité quant aux dommages indirects (perte d'image de marque, perte de bénéfices, trouble commercial…) éventuellement subi par les porteurs.

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, le 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 Conformité aux législations et réglementations

Les lois suivantes doivent être suivies afin d'être en conformité aux législations et réglementation en vigueur au Maroc :

- Les dispositions de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques promulguée par le dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020)

- Les dispositions du décret n° 2.22.687 pris pour l'application de la loi n°43-20

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 5.8-11.

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 majeure habituellement appliqués sont ceux définis au niveau du Dahir formant le code des obligations et des contrats.

9.17 Autres dispositions

Sans Objets.