POLITIQUE DE CERTIFICATION

AUTORITE DE CERTIFICATION

Chaabi eSign – SealsTS CA

Version 1.1

MODIFICATIONS

Date	Etat	Version	Commentaires

REFERENCES

Référence	Version	Titre des documents

Table des matières

1. INTRODUCTION 10

11 1 Présentation générale 10

12 2 Identification du document 11

13 3 Définitions et acronymes 11

1.3.1 Acronymes 11
1.3.2 Définitions 12

14 4 Entités intervenant dans l'IGC 16

1.4.1 Autorité de certification 16
1.4.2 Autorité d'enregistrement 17
1.4.3 Responsables de certificats 18
1.4.4 Porteurs de certificats 18
1.4.5 Utilisateurs de certificats 18
1.4.6 Autres participants 18

15 5 Usage des certificats 19

1.5.1 Domaines d'utilisation applicables 19
1.5.2 Domaines d'utilisation interdits 19

16 6 Gestion de la PC 19

1.6.1 Entité gérant la PC 19
1.6.2 Point de contact 19
1.6.3 Entité déterminant la conformité d'une DPC avec cette PC 19
1.6.4 Procédure d'approbation de la conformité de la DPC vis-à-vis de la PC 20

2. RESPONSABILITÉS CONCERNANT LA MISE À 20

21 1 Entités chargée de la mise à disposition des informations 20

22 2 Information devant être publiées 20

2.2.1 Publication de la Politique de Certification 20
2.2.2 Publication du certificat de l'Autorité de Certification 20
2.2.3 Publication de la liste des certificats/autorités révoqués 20

23 3 Délais et fréquences de publication 21

24 4 Contrôle d'accès aux informations publiées 21

3. IDENTIFICATION ET AUTHENTIFICATION 21

31 1 Nommage 21

3.1.1 Types de noms 21
3.1.2 Nécessité d'utilisation de noms explicites 21
3.1.3 Pseudonymisation des serveurs 22

3.1.4 Règles d'interprétation des différentes formes de noms 22
3.1.5 Unicités des noms 22
3.1.6 Identification, authentification et rôle des marques déposées 22

32 2 Validation initiale de l'identité 22
3.2.1 Méthode pour prouver la possession de la clé privée 23
3.2.2 Validation de l'identité d'un organisme 23
3.2.3 Informations non vérifiées du RC et/ou du serveur informatique 24
3.2.4 Validation de l'autorité du demandeur 24

33 3 Identification et validation d'une demande de renouvellement des clés 25
3.3.1 Identification et validation pour un renouvellement courant 25
3.3.2 Identification et validation pour un renouvellement après révocation 25

34 4 Identification et validation d'une demande de révocation 25

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 25

41 1 Demande de certificat 25
4.1.1 Origine d'une demande de certificat 25
4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat 25

42 2 Traitement d'une demande de certificat 26
4.2.1 Exécution des processus d'identification et de validation de la demande 26
4.2.2 Acceptation ou rejet de la demande 26
4.2.3 Durée d'établissement du certificat 26

43 3 Délivrance du certificat 26
4.3.1 Actions de l'AC concernant la délivrance du certificat 26
4.3.2 Notification par l'AC de la délivrance du certificat au RC 26

44 4 Acceptation du certificate 26
4.4.1 Démarche d'acceptation du certificat 27
4.4.2 Publication du certificat 27
4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat 27

45 5 Usage de la bi-clé et du certificat 27
4.5.1 Utilisation de la clé privée et du certificat par le RC 27
4.5.2 Utilisation de la clé publique et du certificat par Le porteur du certificat 27

46 6 Renouvellement d'un certificat 27
4.6.1 Causes de renouvellement d'un certificat 27
4.6.2 Origine d'une demande de renouvellement 27
4.6.3 Procédure de traitement d'une demande de renouvellement 27
4.6.4 Notification au RC de l'établissement du nouveau certificat 27
4.6.5 Processus d'acception du nouveau certificat 28
4.6.6 Démarche de publication du nouveau certificat 28
4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat 28

47 7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE 28
4.7.1 Causes possibles de changement d'une Bi-clé 28
4.7.2 Origine d'une demande d'un nouveau certificat 28
4.7.3 Procédure de traitement d'une demande d'un nouveau certificat 28
4.7.4 Notification au RC de l'établissement du nouveau certificat 28

4.7.5 Démarche d'acceptation du nouveau certificat 28
4.7.6 Publication du nouveau certificat 28
4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat 28

4.8 8 MODIFICATION DU CERTIFICAT 29
4.8.1 Causes possibles de modification d'un certificat 29
4.8.2 Origine d'une demande de modification d'un certificat 29
4.8.3 Procédure de traitement d'une demande de modification d'un certificat 29
4.8.4 Notification au RC de l'établissement du certificat modifie 29
4.8.5 Démarche d'acceptation du certificat modifie 29
4.8.6 Publication du certificat modifie 29
4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat modifie 29

4.9 9 Révocation et suspension des certificats 29
4.9.1 Causes possibles d'une révocation 29
4.9.2 Origine d'une demande de révocation 30
4.9.3 Procédure de traitement d'une demande de révocation 31
4.9.4 Délai accordé au RC pour formuler la demande de révocation 31
4.9.5 Délai de traitement par l'AC d'une demande de révocation 31
4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats 32
4.9.7 Fréquence d'établissement des LCR 32
4.9.8 Délai maximum de publication d'une LCR 32
4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état descertificats 32
4.9.10 Exigences de vérification en ligne de la révocation des certificats par lesapplications utilisatrices de certificats 32
4.9.11 Autres moyens disponibles d'information sur les révocations 32
4.9.12 Exigences spécifiques en cas de compromission de la clé privée 32
4.9.13 Causes possibles d'une suspension 32
4.9.14 Origine d'une demande de suspension 33
4.9.15 Procédure de traitement d'une demande de suspension 33
4.9.16 Limites de la période de suspension d'un certificat 33

4.10 0Fonction d'information sur l'état des certificats 33
4.10.1 Caractéristiques opérationnelles 33
4.10.2 Disponibilité de la fonction 33
4.10.3 Dispositifs optionnels 33

4.11 1FIN DE LA RELATION ENTRE LE RC ET L'AC 33

4.12 2SEQUESTRE DE CLE ET RECOUVREMENT 34
4.12.1 Politique et pratiques de recouvrement par séquestre des clés 34
4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session 34

5. MESURE DE SÉCURITÉ NON TECHNIQUES 34

5.1 1 Mesures de sécurité physique 34
5.1.1 Situation géographique et construction des sites 34
5.1.2 Accès physique 35
5.1.3 Alimentation électrique et climatisation 35
5.1.4 Vulnérabilité aux dégâts des eaux 35
5.1.5 Prévention et protection incendie 35
5.1.6 Conservation des supports 36
5.1.7 Mise hors service des supports 36

5.1.8 Sauvegarde hors site 36

5.2 2 Mesures de sécurité procédurales 36
5.2.1 Rôles de confiance 36
5.2.2 Nombre de personnes requises par tâches 37
5.2.3 Identification et authentification pour chaque rôle 37
5.2.4 Rôles exigeant une séparation des attributions 37

5.3 3 Mesures de sécurité vis-à-vis du personnel 38
5.3.1 Qualifications, compétences et habilitations requises 38
5.3.2 Procédures de vérification des antécédents 38
5.3.3 Exigences en matière de formation initiale 39
5.3.4 Exigences et fréquences en matière de formation continue 39
5.3.5 Fréquence et séquence de rotation entre différentes attributions 39
5.3.6 Sanctions en cas d'actions non autorisées 39
5.3.7 Exigences vis-à-vis du personnel des prestataires externes 39
5.3.8 La documentation fournie au personnel 39

5.4 4 Procédures de constitution des données d'audit 39
5.4.1 Type d'événement à enregistrer 39
5.4.2 Fréquence de traitement des journaux d'évènements 40
5.4.3 Période de conservation des journaux d'évènements 40
5.4.4 Protection des journaux d'événements 40
5.4.5 Procédure de sauvegarde des journaux d'événements 41
5.4.6 Système de collecte des journaux d'événements 41
5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement 41
5.4.8 Évaluation des vulnérabilités 41

5.5 5 Archivage des données 41
5.5.1 Types de données à archiver 41
5.5.2 Période de conservation des archives 42
5.5.3 Protection des archives 43
5.5.4 Procédure de sauvegarde des archives 43
5.5.5 Exigences d'horodatage des données 43
5.5.6 Système de collecte des archives 43
5.5.7 Procédure de récupération et de vérification des archives 43

5.6 6 Changement de clés d'AC 43

5.7 7 Reprise suite à compromission et sinistre 44
5.7.1 Procédures de remontée et de traitement des incidents et des compromissions 44
5.7.2 Procédures de reprise en cas de corruption des ressources informatiques(matériels, logiciels et / ou donnée) 44
5.7.3 Procédures de reprise en cas de compromission de la clé privée d'unecomposante 44
5.7.4 Capacités de continuité d'activités suite à un sinistre 44

5.8 8 Fin de vie de l'IGC 45

6. MESURES DE SÉCURITÉ TECHNIQUES 45

6.1 1 Génération et installation de bi-clés 45
6.1.1 Génération des bi-clés 45
6.1.2 Transmission de la clé privée au serveur 46
6.1.3 Transmission de clé publique à l'AC 46

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats 46
6.1.5 Tailles des clés 46
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité 46
6.1.7 Objectifs d'usage de la clé 46

62 2 Mesures de sécurité pour la protection des clés privées etpour les modules cryptographiques 47
6.2.1 Standards et mesures de sécurité pour les modules cryptographiques 47
6.2.2 Contrôle de la clé privée par plusieurs personnes 47
6.2.3 Séquestre de la clé privée 47
6.2.4 Copie de secours de clé privée 47
6.2.5 Archivage de la clé privée 48
6.2.6 Transfert de la clé privée vers / depuis le module cryptographique 48
6.2.7 Stockage de la clé privée dans un module cryptographique 48
6.2.8 Méthode d'activation de la clé privée 48
6.2.9 Méthode de désactivation de la clé privée 48
6.2.10 Méthode de destruction des clés privées 48

63 3 Autres aspects de la gestion des bi-clés 49
6.3.1 Archivage des clés publiques 49
6.3.2 Durée de vie des bi-clés et des certificats 49

64 4 Données d'activation 49
6.4.1 Génération et installation des données d'activations 49
6.4.2 Protection des données d'activation 49
6.4.3 Autres aspects liés aux données d'activation 49

65 5 Mesures de sécurité des systèmes informatiques 50
6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques 50

66 6 Mesures de sécurité des systèmes durant leur cycle de vie 50
6.6.1 Mesures de sécurité liées au développement des systèmes 50
6.6.2 Mesures liées à la gestion de la sécurité 50
6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes 51

67 7 Mesures de sécurité réseau 51

68 8 Horodatage / système de datation 51

7. PROFILS DES CERTIFICATS ET CRLS 51

71 1 Profil Certficat AC 51

7.2 Certificats de signature des jetons d'horodatage 52

7.3 Profil des listes de certificats révoqués 53

7.4 Profil OCSP 54

8. AUDIT DE CONFORMITÉ ET AUTRESÉVALUATIONS 54

81 1 Fréquences et/ou circonstances des évaluations 54

82 2 Identités / qualification des évaluateurs 55

83 3 Relations entre évaluateurs et entités évaluées 55
8.3.1 Le comité d'audit GBP 56

8.3.2 Les comités d'audits régionaux 56
84 4 Sujets couverts par les évaluations 56
85 5 Actions prises suite aux conclusions des évaluations 56
86 6 Communication des résultats 57
9. AUTRES PROBLÉMATIQUES MÉTIERS ETLÉGALES 57
91 1 Tarifs 57
92 2 Responsabilité financière 57
93 3 Confidentialité des données professionnelles 57
9.3.1 Périmètre des informations confidentielles 57
9.3.2 Information hors du périmètre des informations confidentielles 58
9.3.3 Responsabilités en termes de protection des informations confidentielles 58
94 4 Protection des données à caractère personnel 58
9.4.1 Politique de protection des données à caractère personnel 58
9.4.2 Données à caractère personnel 58
9.4.3 Données à caractères non personnel 58
9.4.4 Responsabilité en termes de protection des données à caractère personnel 58
9.4.5 Notification et consentement d'utilisation des données à caractère personnel 58
9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciairesou administratives 59
9.4.7 Autres circonstances de divulgation de données à caractère personnel 59
95 5 Droits de propriété intellectuelle 59
96 6 Interprétations contractuelles et garanties 59
9.6.1 Autorités de certification 59
9.6.2 Service d'enregistrement 60
9.6.3 Porteurs de certificats 60
9.6.4 Utilisateurs de certificats 61
9.6.5 Autres participants 61
97 7 Limites de garanties 61
98 8 Limites de responsabilités 61
99 9 Indemnités 61
910 0 Durée et fin anticipée de validité de la PC 61
911 1 Notifications individuelles et communications entre les participants 62
912 2 Amendements à la PC 62
9.12.1 Procédures d'amendements 62
9.12.2 Mécanisme et période d'information sur les amendements 62
9.12.3 Circonstances selon lesquelles l'OID doit être changé 62
913 3 Dispositions concernant la résolution de conflits 62
914 4 Juridictions compétentes 63
915 5 Conformité aux législations et réglementations 63

9.16 6 Dispositions diverses 63
9.16.1 Accord global 63
9.16.2 Transfert d'activités 63
9.16.3 Conséquences d'une clause non valide 63
9.16.4 Application et renonciation 63
9.16.5 Force majeure 63

9.17 7 Autres dispositions 64

1. INTRODUCTION

1.1 1 Présentation générale

Le Groupe Banque Populaire (GBP) a mis en place une Infrastructure à Gestion de Clés afin de délivrer des certificats pour ses serveurs et ses agents sur l'ensemble du territoire marocain ainsi que ses filiales étrangères. 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 le Politique de Certification (notée PC dans la suite du document) mise en œuvre par l'AC « Chaabi eSign – SealsTS CA »
Le GBP a créé une hiérarchie de certification (illustrée sur le schéma ci-après) structurée sur la base :

Chacune des AC émet plusieurs types de certificats, selon différents profils.
L'AC Chaabi eSign - SealsTS CA émet notamment des certificats « Signature de jetons d'horodatage ». Ces certificats sont destinés à la signature de jetons émis par l'Autorité d'Horodatage de GBP.
Ces certificats sont de type logiciel.
Le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification Chaabi eSign - SealsTS CA - Profil « Signature de jetons d'horodatage » de GBP.

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.
L'AC « Chaabi eSign - SealsTS CA » émet des certificats « Signature de jetons d'horodatage ». Ils sont destinés à la signature de jetons émis par l'Autorité d'Horodatage de GBP.

Cette Politique de Certification a vocation à être consultée et examinée par les personnes qui utilisent ces certificats pour les aider à apprécier le degré de confiance qu'ils peuvent placer dans ces certificats. Cette Politique de Certification est un document public et est mise à disposition du public sous format électronique sur le site web de GBP.

1.2 2 Identification du document

La présente Politique de Certification est identifiée de manière unique par l'OID suivant :
OID
Ce document est complété par une Déclaration des Pratiques de certification correspondante référencée par le numéro d'OID : 1.2.504.1.1.2.1.3.9.1
La Politique de Certification et la Déclaration des Pratiques de Certification identifiées ci-dessus sont désignées dans la suite du document respectivement sous le nom de « PC » et de « DPC ».

1.3 3 Définitions et acronymes

1.3.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC	Autorité de Certification
ACR	Autorité de Certification Racine
ACS	Autorité de Certification Subordonnée
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage émettant des jetons d'horodatage à destination de Porteurs et de serveurs.
CN	Common Name
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
DSA	Digital Signature Algorithm
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés.
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Electronique
RC	Responsable du Certificat de Cachet. Il s'agit de la personne physique qui porte la responsabilité du certificat de signature des jetons d'horodatage.
RFC	Request For Comment
RGS	Référentiel Général de Sécurité

RSA	Rivest Shamir Adelman
SHA-2	Secure Hash-Algorithm Two
SSI	Sécurité des Systèmes d'Information
URL	Universal Ressource Locator
X.509	Format des certificats d'identité recommandé par l'Union Internationale des Télécommunications (UIT).

1.3.2 Définitions

Les termes utilisés dans la présente PC sont les suivants :

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

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins de signature du porteur du certificat.

Autorités administratives - Ce terme générique désigne les administrations de l'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 (AE) - Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.

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

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

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

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

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le

certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

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

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

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

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

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

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

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

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

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

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

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

Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises parl'autorité d'enregistrement et de la clé publique du porteur ou du responsable du certificat.

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

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

Fonction de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

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

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

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

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

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

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

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

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

Mandataire de certification - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis).

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

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

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

Qualification d'un prestataire de services de certification électronique - Acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

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

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

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

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

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

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

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

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

1.4 4 Entités intervenant dans l'IGC

L'AC « Chaabi eSign – Root CA » gère des certificats d'AC Subordonnées :

1.4.1 Autorité de certification

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

Afin de clarifier et faciliter l'identification des exigences, la décomposition fonctionnelle de l'IGC de GBP qui est retenue dans la présente PC est la suivante :

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

- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère la bi-clé du porteur.

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

- **Fonction de publication** - Cette fonction met à disposition les différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.

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

- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) ou selon un mode requête / réponse temps réel (OCSP).

Les fonctions de l'AC doivent être exécutées par du personnels autorisés ayant connaissance et respectant les règles, principes et procédures énoncés dans la PC et la DPC liées au fonctionnement de l'«Chaabi eSign - SealsTS».

L'AC assure ces fonctions directement ou en les déléguant, ou en les sous-traitant, pour tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.

1.4.2 Autorité d'enregistrement

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

- la prise en compte et la vérification des informations du futur RC, ainsi que son entité de rattachement et la constitution du dossier d'enregistrement correspondant,

- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RC 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).

Il est à noter que l'AE peut déléguer tout ou partie de ses fonctions à des unités de proximité désignées sous le nom d'autorités d'enregistrement déléguées (AED).

Dans ce cas, l'AE s'assure que les demandes sont complètes et exactes et, effectuées par un MC dûment autorisé. Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE (cf. chapitre 5.5).

1.4.3 Responsables de certificats

Dans le cadre de la présente PC, un RC est une personne physique qui est responsable de l'utilisationdu certificat de signature de jetons d'horodatage 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 RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.
Le RC 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 RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC 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 RC de ses fonctions et lui désigner un successeur. Une AC doit révoquer un certificat de signature de jetons d'horodatage pour lequel il n'y a plus de RC explicitement identifié.

1.4.4 Porteurs de certificats

Dans le cadre de la présente PC, le porteur est le serveur informatique tiers utilisé pour la signature des jetons émis par l'Autorité d'Horodatage.

1.4.5 Utilisateurs de certificats

L'utilisateur des présents certificats de signature de jetons d'horodatage est le serveur identifiécomme Porteur de certificats, ainsi que l'ensemble des personnes physiques (ou éléments d'infrastructure) dont le rôle est de vérifier la signature de jetons d'horodatage.

1.4.6 Autres participants

1.4.6.1 Composante de l'IGC

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

1.5 5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

L'AC « Chaabi eSign - SealsTS CA » délivre des certificats de signature des jetons d'horodatage.

1.5.1.1 Bi-clés et certificats des serveurs

Les certificats du profil « Signature de jetons d'horodatage » permettent à un service de signature de jetons d'horodatage tiers de signer les jetons émis par l'Autorité d'Horodatage de GBP.
Le service de signature de jetons d'horodatage tiers ne peut utiliser les certificats de signature de jetons d'horodatage uniquement pour signer les jetons d'horodatage émis par l'Autorité d'Horodatagede GBP.

1.5.1.2 Bi-clés et certificats d'AC et de ses composants

La clé privée de l'Autorité de Certification Chaabi eSign - SealsTS CA n'est utiliséeque dans les cas suivants :

- signature des certificats émis par l'Autorité de Certification Chaabi eSign - SealsTS, dont les certificats permettant la signature de jetons d'horodatage ;
- signature de la Liste des Certificats Révoqués (LCR) émise par l'Autorité de Certification – Chaabi eSign – SealsTS CA

1.5.2 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.

1.6 6 Gestion de la PC

1.6.1 Entité gérant la PC

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

1.6.2 Point de contact

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

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

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

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

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

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

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

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

21 1 Entités chargée de la mise à disposition des informations

L'AC est responsable de la mise à disposition des informations devant être publiées.
Ces informations sont publiées sur internet sur le site web de GBP par la direction de l'organisation pour la PC et le certificat d'AC.
La liste des certificats révoqués (LCR) est publiée automatiquement par la plate-forme IGC.

22 2 Information devant être publiées

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

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

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

2.2.1 Publication de la Politique de Certification

La présente PC est accessible à partir des URL suivantes :

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

2.2.2 Publication du certificat de l'Autorité de Certification

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

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

2.2.3 Publication de la liste des certificats/autorités révoqués

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

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

2.3 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 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 1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X.509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN).

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,

}

L'identité du serveur peut-être la raison sociale de l'entité.

3.1.3 Pseudonymisation des serveurs

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

3.1.4 Règles d'interprétation des différentes formes de noms

Le contenu du DN du certificat s'appuie le FQDN du serveur informatique tiers porteur de certificats.

3.1.5 Unicités des noms

Le DN de chaque certificat permet d'identifier de façon unique le serveur correspondant au sein du domaine de l'AC. Le DN comporte, entre autres, l'adresse email permettant d'assurer l'exigence d'unicité.
De plus, l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC.

3.1.6 Identification, authentification et rôle des marques déposées

Les marques et noms d'organisations présentent au sein des certificats des porteurs font l'objet d'un dépôt de marques auprès de l'OMPIC.

32 2 Validation initiale de l'identité

L'enregistrement d'un service de création de signature de jetons d'horodatage d'une entité auquel un certificat doit être délivré se fait via l'enregistrement du RC correspondant.
L'enregistrement d'un RC, et du serveur informatique correspondant se fait directement auprès del'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 RC pour un certificat de signature de jeton d'horodatage : validation par l'AE de l'identité "personne morale" de l'entité de rattachement du RC, de l'identité "personne

physique" du futur RC, de son habilitation à être RC pour le service de signature de jeton d'horodatage et pour l'entité considérée.
- Enregistrement d'un nouveau RC pour un certificat de signature de jetons d'horodatage déjà émis : validation par l'AE de l'identité "personne physique" du futur RC et de son habilitation à être RC pour le service de création de jetons d'horodatage considéré et pour l'entité considérée.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre 3.2.3.

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

3.2.2.1 Enregistrement d'un RC pour un certificat de signature de jetons d'horodatage à mettre

L'enregistrement du futur RC (personne physique) représentant une entité nécessite l'identification de cette entité et l'identification de la personne physique.
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 signature de jetons d'horodatage concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être RC pour le service de création de signature de jetons d'horodatage pour lequel le certificat de signature de jetons d'horodatage doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RC,
- une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du futur RC 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

L'authentification du RC se fait notamment :
- Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").
- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RC à l'aide du procédé de signature électronique et que la signature soit vérifiée et valide au moment de l'enregistrement.
- Soit par la communication d'un élément propre au futur RC permettant de l'identifier au sein d'une base de données administrative préétablie.

3.2.2.2 Enregistrement d'un nouveau RC pour un certificat de signature de jetons d'horodatage déjà émis

Dans le cas de changement d'un RC en cours de validité d'un certificat de signature de jetons d'horodatage, le nouveau RC est enregistré en tant que tel par l'AC en remplacement de l'ancien RC.
L'enregistrement du nouveau RC (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 signature de jetons d'horodatage est rattaché et en tant que RC pour ce service.
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 signature de jetons d'horodatage concerné par cette demande,
- un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être RC pour le service de création de signature de jetons d'horodatage pour lequel le certificat de signature de jetons d'horodatage doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RC,
- une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du futur RC 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

L'authentification du RC se fait notamment :

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

3.2.3 Informations non vérifiées du RC et/ou du serveur informatique

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

3.2.4 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 3 Identification et validation d'une demande de renouvellement des clés

Le renouvellement d'une bi-clé entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat de signature de jetons d'horodatage ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante

3.3.1 Identification et validation pour un renouvellement courant

Concernant le premier renouvellement, la vérification de l'identité du RC et des informations du serveur informatique correspondant est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé.
Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le RC et vérifiera les informations du serveur informatique selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

3.3.2 Identification et validation pour un renouvellement après révocation

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

3.4 4 Identification et validation d'une demande de révocation

Une demande de révocation doit être faite par mail signé envoyé à l'AE, ce dernier vérifie et valide l'identité du demandeur et le transmet au service de gestion des révocations.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 1 Demande de certificat

4.1.1 Origine d'une demande de certificat

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

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

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

- Le nom du service de création de signature de jetons d'horodatage à utiliser dans le certificat ;
- Les données personnelles d'identification du RC ;
- Les données d'identification de l'entité.

Le dossier de demande est établi soit directement par le futur RC à partir des éléments fournis par son entité, soit par son entité et signé par le futur RC.
Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le futur RC du certificat.

4.2 2 Traitement d'une demande de certificat

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

Une fois ces opérations effectuées, l'AE émet la demande transmise par le RC pour la génération de la Bi-clé et du certificat associé. L'AE conserve ensuite une trace des justificatifs présentés

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE informe le RC en mentionnant le motif du rejet.

4.2.3 Durée d'établissement du certificat

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

4.3 3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'Chaabi eSign - SealsTS CA déclenche les processus de génération et de préparation des différents éléments destinés au RC : la bi-clé et le certificat associé, son dispositif de création de signature de jetons d'horodatage, les codes d'activation, etc. (cf. chapitre 1.4.1).
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, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

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

Le certificat est transmis par message électronique à une adresse fournie par le RC. Le certificat complet et exact est mis à la disposition du RC.
NB – Si la remise du certificat doit se faire en main propre auprès de l'AE, le RC sera également tributaire des modalités d'accueil de l'AE.

4.4 4 Acceptation du certificate

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

Les certificats ne sont pas publiés après leur délivrance.

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.

4.5 5 Usage de la bi-clé et du certificat

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

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service de signature de jetons d'horodatage de données. (cf. chapitre 1.5.1.1). Les RC 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. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RC par l'AC avant d'entrer en relationcontractuelle.

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

Cf. chapitre précédent et chapitre 1.5.
Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 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 doit-elle s'en assurer auprès du RC, au minimum au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC.

4.6.1 Causes 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 RC de l'établissement du nouveau certificat

Sans objet

4.6.5 Processus d'acception du nouveau certificat

Sans objet

4.6.6 Démarche de 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 7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

4.7.1 Causes possibles de changement d'une Bi-clé

La délivrance d'un nouveau certificat peut résulter de l'expiration du certificat courant dans le cadre d'un renouvellement de bi-clé. Dans ce cas, le renouvellement ne peut avoir lieu que pendant la période de renouvellement du certificat associé à la bi-clé changée.
La délivrance d'un nouveau certificat peut également résulter d'une nouvelle demande suite à une révocation ou suite à un oubli de renouvellement (délivrance en dehors de la période de renouvellement).

4.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat de signature de jetons d'horodatage est à l'initiative du RC. 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

La procédure de demande d'un nouveau certificat est identique à la procédure de demande initiale.

4.7.4 Notification au RC 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

La publication du nouveau certificat se fera de la même façon qu'à l'enregistrement initial.

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

La notification se fera de la même façon qu'à l'enregistrement initial.

4.8 8 MODIFICATION DU CERTIFICAT

La modification d'un Certificat consistant à la modification d'informations du Certificat sans changement de la clé publique, et autres qu'uniquement la modification des dates de validité, n'estpas autorisée dans le cadre de la présente PC.

4.8.1 Causes possibles de modification d'un certificat

Sans object

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 RC de l'établissement du certificat modifie

Sans objet

4.8.5 Démarche d'acceptation du certificat modifie

Sans objet

4.8.6 Publication du certificat modifie

Sans objet

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

Sans objet

4.9 9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de signature de jeton d'horodatage

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat de signature de jetons d'horodatage :

- 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 RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le RC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;

- la clé privée du serveur est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées) ;
- le RC ou une entité autorisée (représentant légal de l'entité par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- l'arrêt définitif du serveur ou la cessation d'activité de l'entité du RC de rattachement du serveur.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.
Lorsque l'une des circonstances ci-dessus se réalise, le certificat concerné est révoqué et son numéro de série placé dans la Liste de Certificats Révoqués (LCR) tant que la date d'expiration du certificat n'est pas dépassé.
Toute demande de révocation doit être accompagnée d'une cause de révocation.

4.9.1.2 Certificats d'une composante de l'IGC

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

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de signature de jeton d'horodatage

Les personnes / entités qui peuvent demander la révocation d'un certificat de signature de jetons d'horodatage sont les suivantes :
- le RC pour le serveur considéré ;
- un représentant légal de l'entité ;
- L'AC émettrice du certificat ou l'une de ses composantes (AE).

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

4.9.2.2 Certificat d'une composante de l'IGC

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

La validation de l'identité et de l'autorité de la personne physique à l'origine de la demande sont vérifiées par l'AE. La révocation d'un certificat d'AC subordonnée émis par l'ACR peut être aussi déclenchée par l'entité responsable de l'ACR dans le cas de non-respect des exigences de l'IGC par cette AC subordonnée. L'entité responsable de l'AC subordonnée est ensuite prévenue dans les plus brefs délais de cette décision.

La révocation d'un certificat d'AC subordonnée nécessite une cérémonie des clés.

L'ACR vérifie l'origine et l'intégrité de la demande de révocation du certificat. Si la demande est correcte, L'AC met à jour le dossier du porteur dans sa propre base de données et ajoute le numéro de série du certificat à la Liste des Certificats Révoqués (CRL).

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat de signature de jeton d'horodatage

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.
L'AC précise dans sa PC comment la fonction de gestion des révocations est organisée et quels sont les points d'accès à cette fonction pour les demandeurs de révocation.
Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- 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,...) ;
- la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation doit être diffusée au minimum via une LCR. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC (cf. chapitre 4.9.9).
Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le RC n'est pas le demandeur, il doit également être informé de la révocation effective de ce certificat.

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

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

4.9.4 Délai accordé au RC pour formuler la demande de révocation

Dès que le RC (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 desrévocations 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 signature de jetons d'horodatage est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.
La méthode utilisée (LCR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité.

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): 0jours ;

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.

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

La mise en œuvre d'un service OCSP est appliquée. Il sera uniquement en usage interne.

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

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

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Les entités autorisées à effectuer une demande de révocation (cf. partie 4.9.2) sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

4.9.13 Causes possibles d'une suspension

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

4.9.14 Origine d'une demande de suspension

Sans objet

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet

4.9.16 Limites de la période de suspension d'un certificat

Sans objet

4.10 0Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats a pour but de permettre aux utilisateurs de vérifier le statut d'un certificat et de sa chaîne de certification, c'est à dire de vérifier également les signatures des certificats de la chaîne de certification et les signatures garantissant l'origine et l'intégrité des LCR.
La fonction d'information sur l'état des certificats un mécanisme de consultation libre de LCR. Ces LCR sont au format LCRv2, publiées électroniquement aux URL définies à la partie 2.2. Ces adresses figurent également dans le champ « Point de Distribution des LCR » de chaque certificat.

4.10.2 Disponibilité de la fonction

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

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) et une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

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

4.10.3 Dispositifs optionnels

Sans objet

4.11 1FIN DE LA RELATION ENTRE LE RC 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 signature de jetons d'horodatage pour lequel il n'y a plus de RC explicitement identifié.

4.12 2 SEQUESTRE DE CLE ET RECOUVREMENT

Ce document ne traite pas de chiffrement de données et interdit donc le séquestre des clés privées des serveurs.
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. MESURE DE SÉCURITÉ NON TECHNIQUES

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

Suite à une analyse de risque menée par 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 - SealsTS CA » respecte. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement de travail du GBP et des résultats de l'analyse de risque pour garantir un niveau de sécurité homogène.

5.1 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 que les résultats de l'analyse de risque réalisée. Les sites d'hébergement de l'IGC couvrent les risques inhérents aux tremblements de terre ou explosion.

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

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC « Chaabi eSign - SealsTS 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 (opéré par des groupes électrogènes) et de génération d'air conditionné sont mis en œuvre afin d'assurer la disponibilité et la continuité des services délivrés, en particulier le service de gestion des révocations et le service d'information sur l'état des certificats.

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

5.1.4 Vulnérabilité aux dégâts des eaux

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

De faux planchers ainsi que des détecteurs d'humidité sont mis en place dans les locaux de l'IGC afin de protéger la salle.

5.1.5 Prévention et protection incendie

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

Des détecteurs d'incendies ainsi que des systèmes d'extinction basée sur le gaz sont mis en place dans les locaux de l'IGC afin de prévenir les incendies et de protéger la sale.

5.1.6 Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Les supports (papier, disque dur, clé USB, CD, etc.) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.

5.1.7 Mise hors service des supports

En fin de vie, les supports seront détruits.
Les procédures et moyens de destruction sont conformes au niveau de confidentialité des informations correspondantes.

A l'occasion du comité de pilotage de l'IGC, des tests des clés des porteurs de secrets sont réalisés.
Une procédure est également appliquée pour la destruction du matériel obsolescent.

5.1.8 Sauvegarde hors site

En complément de sauvegardes sur site, les composantes de l'infrastructure de l'IGC mettent en œuvre des sauvegardes hors site de leurs applications et de leurs informations.

Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC après incident respectant les engagements de service tels que définis dans la présente PC.

Ces sauvegardes sont chiffrées afin de garantir la sécurité des données. Les informations sauvegardées sont redirigées vers le site de backup.

52 2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiances 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 desperformances 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 ;

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

5.2.2 Nombre de personnes requises par tâches

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

Toutes les opérations techniques sensibles nécessitent l'utilisation d'une carte d'administration du module cryptographique qui est délivré au moment de l'initialisation aux administrateurs de l'AC.

5.2.3 Identification et authentification pour chaque rôle

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

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

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

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Pour les rôles de confiance, les cumuls suivants sont 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.

53 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 autorisées ;
- Les exigences vis-à-vis du personnel des prestataires externes ;
- La documentation fournie au personnel.

5.3.1 Qualifications, compétences et habilitations requises

Toutes les personnes amenées à travailler sur les composantes de l'IGC sont soumises à une clause de secret professionnel 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 Procédures 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 remettent à leur employeur une copie du bulletin n°3 de leur casier judiciaire. Les personnes ayant un rôle de confiance ne souffrent pas de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

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

5.3.3 Exigences en matière de formation initiale

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

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

5.3.4 Exigences et fréquences en matière de formation continue

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

5.3.5 Fréquence et séquence de rotation entre différentes attributions

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

5.3.6 Sanctions en cas d'actions non autorisées

Des sanctions d'ordre légal ou disciplinaire sont applicables en cas d'abus de droit. 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 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 4 Procédures de constitution des données d'audit

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

5.4.1 Type d'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.
Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux. Ces mécanismes seront implémentés suite à la mise en production de l'IGC.

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

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

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

5.4.5 Procédure de sauvegarde des journaux d'événements

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

5.4.6 Système de collecte des journaux d'événements

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

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

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

5.4.8 Évaluation des vulnérabilités

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

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

Les journaux d'évènements sont analysés dans leur totalité au minimum 1 fois toutes les 2 semaines et dès la détection d'une anomalie.

Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre-elles (autorité d'enregistrement et fonction de génération, fonction des révocations et fonction d'information sur l'état des certificats, etc.) est effectué 1 fois par mois, ceci afin devérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

55 5 Archivage des données

5.5.1 Types de données à archiver

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

Il est également conservé des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configurations des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les CGU ;
- Les accords contractuels avec d'autres AC ;
- Les certificats, LCR ou réponses OCSP tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les engagements signés des MC ;
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- Les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat
Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire, et pendant au moins sept ans, pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

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

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

Lorsque des MC sont également dans un autre pays, alors il convient de prendre également en compte les exigences contractuelles et légales applicables à ces MC.
La durée de conservation des dossiers d'enregistrement est portée à la connaissance du porteur ou du MC.

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 ou le MC, 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 V.4 seront archivés pendant sept années après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offriront le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements sera assurée tout au long de leur cycle de vie.

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

5.5.3 Protection des archives

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

Pendant tout le temps de leur conservation, les archives sont :

- protégées en intégrité ;
- protégées contre la destruction ;
- protégées contre les accès illicites ;
- peuvent être relues et exploitées.

La DPC précise les moyens mis en œuvre.

5.5.4 Procédure de sauvegarde des archives

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

5.5.5 Exigences d'horodatage des données

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

5.5.6 Système de collecte des archives

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

5.5.7 Procédure de récupération et de vérification des archives

Les archives ne sont accessibles qu'aux entités en charge de la gestion de l'IGC. L'accès aux archives est contrôlé suivant le rôle demandant l'accès aux archives et le composant associé.

Le temps de récupération des archives est inférieur à deux jours ouvrés.

5.6 6 Changement de clés d'AC

Une AC ne peut pas générer des certificats pour les AC subordonnées ou les porteurs dont les dates de fin seraient postérieures à la date d'expiration du certificat de l'AC « Chaabi eSign - SealsTS CA ».

De ce fait, la période de validité du certificat de l'AC est supérieure à celle des certificats des AC subordonnées ou des porteurs.

Lorsqu'un nouveau certificat d'AC « Chaabi eSign - SealsTS CA » est émis, le certificat de l'AC « Chaabi eSign - SealsTS CA » précédent peut toujours être utilisé pour vérifier l'authenticité des certificats d'AC subordonnées ou des porteurs émis sous cet ancien certificat, et ce jusqu'à ce que ces certificats d'AC subordonnées ou des porteurs aient expiré.

5.7 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 - SealsTS 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 - SealsTS CA », l'information est publiée dans l'urgence dans l'annuaire interne et sur le site internet du recouvrement.

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

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

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

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

Dans les cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué : cf. chapitre 4.9.
En outre, l'AC respecte les engagements suivants :

- informer les entités suivantes de la compromission : tous les porteurs, 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 d'une fois tous les 3 ans.

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

En cas de transfert de l'activité à un tiers, 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. MESURES DE SÉCURITÉ TECHNIQUES

6.1 1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'AC sont générées lors d'une cérémonie des clés à l'aide d'une ressource cryptographique matérielle.

Les rôles des personnes impliquées dans les cérémonies de clés sont précisés dans la DPC.

Suite à leur génération, les parts de secrets (données d'activation) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même

porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets est mise en œuvre par son porteur.

6.1.1.2 Clés des serveurs générées pas l'AC

Les bi-clés sont générées en central par l'AC. Elles ne sont pas séquestrées par l'AC.

6.1.2 Transmission de la clé privée au serveur

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 de création de signature de jetons d'horodatage destiné au serveur, ou suivant un moyen équivalent.
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 clé publique à l'AC

Sans objet.

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

L'AC « Chaabi eSign - SealsTS » publie son certificat. Le certificat se situe danstout documents ou donnés horodatées, dans l'espace de publication mais aussi, éventuellement, dans les magasins de certificats des applications utilisatrices.

6.1.5 Tailles des clés

- 4096 bits pour la taille des clés de l'AC « Chaabi eSign - SealsTS CA » ;
- 3072 pour les certificats de signature d'horodatage ;

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.
Le gabarit associé aux certificats « Signature de jetons d'horodatage » est préconfiguré dans la console de configuration de l'IGC. Seul un nombre restreint de personnes identifiées sont habilitées à accéder à la console de configuration pour édition. De plus, toute modification effectuée sur le profil figure dans les rapports d'audit.

6.1.7 Objectifs d'usage de la clé

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

62 2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques (HSM), utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature sont certifiés Fips 140-2 niveau 3 et CC EAL4+

6.2.1.2 Dispositifs de création de jetons d'horodatage

Les dispositifs de création de signature de jetons d'horodatage 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 RC, elle doit s'assurer auprès du RC 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 RC, directement ou indirectement, elle doit s'assurer que :

- La préparation des dispositifs de création de signature de jetons d'horodatage est contrôlée de façon sécurisée ;
- les dispositifs de création de signature de jetons d'horodatage sont stockés et distribués de façon sécurisée ;
- les désactivations et réactivations des dispositifs de création de signature de jetons d'horodatage 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 serveurs

La méthode d'activation de la clé privée du serveur dépend du dispositif utilisé. L'activation de la clé privée du serveur doit au minimum être contrôlée via des données d'activation (cf. chapitre 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 sontaussi 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 de jeton d'horodatage dans un serveur, le certificat logiciel est complétement supprimé de ce serveur après sa révocation.

6.3 3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC « Chaabi eSign - SealsTS CA » sont archivées par archivagedes 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 serveur

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

6.4 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 RC, 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 quele RC 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 RC.
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 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 lesfonctions 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 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 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 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. PROFILS DES CERTIFICATS ET CRLS

7.1 1 Profil Certficat AC

Le tableau ci-dessous décrit les valeurs des attributs du Certificat de l'AC « Chaabi eSign - SealsTS 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 with RSA
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 - SealsTS CA
		O	Groupe Banques 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 **1.2.504.1.1.2.1.3.9.1**	
Identificateur de la clé de l'autorité		Empreinte SHA-1 de la clé publique de l'issuer	
Accès aux informations de l'autorité		1.3.6.1.5.5.7.48.2 http://www.gbp.ma/certificats/Chaabbi_eSign_Root_CA.cer	
Point de distribution CRL		http://crl.gbp.ma/crldp/chaabi_esign.crl	
Utilisation de clé	**oui**	Signature du certificat, Signature de la liste de révocation des certificats hors connexion, Signature de la liste de révocation des certificats	
Contrainte de base	**oui**	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=Aucun(e)	
Algorithme d'empreinte numérique		SHA-1	

7.2 Certificats de signature des jetons d'horodatage

Le tableau suivant renseigne les valeurs par défaut des attributs d'un Certificat de signature de jeton d'horodatage émis par l'AC Chaabi eSign - SealsTS
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 with RSA
Algorithme de hachage de la signature		SHA-512
Emetteur		CN= « Chaabi eSign - SealsTS CA »

		O= «Groupe Banques Populaires »C= MA	
Valide à partir de		Date de génération du certificat	
Valide jusqu'au		Date de génération +3ans	
subject		CN	FQDN du serveur
		O	«Groupe Banques Populaires »
		C	MA
		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 »
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= 1.2.504.1.1.2.1.3.9.1	
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/chaabi_eSign_SealsTS_CA.cer	
Point de distribution CRL		http://crl.gbp.ma/crldp/chaabi_eSign_SealsTS_CA.crl	
Utilisation de clé	**oui**	Signature numérique, Non répudiation	
Extended Key Usage	**oui**	Enregistrement des informations de date (1.3.6.1.5.5.7.3.8) « id-kp-timeStamping »	
Algorithme d'empreinte numérique		SHA-1	

7.3 Profil des listes de certificats révoqués

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

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

7.4 Profil OCSP

Il n'y a pas d'exigence spécifique. Le service doit être conforme au [RFC2560].

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 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.

82 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 ;
- respecter les règles de bonne conduite prévues dans le statut du personnel et le règlement intérieur de l'entité auditée (horaires de travail, etc.) ;
- veiller à ne pas perturber le bon fonctionnement de l'entité qu'ils auditent.
- refuser toute invitation ou cadeaux offerts par le personnel ou la Direction de l'entité auditée et ce à quelque titre que ce soit. Lorsqu'il s'agit d'invitation officielle, l'accord express de la hiérarchie est nécessaire.
- être attentifs aux réclamations des clients qui se seraient présentés à eux, en dehors des locaux de l'entité auditée et des horaires du travail. Ils doivent inviter ces clients à se présenter aux locaux des entités auditées aux heures de travail, pour que leurs réclamations soient recueillies en bonne et due forme. Ils doivent également procéder aux investigations nécessaires pour vérifier le bien-fondé de ces réclamations.

83 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 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 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 de 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 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 - SealsTS CA ».

Si des risques critiques sont constatés la demande de délivrance de certificat est refusée.
Selon les non-conformités observées, l'AC « Chaabi eSign - SealsTS CA » peut accepterla délivrance du certificat sous réserve de l'engagement de GBP à corriger les non-conformités dansle 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 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 CPM 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 CPM 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 CPM.

9. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1 1 Tarifs

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

9.2 2 Responsabilité financière

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

9.3 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 ladestruction 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 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 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 droitde 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 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 etposséder 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 7 Limites de garanties

Sans objet.

9.8 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 9 Indemnités

Sans objet.

9.10 0 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 1 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 2 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 3 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 4 Juridictions compétentes

Les éventuels litiges seront traités par le tribunal compétent.

9.15 5 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 6 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 7 Autres dispositions

Sans objet.