GOUVERNEMENT
DE LA RÉPUBLIQUE
DU BÉNIN

Politique de Certification de l'Autorité de Certification du Gouvernement du Bénin

(« CP de la GovCA du Bénin »)

12 mars 2020

Version 1.0 (Finale)

Ce document est destiné au public et peut être distribué gratuitement

PAGE DE SIGNATURE

_____ _____

Thierry AHOUASSOU

Government of Benin Certification Authority Policy Authority DATE

TABLE DES MATIERES

REGISTRE DES MODIFICATIONS

Version	Date	Auteur(s)	Description
0.1 (Ébauche)	21 octobre 2019	Entrust Datacard M. Bouchard	Première ébauche soumise à l'examen par le GdB.
0.2 (Ébauche)	18 octobre 2019	Entrust Datacard M. Bouchard	Commentaires reçus du GdB le 4 novembre. Courriel de C. Mugisha. Ajout des articles du Code du Numérique du Gouvernement du Bénin. Document mis à jour sur la base de l'atelier du 4 au 8 novembre.
0.3 (Ébauche)	18 décembre 2019	Entrust Datacard M. Bouchard	Commentaires reçus du GdB le13 décembre. Courriel de C. Mugisha. Premiers commentaires reçus de la part d'EDC/Trustis.
0.4 (Ébauche)	20 décembre 2019	Entrust Datacard M. Bouchard	Commentaires reçus du GdB les 19 et 20 décembre. Courriel de C. Mugisha. Commentaires reçus d'EDC/Trustis.
0.5 (Ébauche)	14 janvier 2020	Entrust Datacard M. Bouchard	Commentaires reçus du GdB le 14 janvier. Courriel de C. Mugisha. Suppression des références à la Gov CA en cours d'organisation par l'EDC/Trustis.
0.6 (Ébauche)	12 février 2020	Entrust Datacard M. Bouchard	Ramener les références à la Gov CA en cours d'organisation par l'EDC/Trustis.
0.7 (Ébauche)	10 mars 2020	Entrust Datacard M. Bouchard	Les certificats de citoyenneté stockés sur les cartes NID peuvent avoir une durée de vie de 5 ans (approuvée par la Pa et l'OA du GdB). Commentaires reçus du GdB le 10 mars.
1.0 (Final)	12 mars 2020	Entrust Datacard M. Bouchard	Version finale acceptée par le GdB.

1. INTRODUCTION

1.1 APERÇU

La présente Politique de Certification (CP) s'applique au Gouvernement du Bénin, ci-après dénommé « Bénin », Autorité de Certification du Gouvernement (GovCA).

La GovCA du Bénin est subordonnée à la CA racine du Bénin. La GovCA du Bénin permet la délivrance de certificats X.509 aux abonnés tels que, mais sans s'y limiter, les citoyens du Bénin, les personnes morales, les résidents et les employés du Gouvernement du Bénin, les entrepreneurs, les applications et les dispositifs. La GovCA du Bénin peut également délivrer des certificats aux personnes qui exploitent la GovCA du Bénin.

La GovCA est soumise à la CP de la GovCA du Bénin et à la CP de la CA racine du Bénin et fait l'objet d'un audit de conformité à la CP de la GovCA du Bénin et à la CP de la CA racine du Bénin.

Les certificats de la GovCA du Bénin contiennent un identificateur d'objets enregistré de la CP (OID) qui peut être utilisé par une partie utilisatrice pour décider si un certificat est fiable dans un but particulier. L'OID correspond à un niveau d'assurance spécifique établi par la présente CP qui doit être disponible pour les parties utilisatrices. Chaque certificat délivré par la GovCA du Bénin fait valoir le niveau d'assurance approprié dans l'extension certificatePolicies.

La GovCA du Bénin est exploitée de manière à répondre aux exigences du niveau d'assurance élevé et est autorisée à délivrer des certificats d'assurance basique, moyenne et élevée à ses abonnés.

Toute utilisation ou référence à la présente CP de la GovCA du Bénin en dehors du champ de l'autorité politique de la GovCA du Bénin est entièrement au risque de la partie utilisatrice.

La GovCA du Bénin est mise en œuvre à l'appui de :

- LOI N°2017 -20 DU 20 AVRIL portant code du numérique en République du Bénin, ci-dessous référencé « Bénin Code du Numérique » ;
- DECRET N° 2018 - 530 DU 14 NOVEMBRE 2018 portant cadre institutionnel de gouvernance du système national d'Infrastructure à Clé Publique ;
- DECRET N°2018 -529 du 14 Novembre 2018 portant approbation des statuts de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ; et
- La politique de certification de la CA racine du Bénin V1.0 (Final).

La présente CP est basé sur les recommandations de l'Internet Engineering Task Force for Public Key Infrastructure (RFC 3647).

1.2 IDENTIFICATION

Ce document est connu sous le nom de Politique de Certification de l'Autorité de Certification du Gouvernement du Bénin (Benin GovCA CP).

La CP de la GovCA du Bénin est attribuée à l'OID suivant : `2.16.204.1.2.1.1`

Il existe trois politiques spécifiées à trois niveaux d'assurance différents dans la présente CP qui sont définies dans les sections suivantes. À chaque niveau d'assurance est attribué au moins un OID de la politique, à faire valoir dans les certificats délivrés par la GovCA du Bénin. Les OID des politiques de la GovCA du Bénin sont enregistrés dans le registre des objets de l'Organisation internationale de normalisation (ISO) de l'Union internationale des télécommunications (ITU) comme suit :

Tableau 1 – Niveaux d'assurance

Niveau d'Assurance	OID de la Politique
Assurance élevée	`2.16.204.1.2.1.1.1` (réservée aux cartes d'identité nationales) `2.16.204.1.2.1.1.4` (Utilisée par tous les autres types de certificats d'assurance élevée)
Assurance Moyenne	`2.16.204.1.2.1.1.2` (réservée aux identités virtuelles) `2.16.204.1.2.1.1.3` (réservée aux identités de mobile) `2.16.204.1.2.1.1.5` (Utilisée par tous les autres types de certificats d'assurance moyenne)
Assurance basique	`2.16.204.1.2.1.1.6` (Utilisée par tous les types de certificats d'assurance basique)

1.3 PARTICIPANTS DE LA PKI

1.3.1 Autorité Nationale de la Politique de Certification du Bénin

L'Autorité Nationale de Politique de Certification (NCPA) du Gouvernement du Bénin doit se charger de :

- Fournir une orientation stratégique pour le développement et l'utilisation du PKI nationale du Bénin et des systèmes de certification numérique ; et
- Approuver les politiques, normes et procédures du PKI.

Le rôle de la NCPA est confié au Conseil National de Sécurité du Numérique (CNSN) du Gouvernement du Bénin.

1.3.2 Autorité de la Politique du GovCA du Bénin

L'Autorité de la Politique du Gouvernement du Bénin (PA de la GovCA du Bénin) doit être un employé ou un groupe d'employés de l'Agence des Services et Systèmes d'Information (ASSI) du Gouvernement du Bénin.

La PA de la GovCA du Bénin doit se charger de :

- Assurer la conformité continue de la GovCA avec la CP de la GovCA du Bénin ;
- Développer, vérifier, approuver et maintenir la CP de la GovCA du Bénin ;

- Examiner et approuver le CPS de la GovCA du Bénin ;
- Examiner et approuver tout rapport d'audit pour la GovCA qui délivre des certificats dans le cadre de la CP de la GovCA du Bénin ;
- Examiner et approuver le CPS de la LRA partenaire ;
- Une fois que la GovCA du Bénin est autorisée à interopérer en utilisant la CA racine du Bénin, assurer la conformité continue de cette GovCA avec les exigences applicables comme condition pour permettre l'interopérabilité continue en utilisant la CA racine du Bénin.

La PA de la GovCA du Bénin doit signer un protocole d'accord (MOA) avec la PA de la CA racine du Bénin qui définit les responsabilités et les obligations respectives des deux parties et les correspondances entre les niveaux de certification contenus dans la CP de la CA racine du Bénin et ceux de la CP de la GovCA.

1.3.3 Autorité d'exploitation de la GovCA du Bénin

L'Autorité d'Exploitation de la GovCA du Bénin (OA de la GovCA du Bénin) doit être un employé ou un groupe d'employés de l'ANSSI du Gouvernement du Bénin ou une organisation agréée par la PA de la GovCA du Bénin pour gérer la GovCA du Bénin pour le compte du Gouvernement du Bénin. L'OA est chargée de l'exploitation des serveurs de la GovCA du Bénin et des systèmes connexes de la GovCA du Bénin. L'OA doit se charger de :

- Élaborer et soumettre le CPS de la GovCA à l'examen et à l'approbation de la PA de la GovCA du Bénin ;
- Tous les équipements et logiciels nécessaires au fonctionnement de la GovCA du Bénin ainsi que de la tenue d'un inventaire des biens matériels ;
- S'assurer que les CA, les Répertoires, le Serveur de Statut de Certificat (CSS), les Systèmes d'Enregistrement et les autres composantes de la GovCA du Bénin sont opérationnels conformément à la CP et au CPS de la GovCA ; et
- Mettre en œuvre l'interopérabilité entre la CA racine du Bénin et la GovCA du Bénin après approbation par la PA de la CA racine du Bénin et la PA de la GovCA du Bénin.

Note : La GovCA du Bénin sera initialement déployée et hébergée par Entrust Datacard (EDC) pour le compte du Gouvernement du Bénin. Au cours de cette phase, l'EDC se verra confier le rôle de l'OA de la GovCA du Bénin. Ce rôle sera transféré de l'EDC à l'ANSSI lorsque la GovCA du Bénin sera physiquement transférée de l'environnement de l'EDC au Centre National de Données du Gouvernement du Bénin.

1.3.4 Autorité d'Enregistrement de la GovCA du Bénin

L'Autorité d'Enregistrement de la GovCA du Bénin (RA de la GovCA du Bénin) doit être un employé ou un groupe d'employés de l'ASSI du Gouvernement du Bénin ou un organisme agréé par la PA de la GovCA du Bénin pour exploiter les services d'enregistrement de la GovCA du Bénin pour le compte du Gouvernement du Bénin. La RA de la GovCA du Bénin recueille et vérifie l'identité et les informations de chaque abonné pour les inclure dans le certificat de clé

publique de l'abonné délivré par la GovCA du Bénin. Les exigences applicables aux RA de la GovCA du Bénin sont énoncées dans d'autres parties du présent document.

Plus précisément, la RA de la GovCA doit se charger de :

- Effectuer une vérification en personne de l'identité des demandeurs de certificat ;
- Gérer les certificats d'abonné (c'est-à-dire émettre, renouveler ou révoquer les certificats) ;
- Gérer les LRA et veiller au respect de leur RPS ; et
- Aider les LRA tout en développant leur RPS.

La RA de la GovCA du Bénin peut déléguer certaines de ses responsabilités aux Autorités Locales d'Enregistrement (LRA partenaires) et aux Agents de Confiance (Benin GovCA-TA). Les LRA partenaires doivent élaborer des Déclarations de Pratiques d'Enregistrement (RPS) qui définiront clairement les types de certificats à délivrer, les formes de noms acceptables et la manière dont la LRA doit traiter les demandes de certificats, la vérification de l'identité des demandeurs et les opérations de gestion des certificats telles que la délivrance, la révocation, la modification et le renouvellement. Les RPS élaborées par les LRA partenaires doivent être examinées par la RA de la GovCA du Bénin et approuvées par la PA de la GovCA du Bénin avant que la LRA partenaire ne soit autorisée à délivrer et à gérer les certificats d'abonnés.

1.3.5 Autorité de la Politique de la CA Racine du Bénin

L'Autorité de la Politique de la CA racine du Bénin (Benin Root CA-PA) doit être un employé ou un groupe d'employés de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) du Gouvernement du Bénin.

La PA de la CA racine du Bénin doit se charger de :

- Assurer la conformité continue de chaque CA, y compris la GovCA qui délivre des certificats dans le cadre de la PA de la CA racine du Bénin et de la CP de la GovCA du Bénin avec les exigences applicables comme condition pour permettre la poursuite de la participation ;
- Développer, vérifier, approuver et maintenir la CP de la CA racine du Bénin ;
- Examiner et approuver le CPS de la CA racine du Bénin ;
- Examiner et approuver tout rapport d'audit pour les CA, y compris la GovCA, qui délivrent des certificats dans le cadre de la CP de la CA racine du Bénin ;
- Examiner et approuver les demandes des CA partenaires, y compris les demandes de la GovCA, pour l'interopérabilité avec la CA racine du Bénin ;
- Déterminer les correspondances entre les certificats délivrés par les CA partenaires candidates et les niveaux d'assurance définis dans la CP de la GovCA du Bénin et la CP de la CA racine du Bénin (ce qui comprendra une évaluation objective et subjective du contenu des CP respectives et de tout autre fait jugé pertinent par la PA de la CA racine du Bénin) ; et

- Après qu'une CA partenaire (par exemple, la GovCA) ait été autorisée à interopérer en utilisant la CA racine du Bénin, assurer la conformité continue de cette CA partenaire avec les exigences applicables comme condition pour permettre l'interopérabilité continue en utilisant la CA racine du Bénin.

La PA de la CA racine du Bénin doit signer un protocole d'accord (MOA) avec chaque CA partenaire à certification croisée (par exemple la GovCA), qui définit les responsabilités et les obligations respectives des deux parties et les correspondances entre les niveaux d'assurance des certificats contenus dans la CP de la CA racine du Bénin et ceux de la CP de la CA partenaire.

1.3.6 Autorité D'exploitation de la CA Racine du Bénin

L'Autorité d'Exploitation de la CA racine du Bénin (OA de la CA racine du Bénin) doit être un employé ou un groupe d'employés de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) du Gouvernement du Bénin ou un organisme agréé par la PA de la GovCA du Bénin pour exploiter la CA racine du Bénin pour le compte du Gouvernement du Bénin. L'OA est chargée de l'exploitation des serveurs de la CA et des systèmes connexes de la CA racine du Bénin. L'OA doit se charger de :

- Développer et soumettre le CPS de la CA racine du Bénin à la PA de la CA racine du Bénin pour vérification et approbation ;
- Être responsable de tous les équipements et logiciels nécessaires au fonctionnement de la CA racine du Bénin, ainsi que de la tenue d'une liste d'inventaire des biens physiques ;
- S'assurer que les CA, les Répertoires, les Systèmes d'Enregistrement et les autres composantes de la CA racine du Bénin sont opérationnels conformément à la CP et au CPS de la CA racine du Bénin ; et
- Mettre en œuvre l'interopérabilité entre la CA racine du Bénin et les CA partenaires (par exemple, la GovCA) lorsqu'elle est approuvée par la PA de la CA racine du Bénin.

Note : La CA racine du Bénin sera initialement déployée et hébergée par l'EDC pour le compte du Gouvernement du Bénin. Au cours de cette phase, l'EDC se verra confier le rôle de la PA de la CA racine du Bénin. Ce rôle sera transféré de l'EDC à l'ANSSI lorsque la CA racine du Bénin sera physiquement transférée de l'environnement de l'EDC au Centre National de Données du Gouvernement du Bénin. Les certificats délivrés au personnel de l'EDC seront révoqués lorsque les rôles de confiance seront transférés à l'ANSSI.

1.3.7 Autorité d'Enregistrement de la CA Racine du Bénin

L'Autorité d'Enregistrement (RA) de la CA racine du Bénin recueille et vérifie l'identité et les informations de chaque abonné pour les inclure dans le certificat de clé publique de l'abonné délivré par la CA racine du Bénin. L'OA de la CA racine du Bénin agit en tant que RA pour la CA racine du Bénin et exerce sa fonction conformément à un CPS approuvé par la PA de la CA racine du Bénin. Les CA partenaires, comme la GovCA, désignent leurs propres RA.

Dans le contexte de la CA racine du Bénin, la RA de la CA racine ne délivre des certificats qu'aux Serveurs d'Etat des Certificats (CSS) et au Personnel du Rôle de Confiance.

1.3.8 Abonnés

Un abonné est une personne physique ou morale dont le nom figure comme sujet dans un certificat. Les abonnés affirment utiliser les clés et les certificats conformément à la CP de la GovCA du Bénin et à l'article 316 du Code du Numérique n° 2017-20 du Gouvernement du Bénin et notamment :

- L'exactitude des représentations dans la demande de certificat ;
- La protection de la clé privée ;
- Les restrictions de l'utilisation des clés privées et des certificats ; et
- La notification de compromission de la clé privée.

1.3.9 Point de Contact de la GovCA du Bénin

Le point de contact (POC) de la GovCA du Bénin sera un employé ou un groupe d'employés de l'OA de la GovCA ayant besoin d'établir une relation de confiance avec la CA Racine du Bénin. Le POC de la GovCA du Bénin est entièrement chargé de l'interaction avec la PA de la CA Racine du Bénin ou son représentant en ce qui concerne l'établissement d'une relation de confiance entre la GovCA et la CA Racine du Bénin, conformément au CP de la GovCA du Bénin et au CPS de la GovCA du Bénin.

1.3.10 LRA Partenaire

Une LRA partenaire est une organisation autorisée par la PA de la GovCA du Bénin à délivrer des certificats à sa communauté d'abonnés.

Une LRA partenaire peut être composée d'une ou plusieurs personnes ayant des privilèges d'administration auprès de la GovCA du Bénin permettant la délivrance, la révocation, le renouvellement et la modification des certificats d'abonnés. En option, une LRA partenaire peut héberger et exploiter ses propres applications administratives dans son environnement permettant la délivrance et la gestion des certificats.

La LRA partenaire recueille et vérifie l'identité et les informations de chaque abonné pour les inclure dans le certificat de clé publique de l'abonné délivré par la GovCA du Bénin.

Le personnel et les applications de la LRA partenaire exercent leurs fonctions conformément au RPS applicable approuvé par la PA de la GovCA du Bénin.

Les exigences applicables aux LRA partenaires sont énoncées ailleurs dans le présent document.

1.3.11 Point de Contact des LRA Partenaires

Le POC de la LRA partenaire est un employé ou un groupe d'employés d'une organisation LRA partenaire autorisée qui exploite un service de la LRA utilisé pour émettre et exploiter les certificats d'abonnés. Le POC de la LRA partenaire est entièrement responsable de l'interaction avec la PA de la GovCA du Bénin ou le représentant de son RA en ce qui concerne l'établissement d'une relation de confiance permettant la délivrance d'un ou plusieurs certificats de LRA au personnel de la LRA partenaire et les demandes conformément à la CP de la GovCA du Bénin et à la RPS de la LRA partenaire approuvée.

1.3.12 Autorités de Certification

1.3.12.1 CA Racine du Bénin

La CA Racine du Bénin est composée d'une CA auto-signée. La CA Racine du Bénin est autorisée à délivrer les types de certificats suivants :

- Certificats de CA subordonnée ;
- Certificats croisés ;
- Certificats de rôle de confiance de la CA racine aux administrateurs de la CA ; et
- Certificats de serveur CSS, également appelés certificats OCSP.

Dans le cadre de la GovCA, la CA racine du Bénin est responsable de la délivrance des certificats de CA subordonnées à la GovCA.

1.3.12.2 GovCA du Gouvernement du Bénin

La GovCA du Gouvernement du Bénin est composée d'une ou plusieurs CA subordonnées. Une CA subordonnée n'a pas de certificat de CA auto-signé. Les CA subordonnées font signer leurs certificats par la CA racine du Bénin au cours de leur configuration.

1.3.13 Serveur de Statut des Certificats

La GovCA du Bénin comprendra une autorité qui fournira des informations sur le statut des certificats par le biais de transactions en ligne. En particulier, la GovCA du Bénin doit inclure des transpondeurs OCSP pour fournir des informations en ligne sur le statut des certificats. Une telle autorité est appelée Serveur d'Etat de Certificat (CSS). Lorsque le CSS est identifié dans les certificats comme une source faisant autorité pour les informations de révocation, les opérations de cette autorité sont considérées comme relevant du champ d'application de la présente CP. Les serveurs OCSP qui sont identifiés dans l'extension « Authority Information Access » (AIA) en sont des exemples.

1.3.14 Personnel de Rôle de Confiance

Le personnel de rôle de confiance relève de l'OA de la GovCA du Bénin et est chargé de déployer et d'exploiter l'infrastructure du GovCA du Bénin. Le Personnel de rôle de confiance de la GovCA du Bénin est responsable de l'exploitation de la PKI conformément à la CP et au CPS de la GovCA du Bénin.

Le personnel de rôle de confiance peut se voir délivrer des certificats par la GovCA du Bénin afin d'authentifier et d'effectuer les opérations de gestion de sa CA.

Note : La GovCA du Bénin sera initialement déployée et hébergée par l'EDC pour le compte du Gouvernement du Bénin. Au cours de cette phase, des Rôles de Confiance seront attribués au personnel de l'EDC. Ces rôles seront transférés de l'EDC à l'ANSSI lorsque la GovCA du Bénin sera physiquement transférée de l'environnement de l'EDC au Centre National de Données du Gouvernement du Bénin.

1.3.15 Parties Utilisatrices

Une partie utilisatrice est une entité qui vérifie la signature d'un certificat ou d'une demande de certificat en utilisant un chemin de certification de confiance.

1.3.16 Agent de Confiance

Entité autorisée à agir en tant que représentant de la RA de la GovCA du Bénin ou de la LRA partenaire pour confirmer l'identification de l'abonné pendant le processus d'enregistrement. Les agents de confiance n'ont pas d'interfaces automatisées avec la GovCA.

1.3.17 Agent de Conformité de la Sécurité de la GovCA du Bénin

Le rôle du Responsable de la Conformité de la Sécurité du GovCA du Bénin (GovCA-SCO) est d'être un employé ou un groupe d'employés de l'OA de la GovCA du Bénin ou d'une organisation approuvée par la PA de la GovCA du Bénin pour auditer et évaluer la GovCA du Bénin pour le compte du Gouvernement du Bénin.

Le SCO de la GovCA du Bénin est autorisé à consulter, mais pas à modifier, les journaux d'audit générés par le SCO de la GovCA du Bénin.

Les journaux d'audit doivent être vérifiés par le SCO de la GovCA du Bénin pour des événements tels que des échecs répétés, des demandes d'informations privilégiées, des tentatives d'accès aux fichiers du système et des réponses non authentifiées.

1.3.18 Auditeur de Conformité

Un auditeur de conformité doit être engagé par l'OA de la GovCA du Bénin, conformément à la PA de la GovCA du Bénin pour réaliser un audit de conformité sur les composantes et services de la GovCA du Bénin.

Un auditeur doit être engagé par les LRA partenaires pour effectuer un audit de conformité sur ses services de délivrance et de gestion des certificats d'abonnés.

1.3.19 Organe de Contrôle du Gouvernement du Bénin

L'Organe de Contrôle du Gouvernement du Bénin est chargé d'accomplir les tâches suivantes :

- Veiller à ce que les partenaires, y compris la GovCA du Bénin, se conforment à la CP de la CA racine du Bénin et au Code du numérique du Gouvernement du Bénin et mettent en œuvre les contrôles appropriés. Les évaluations effectuées par l'Organe de contrôle du Gouvernement du Bénin, ou par une organisation engagée par l'Organe de contrôle du Gouvernement du Bénin ont lieu avant et après que le partenaire soit autorisé à recevoir un certificat croisé ou un certificat de CA subordonnée par la CA racine du Bénin ;
- Évaluer les rapports d'audit de conformité produits par les partenaires (par exemple, la GovCA) ;
- Informer la communauté de la CA racine du Bénin, y compris les abonnés, les parties utilisatrices et les partenaires, qu'un incident de sécurité a affecté la CA racine du Bénin ou l'un de ses partenaires ;
- Attribuer le statut de Partenaire qualifié et retirer ce statut si nécessaire conformément aux dispositions de l'article 317 du Code du Numérique du Gouvernement du Bénin n° 2017-20 ;
- Informer les parties prenantes appropriées lorsque le statut de Partenaire qualifié est attribué ou retiré ;

- Évaluer les plans de reprise après sinistre et les plans de continuité des activités du Partenaire ; et
- Exiger des partenaires qu'ils mettent en œuvre des mesures correctives liées aux lacunes identifiées dans les rapports d'audit de conformité.

1.3.20 Autres Participants

La GovCA du Bénin peut avoir besoin des services d'autres autorités de sécurité, communautaires et d'application. Si nécessaire, le CPS de la GovCA du Bénin doit identifier les parties, définir les services et désigner les mécanismes utilisés pour soutenir ces services.

1.4 UTILISATION DES CERTIFICATS

1.4.1 Utilisations appropriées des certificats

GovCA du Bénin varie considérablement. Les parties utilisatrices doivent évaluer l'environnement, les menaces et vulnérabilités associées et déterminer le niveau de risque qu'elles sont prêtes à accepter en fonction de la sensibilité ou de l'importance des informations. Cette évaluation est effectuée par chaque partie utilisatrice pour son application et n'est pas contrôlée par la présente CP. Afin d'assurer une granularité suffisante, la présente CP précise les exigences de sécurité à trois niveaux qualitatifs croissants d'assurance : basique, moyen et élevé.

Le tableau suivant fournit une brève description des utilisations appropriées des certificats à chaque niveau d'assurance défini dans la présente CP ainsi que des caractéristiques de leur niveau d'assurance. Ces descriptions sont données à titre indicatif et ne sont pas contraignantes.

Tableau 2 – Utilisations des Certificats et caractéristiques des Niveaux d'assurance

Niveau d'Assurance	Utilisations appropriées des Certificats et caractéristiques du Niveau d'assurance
Assurance élevée	Ce niveau est réservé pour ces environnements où les menaces sur les données sont élevées ou les conséquences de la défaillance des services de sécurité sont importantes. Il peut s'agir de transactions de très grande valeur ou de niveaux élevés de risque de fraude. Le module cryptographique doit protéger les clés contre le clonage, la duplication et la falsification ainsi que contre les attaquants à fort potentiel. Le module cryptographique doit être protégé de manière fiable par la personne à laquelle il appartient contre l'utilisation par d'autres personnes. Les certificats chargés sur les cartes d'identité nationales (NID) affirmant une OID de la politique d'assurance élevée doivent répondre aux exigences minimales suivantes : • Ne peuvent être délivrés qu'à un abonné humain (c'est-à-dire qu'ils ne peuvent être délivrés à une application ou à un dispositif) ;

	• Une vérification en personne de l'identité auprès d'un bureau d'enregistrement est requise à la suite d'un processus de vérification de l'identité approuvé ; • Les clés sont générées sur la carte d'identité nationale et les clés privées de signature et d'authentification ne quittent jamais le module cryptographique de la carte d'identité nationale et la mémoire de clés ; et • Le module cryptographique de la d'identité nationale doit être certifié FIPS 140-2 niveau 3 ou supérieur. Les autres types de certificat affirmant une OID de la politique d'assurance élevée doivent répondre aux exigences minimales suivantes : • Ne peuvent être délivrés qu'à un abonné humain (c'est-à-dire qu'il ne peut être délivré à une application ou à un dispositif) ; • Une vérification en personne de l'identité auprès d'un bureau d'enregistrement ou d'un agent de confiance est requise ; • Les informations fournies par le demandeur doivent être vérifiées par le bureau d'enregistrement ou l'Agent de Confiance afin de s'assurer de leur légitimité ; • Le demandeur doit présenter au moins deux formulaires justificatifs d'identité approuvés au bureau d'enregistrement. Les formes acceptables de justificatifs d'identité peuvent être des pièces d'identité ou biométriques délivrées par le Gouvernement du Bénin, telles qu'une carte d'identité nationale, un passeport, une carte d'électeur et une carte d'identité de résident du Bénin ou d'autres documents administratifs approuvés par la PA de la GovCA du Bénin ou des cartes d'identité à photo délivrées par un Gouvernement étranger et approuvé par la PA de la GovCA du Bénin. • La signature d'un formulaire de contrat d'abonnement et d'un formulaire de vérification de l'identité d'abonné par le demandeur et le bureau d'enregistrement est requise ; • Les clés générées et stockées dans un module cryptographique matériel FIPS 140-2 de niveau 2 ou supérieur ou attestant d'une autre validation de sécurité par un tiers reconnu et approuvé par la PA de la GovCA du Bénin ; et • les clés de signature privées doivent être générées par les abonnés. La clé de signature privée ne peut pas être générée par un bureau d'enregistrement pour le compte d'un abonné.
Assurance Moyenne	Ce niveau est pertinent pour les environnements où les risques et les conséquences de la compromission des données sont modérés. Cela peut inclure des transactions ayant une valeur monétaire modérée ou un risque

	de fraude ou impliquant l'accès à des informations privées lorsque la probabilité d'un accès malveillant est modérée. Les types de certificats qui affirment une OID de la politique d'assurance moyenne doivent répondre à aux exigences minimales suivantes : • Les certificats peuvent être délivrés pour des personnes, des applications ou des dispositifs ; • Une vérification en personne de l'identité avec un bureau d'enregistrement ou un agent de confiance ou une vérification à distance de l'identité en utilisant des justificatifs d'identité approuvés par la PA de la GovCA du Bénin et la LRA partenaire ; • Les informations d'identification fournies par le demandeur sont vérifiées par le bureau d'enregistrement ou l'agent de confiance ou l'application de la RA. Les informations d'identification comprennent le numéro d'identification et le numéro de compte validés par des vérifications de dossiers soit avec les bases de données du ministère, de l'agence ou de l'institution concernés et confirment que : le nom, la date de naissance, l'adresse et d'autres informations personnelles dans les dossiers sont conformes à la demande et suffisantes pour identifier un individu unique. Les justificatifs d'identité acceptables comprennent, entre autres, le passeport, la carte d'électeur, la carte d'identité de résident du Bénin ou la carte d'identité nationale et les justificatifs d'authentification du Gouvernement du Bénin ou du réseau de partenaires ; • Il est facultatif de remplir un formulaire d'accord d'abonnement ou un formulaire de vérification de l'identité de l'abonné ; • Les clés d'abonné peuvent être générées et stockées dans un module cryptographique matériel ou logiciel FIPS 140-2 de niveau 1 ou supérieur ou dans une autre certification de sécurité approuvée par la GovCA du Bénin et la LRA partenaire ; et • les clés de signature privées peuvent être générées par un bureau d'enregistrement ou une application approuvée par la GovCA du Bénin pour le compte des abonnés ou elles peuvent être générées par les abonnés eux-mêmes.
Assurance basique	Ce niveau fournit un niveau d'assurance basique pertinent pour les environnements où il existe des risques et des conséquences de la compromission des données, mais qui ne sont pas considérés comme étant d'une importance majeure. Cela peut inclure l'accès à des informations privées lorsque la probabilité d'un accès malveillant n'est pas élevée. On suppose à ce niveau de sécurité que les utilisateurs ne sont pas susceptibles d'être malveillants. Les types de certificats qui affirment une OID de la politique d'assurance basique doivent répondre aux exigences minimales suivantes :

	• Les certificats peuvent être délivrés à des personnes, des applications ou des dispositifs ; • Une vérification en personne de l'identité avec un bureau d'enregistrement, un Agent de Confiance ou une vérification à distance de l'identité en utilisant des références approuvées par la PA de la GovCA du Bénin. • Les informations d'identification fournies par le demandeur doivent être vérifiées par le bureau d'enregistrement ou l'agent de confiance. les informations d'identification comprennent le numéro d'identification national et le numéro de compte validé par des vérifications de dossiers soit auprès des bases de données du ministère, de l'agence ou de l'institution concernés, et confirment que : le nom, la date de naissance, l'adresse et d'autres informations personnelles dans les dossiers sont conformes à la demande et suffisantes pour identifier un individu unique. Les justificatifs d'identité acceptables comprennent, sans s'y limiter, le passeport, la carte d'électeur, la carte d'identité de résident du Bénin ou la carte d'identité nationale et les justificatifs d'authentification du Gouvernement du Bénin ou du réseau de partenaires ; • Il n'est pas nécessaire de signer un formulaire d'accord d'abonnement ou un formulaire de vérification de l'identité de l'abonné ; • Il n'est pas nécessaire de générer et de stocker les clés d'abonné dans un module cryptographique certifié FIPS 140-2 ; et • Les clés de signature privées peuvent être générées par le bureau d'enregistrement pour le compte des abonnés ou par les abonnés eux-mêmes.

Les certificats délivrés par la GovCA du Bénin peuvent être utilisés aux fins suivantes :

- Authentification
- Signature numérique et non-répudiation
- Cryptage des données

Les documents du CPS de la GovCA du Bénin et de la RPS de la LRA partenaire doivent faire valoir les cas d'utilisation des certificats et les niveaux d'assurance soutenus.

Les politiques définies dans cette section sont conformes à l'article 278 du Code du Numérique du Gouvernement du Bénin.

1.4.2 Utilisations interdites de Certificats

La présente CP interdit toute utilisation des certificats de la GovCA du Bénin qui ne sont pas explicitement énumérés dans la section **Erreur ! Source du renvoi introuvable.**.

1.5 ADMINISTRATION DE LA POLITIQUE

1.5.1 Responsabilités de l'organisation Concernant la présente Politique de Certification

La PA de la GovCA du Bénin est responsable de tous les aspects de la présente CP.

1.5.2 Informations du Contact

Les questions relatives à la présente CP doivent être adressées à la PA de la GovCA du Bénin dont l'adresse est la suivante :

Agence des Services et Systèmes d'Information du Gouvernement du Bénin (ASSI)

Autorité de Certification du Gouvernement du Bénin- Autorité de Politique

Les cocotiers (Cotonou)

En face du Trésor Public

+229 21 30 78 50/65 73 87 87

info-assi@presidence.bj

www.assi.bj

1.5.3 Personne Déterminant L'adéquation du CPS à la Politique

La PA de la GovCA du Bénin doit approuver le CPS pour chaque CA qui délivre des certificats dans le cadre de la présente politique.

Le CPS de la GovCA du Bénin doit être conforme à la CP correspondant de la GovCA du Bénin. Il incombe à la PA de la GovCA du Bénin d'affirmer que le CPS de la GovCA du Bénin est conforme à la CP du de la GovCA du Bénin.

La PA de la GovCA du Bénin doit désigner la personne ou l'organisation qui affirme que les documents de la CP et du CPS de la GovCA du Bénin sont conformes à la CP de la CA du Bénin.

La détermination de la conformité est basée sur les résultats et les recommandations d'un auditeur de conformité. Voir la section **Erreur ! Source du renvoi introuvable.**pour plus de détails.

1.5.4 CPS Approval Procedure

L'OA de la GovCA du Bénin doit soumettre le CPS de la GovCA du Bénin et les résultats d'un audit de conformité de la PA de la GovCA du Bénin pour approbation. La PA de la GovCA du Bénin doit voter pour accepter ou rejeter le CPS. En cas de rejet, l'OA de la GovCA du Bénin doit résoudre les divergences identifiées et le soumet à nouveau à la PA de la GovCA du Bénin. La GovCA du Bénin est tenue de respecter toutes les facettes de la politique. La PA de la GovCA du Bénin ne délivrera pas de dérogations.

1.5.5 Procédure D'approbation du CPS

La PA de la GovCA du Bénin doit réviser la présente CP **au moins une fois par an**. La PA de la GovCA du Bénin peut modifier la présente CP ou une partie de celle-ci à tout moment et à sa

discrétion. Tous les changements de politique envisagés par la PA de la GovCA sont diffusés aux parties intéressées. Toutes les parties intéressées doivent faire part de leurs observations à la PA de la GovCA du Bénin selon les modalités prescrites par la PA de la GovCA du Bénin. La diffusion d'éventuelles modifications de la politique aux entités de la partie utilisatrice et de l'abonné final n'est pas de la responsabilité de la PA de la GovCA du Bénin. La PA de la GovCA du Bénin fera un effort raisonnable pour s'assurer que ces informations sont accessibles à ces communautés par les canaux de distribution normaux, y compris la publication de la version actualisée de la CP de la GovCA du Bénin sur sa page web publique.

2. RESPONSABILITÉS EN MATIÈRE DE PUBLICATION ET DE REPERTOIRE

2.1 REPERTOIRES

L'OA de la GovCA du Bénin doit exploiter des répertoires pour soutenir les opérations de la GovCA du Bénin.

L'OA de la GovCA du Bénin s'assurera que les répertoires sont compatibles avec le répertoire de la CA racine du Bénin.

2.1.1 Obligations de la GovCA du Bénin en matière de Répertoire

L'OA de la GovCA du Bénin peut utiliser divers mécanismes pour publier des informations dans un répertoire d'archives comme l'exige la présente CP. Ces mécanismes comprennent au minimum :

- Lightweight Directory Access Protocol (LDAP) system;
- Hyper Text Transport Protocol (HTTP) system;
- La disponibilité des informations, conformément aux dispositions de la présente CP relatives à l'affichage et à l'extraction d'informations sur les certificats, et
- des mécanismes de contrôle d'accès et de communication lorsque cela est nécessaire pour protéger les informations du répertoire comme décrit dans les sections suivantes.

2.2 PUBLICATION DES INFORMATIONS DE CERTIFICATION

Les politiques définies dans cette section sont conformes à l'article 323 du Code du Numérique N° 2017-20 du Gouvernement du Bénin.

2.2.1 Publication des Certificats et de L'état des Certificats

Les certificats des CA et des entités finales ne doivent contenir que des Identificateurs de Ressources Uniformes (URI) valides, accessibles aux parties utilisatrices.

La PA de la GovCA du Bénin doit publier tous les certificats de CA délivrés à la GovCA du Bénin et toutes les CLR délivrées par la GovCA du Bénin dans le répertoire de la GovCA du Bénin.

Les répertoires de la GovCA du Bénin doivent contenir au minimum tous les certificats de CA délivrés par ou à la GovCA du Bénin et les CLR délivrés par la GovCA du Bénin.

Pour la GovCA du Bénin, les mécanismes et les procédures doivent être conçus de manière à garantir que les certificats des CA et les CLR soient disponibles 24 heures sur 24, 7 jours sur 7, avec un minimum de 99 % de disponibilité globale par an et un temps d'arrêt programmé ne dépassant pas 0,5 % par an.

2.2.2 Publication des Informations de la CA

L'OA de la GovCA du Bénin doit publier les informations concernant la GovCA du Bénin nécessaires pour soutenir son utilisation et son fonctionnement. La CP de la GovCA du Bénin

doit être accessible au public sur la page web publique de la GovCA du Bénin (voir http://www.gouvca.bj).

2.2.3 Interoperabilité

Lorsque les certificats et les CLR sont publiés dans des répertoires, il est recommandé d'utiliser des schémas basés sur des normes pour les objets et les attributs des répertoires. Des informations détaillées sont disponibles dans le guide technique de l'OA de la GovCA.

2.3 FREQUENCE DE PUBLICATION

La présente CP et toute modification ultérieure doivent être rendues publiques **dans les cinq jours** suivant leur approbation.

2.4 CONTROLES D'ACCES AUX REPERTOIRES

L'OA de la GovCA du Bénin protège toute information du répertoire qui n'est pas destinée à être diffusée ou modifiée par le public. Les certificats et les informations sur le statut des certificats dans le répertoire de la GovCA du Bénin doivent être accessibles au public sur internet.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 NOMMAGE

3.1.1 Types de Noms

Tous les certificats délivrés par la GovCA CA doivent comporter un sujet DN non-NUL. Les certificats à tous les niveaux d'assurance peuvent inclure des formes de noms alternatifs. La présente CP ne restreint pas les types de noms qui peuvent être utilisés.

3.1.2 Nécessité que les Noms soient significatifs

Les noms utilisés dans les certificats délivrés par la GovCA du Bénin doivent identifier la personne ou l'objet auquel ils sont attribués.

Lorsque des DN sont utilisés, l'arbre d'information du répertoire doit refléter avec précision les structures organisationnelles.

Lorsque des DN sont utilisés, le nom commun doit respecter les exigences d'unicité de l'espace nom et ne doit pas être trompeur. Cela n'exclut pas l'utilisation de certificats pseudonymes tels que définis dans la section **Erreur ! Source du renvoi introuvable.**.

3.1.3 Anonymat ou Pseudonymat des Abonnés

La GovCA du Bénin ne délivre pas de certificats anonymes. Des certificats pseudonymes peuvent être délivrés par la GovCA du Bénin pour soutenir les opérations internes.

Les DN des certificats délivrés par la GovCA du Bénin peuvent contenir un pseudonyme (par exemple un grand nombre), à condition que les exigences d'unicité de l'espace nom soient respectées.

3.1.4 Règles d'Interprétation des Différentes Formes de Noms

La PA de la GovCA du Bénin est responsable de la résolution des conflits de noms pour les certificats délivrés par la GovCA du Bénin.

Les règles d'interprétation des formes de noms distinctifs sont spécifiées dans la norme X.501. Les règles d'interprétation des adresses électroniques sont spécifiées dans la RFC 2822.

3.1.5 Unicité des Noms

La GovCA du Bénin doit faire respecter l'unicité du nom.

La PA de la GovCA du Bénin est responsable de la garantie de l'unicité du nom dans les certificats délivrés par la GovCA du Bénin. La GovCA du Bénin, sa RA et les LRA partenaires doivent faire respecter l'unicité du nom dans l'espace X.500.

L'unicité du nom n'est pas violée lorsque plusieurs certificats sont délivrés à la même entité.

Le CPS de la GovCA du Bénin et le RPS de la LRA partenaire doivent identifier la méthode d'attribution des noms de sujets. Les arbres d'information du répertoire de la GovCA peuvent être dédiés à la GovCA ou partagés avec d'autres CA. Lorsque plusieurs CA partagent une seule arborescence d'informations d'annuaire, la PA de la GovCA du Bénin doit examiner et approuver la méthode d'attribution des noms de sujets.

3.1.6 Reconnaissance, Authentification et Rôle des Marques déposées

La PA de la GovCA du Bénin doit résoudre les collisions de noms ou les litiges concernant les certificats délivrés par la GovCA du Bénin qui sont portés à son attention. Conformément à la présente CP, la GovCA du Bénin n'utilisera pas sciemment des marques déposées dans les noms, à moins que le sujet n'ait les droits d'utiliser ce nom.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1 Méthode pour prouver la possession d'une Clé privée

Dans tous les cas où la partie nommée dans un certificat génère ses propres clés, cette partie est tenue de prouver la possession de la clé privée qui correspond à la clé publique dans la demande de certificat.

Pour les clés de signature, cela peut être fait par l'entité qui utilise sa clé privée pour signer une valeur et qui fournit cette valeur à la GovCA du Bénin. La GovCA du Bénin doit valider alors la signature en utilisant la clé publique de la partie. La PA de la GovCA du Bénin peut autoriser d'autres mécanismes au moins aussi sûrs que ceux cités ici.

Dans le cas où une clé est générée par la GovCA du Bénin ou un bureau d'enregistrement autorisé soit (1) directement sur le jeton matériel ou logiciel de la partie, soit (2) dans un générateur de clé qui transfère de manière bénigne la clé sur le jeton de la partie, alors la preuve de la possession n'est pas requise.

3.2.2 Authentification de l'identité de l'organisation

Les demandes de certificats de la GovCA du Bénin ou de certificats d'abonnés pour le compte d'une organisation de confiance doit inclure le nom de l'organisation, son adresse et la documentation de son existence telle que définie à l'article 306 du Code du Numérique du Gouvernement du Bénin N° 2017-20.

Les bureaux d'enregistrement autorisés doivent vérifier les informations, en plus de l'authenticité du représentant demandeur et de l'autorisation du représentant à agir pour le compte de l'organisation.

3.2.3 Authentification de L'identité des Personnes

3.2.3.1 Authentification des Abonnés Humains

Les procédures utilisées par les bureaux d'enregistrement autorisés pour délivrer des certificats à leur propre personnel et à leurs filiales peuvent être plus strictes que celles qui sont exposées ci-dessous. Lorsque c'est le cas, les procédures d'authentification du demandeur s'appliquent en plus des indications de la présente section.

Les bureaux d'enregistrement veillent à ce que les informations relatives à l'identité du demandeur soient vérifiées. L'identité doit être vérifiée **au plus tard 30 jours** avant la délivrance du certificat initial. Pour toutes les politiques, les bureaux d'enregistrement peuvent accepter l'authentification de l'identité d'un demandeur attestée et documentée par un agent de confiance pour soutenir la vérification de l'identité des demandeurs à distance.

3.2.3.1.1 Authentification du Demandeur D'un Certificat D'assurance basique

Le processus d'authentification et de vérification de l'identité pour une demande de certificat d'assurance basique doit répondre aux exigences minimales exprimées dans le Tableau 2.

Il incombe à la PA, l'OA et à la RA de la GovCA du Bénin de définir les politiques spécifiques à faire respecter ainsi que les procédures à utiliser dans le cadre du CPS de la GovCA du Bénin. Les LRA partenaires sont chargées de définir les politiques spécifiques à appliquer ainsi que les procédures à utiliser dans un RPS. Le CPS de la GovCA du Bénin doit être approuvé par la PA de la CA racine du Bénin avant que la GovCA du Bénin ne soit subordonnée à la CA racine du Bénin. Le CPS de la GovCA du Bénin et le RPS de la LRA partenaire doivent être approuvé par la PA de la GovCA du Bénin avant que les certificats d'assurance de basique puissent être délivrés par la GovCA du Bénin et par les LRA partenaires.

3.2.3.1.2 Authentification du Demandeur de Certificat D'assurance Moyenne

Le processus d'authentification et de vérification de l'identité pour une demande de certificat d'assurance moyenne doit répondre aux exigences minimales exprimées dans le Tableau 2.

La PA, l'OA et la RA de la GovCA du Bénin ont la responsabilité de définir les politiques spécifiques à faire respecter ainsi que les procédures à utiliser dans le cadre du CPS de la GovCA du Bénin. Les LRA partenaires sont chargées de définir les politiques spécifiques à faire respecter ainsi que les procédures à utiliser dans leurs RPS. Le CPS de la GovCA du Bénin et les RPS partenaires doivent être approuvés par la PA de la GovCA du Bénin avant que la GovCA du Bénin ne puisse délivrer des certificats d'assurance moyenne.

3.2.3.1.3 Authentification du demandeur de Certificat d'assurance élevée

Le processus d'authentification et de vérification de l'identité pour une demande de certificat d'assurance élevée doit répondre aux exigences minimales exprimées dans le Tableau 2.

La PA, l'OA et la RA de la GovCA du Bénin sont chargés de définir les politiques spécifiques à appliquer ainsi que les procédures à utiliser dans le cadre du CPS de la GovCA du Bénin. Les LRA partenaires sont chargées de définir les politiques spécifiques à faire respecter ainsi que les procédures à utiliser dans leurs RPS. Le CPS de la GovCA du Bénin et le RPS partenaire doivent être approuvés par la PA de la GovCA du Bénin avant la délivrance des certificats d'assurance élevée par la GovCA du Bénin.

3.2.3.2 Authentification des Abonnés Humains pour Les Certificats basés sur les Rôles

Il existe un sous-ensemble d'abonnés humains qui pourraient se voir délivrer des certificats basés sur le rôle. Ces certificats identifieront un rôle spécifique au nom duquel l'abonné est autorisé à agir plutôt que son nom et sont délivrés dans le but de soutenir des pratiques commerciales acceptées. Le certificat basé sur le rôle peut être utilisé dans des situations où la non-répudiation est souhaitée. Normalement, il sera délivré en plus d'un certificat d'abonné individuel. Un rôle spécifique peut être identifié dans les certificats délivrés à plusieurs abonnés, cependant, la paire de clés sera unique à chaque certificat individuel basé sur le rôle (c'est-à-dire qu'il peut y avoir quatre personnes portant un certificat délivré en tant que « Directeur des Systèmes d'Information » ; cependant, chacun des quatre certificats individuels portera des clés et des identifiants de certificats uniques). Les certificats basés sur le rôle ne doivent pas être partagés mais doivent être délivrés à des abonnés individuels et protégés de la même manière que les certificats individuels.

La RA de la GovCA du Bénin ou les LRA partenaires doivent enregistrer les informations identifiées à la section **Erreur ! Source du renvoi introuvable.** pour un sponsor associé au rôle avant de délivrer un certificat basé sur le rôle. Le sponsor doit détenir un certificat individuel en son nom propre délivré par la GovCA au même niveau d'assurance ou supérieur que le certificat basé sur le rôle.

Les procédures de délivrance des certificats basés sur le rôle doivent être conformes à toutes les autres dispositions de la présente CP (par exemple, génération de clés, protection des clés privées et obligations des abonnés).

Pour les certificats pseudonymes qui identifient les sujets par leurs rôles organisationnels, la CA doit valider que la personne détient ce rôle ou qu'elle a reçu l'autorisation de signer au nom du rôle.

3.2.3.3 Authentification des Abonnés Humains pour Les Certificats de Groupe

Normalement, un certificat est délivré à un seul abonné. Dans les cas où plusieurs entités agissent en une seule qualité et où la non-répudiation des transactions n'est pas souhaitée, un certificat peut être délivré qui correspond à une clé privée partagée par plusieurs abonnés. L'OA de la GovCA du Bénin et la RA de la GovCA du Bénin ou les LRA partenaires doivent enregistrer les informations identifiées dans la section **Erreur ! Source du renvoi introuvable.** pour un sponsor avant de délivrer un certificat de groupe.

En plus de l'authentification du sponsor, les procédures suivantes doivent être effectuées pour les membres du groupe :

- Le sponsor doit se charger du contrôle de la clé privée, y compris de la tenue d'une liste des abonnés qui ont accès à la clé privée et expliquer quel abonné avait le contrôle de la clé et à quel moment ;
- Le DN SubjectName ne doit pas impliquer que le sujet soit un individu unique, par exemple par l'inclusion d'une forme de nom humain ;
- La liste des personnes détenant la clé privée partagée doit être fournie à la CA concernée ou à son représentant désigné et conservée par eux ; et
- les procédures de délivrance de jetons destinés à être utilisés dans des applications à clé partagée doivent être conformes à toutes les autres dispositions de la présente CP (par exemple, la génération de clés, la protection des clés privées et les obligations des abonnés).

3.2.3.4 Authentification des Dispositifs

Certains dispositifs informatiques et de communication (routeurs, pare-feu, serveurs, etc.) seront nommés comme sujets de certificat. Dans ce cas, l'appareil doit avoir un détenteur de certificat désigné (DCH). Le DCH est une personne ou un groupe de personnes chargées de fournir les informations d'enregistrement suivantes :

- Identification du dispositif (par exemple, numéro de série) ou nom du service (par exemple, nom du DNS) ;
- Clés publiques de l'appareil ;
- Autorisations et attributs du dispositif (le cas échéant, à inclure dans le certificat) ; et

- Coordonnées permettant à l'OA de la GovCA du Bénin, à la RA de la GovCA du Bénin ou à la LRA partenaire de communiquer avec le DCH le cas échéant

Ces certificats ne doivent être délivrés qu'aux dispositifs placés sous le contrôle du DCH (c'est-à-dire qu'ils doivent être enregistrés et validés conformément à toutes les exigences de l'organisme qui les délivre, et doivent être revalidés avant d'être délivrés à nouveau). En cas de modification d'un DCH, le nouveau DCH doit examiner le statut de chaque dispositif sous son parrainage pour s'assurer qu'il est toujours autorisé à recevoir des certificats. Le CPS et le RPS de la LRA partenaire doivent décrire les procédures visant à garantir que la responsabilité en matière de certificats est maintenue.

Les informations d'enregistrement doivent être vérifiées à un niveau d'assurance correspondant au niveau d'assurance du certificat demandé. Les dispositifs ne peuvent pas recevoir de certificats d'assurance élevée, mais peuvent recevoir des certificats d'assurances basique et moyenne. Les informations d'enregistrement doivent être vérifiées en fonction du niveau d'assurance associé. Les méthodes acceptables pour effectuer cette authentification et cette vérification de l'intégrité comprennent, sans s'y limiter, les suivantes :

- Vérification des messages signés numériquement envoyés du DCH à l'aide de certificats d'assurance équivalente ou supérieure à celle qui est demandée ;
- Enregistrement en personne ou à distance sous la supervision du DCH, l'identité du DCH étant confirmée conformément aux exigences de la **Erreur ! Source du renvoi introuvable.** ; ou
- Enregistrement à distance avec confirmation de l'identité du dispositif par une application automatisée de la RA utilisant des justificatifs d'identité du dispositif (par exemple, justificatifs d'authentification du réseau) approuvés par la PA de la GovCA du Bénin.

3.2.4 Informations Non-Vérifiées sur L'abonné

Les informations qui ne sont pas vérifiées ne doivent pas figurer dans les certificats.

3.2.5 Validation D'autorité

Avant de délivrer des certificats de signature qui affirment l'autorité de l'organisation, l'OA de la GovCA du Bénin et la RA de la GovCA du Bénin ou la LRA partenaire doivent valider l'autorité de la personne à agir pour le compte de l'organisation. Pour les certificats pseudonymes qui identifient les sujets par leurs rôles organisationnels, la GovCA du Bénin doit valider que la personne détient ce rôle ou a reçu l'autorisation de signer pour le compte de ce rôle.

3.2.6 Critères D'interopérabilité

La PA de la GovCA du Bénin détermine les critères d'interopérabilité pour les CA opérant dans le cadre de la présente politique.

La CA de la GovCA du Bénin doit être conçue, mise en œuvre et exploitée de manière à maintenir l'interopérabilité avec la CA racine du Bénin.

3.3 IDENTIFICATION ET AUTHENTIFICATION POUR LES DEMANDES DE RESSAISIE DE CLES

3.3.1 Identification et Authentification pour les Opérations de Routine de Ressaisie de Clés

Les abonnés de la GovCA du Bénin doivent s'identifier aux fins de la ressaisie de clé, comme l'exige le tableau ci-dessous.

Tableau 3 – Identification et Authentification pour les Demandes de Ressaisie de Clés

Niveau d'Assurance	Exigences de Routine de la Ressaisie des Clés D'identité pour les Certificats de Signature, D'authentification et de Cryptage D'abonné
Basique	L'identité peut être établie en suivant les mêmes procédures que pour la délivrance du certificat initial. L'identité peut être établie en utilisant la clé de signature actuelle, à condition que la clé n'ait pas dépassé sa période de validité et que le certificat associé ne soit pas révoqué ou suspendu, L'identité doit être rétablie par la procédure d'enregistrement initial au moins une fois tous les **15 ans** à compter de l'enregistrement initial. La routine automatisée de ressaisie de la clé peut être effectuée en utilisant un protocole et une méthode d'authentification approuvés par la PA de la GovCA du Bénin et documentés dans le CPS de la GovCA du Bénin ou dans le CPS ou dans le RPS de la LRA partenaire.
Moyen	L'identité peut être établie en suivant les mêmes procédures que pour la délivrance du certificat initial. L'identité peut être établie par l'utilisation de la clé de signature actuelle tant que la clé n'a pas dépassé sa période de validité et que le certificat associé n'est pas révoqué ou suspendue, L'identité est rétablie par la procédure d'enregistrement initial au moins une fois tous les **9 ans** à compter de l'enregistrement initial. La routine automatisée de ressaisie de la clé peut être effectuée par l'utilisation d'un protocole et d'une méthode d'authentification approuvés par la PA de la GovCA du Bénin et documentés dans le CPS de la GovCA du Bénin ou dans les CPS de la LRA partenaire.
Élevé	L'identité peut être établie en suivant les mêmes procédures que pour la délivrance du certificat initial. L'identité peut être établie par l'utilisation de la clé de signature actuelle tant que la clé n'a pas dépassé sa période de validité et que le certificat associé n'est pas révoqué ou suspendue,

Niveau d'Assurance	Exigences de Routine de la Ressaisie des Clés D'identité pour les Certificats de Signature, D'authentification et de Cryptage D'abonné
	Pour les abonnés à carte d'identité nationale, l'identité doit être rétablie par le biais d'un processus d'enregistrement initial à chaque délivrance de la nouvelle carte d'identité nationale ou réémission de la carte d'identité nationale. Pour tous les autres abonnés d'assurance élevée, l'identité est rétablie par le biais d'une procédure d'enregistrement initial au moins une fois tous **les 3 ans** à compter de l'enregistrement initial. La routine automatisée de ressaisie de la clé peut être effectuée par l'utilisation d'un protocole et d'une méthode d'authentification approuvés par la PA de la GovCA du Bénin et documentés dans le CPS de la GovCA du Bénin ou dans les CPS de la LRA partenaire.

3.3.2 Identification et Authentification pour la Ressaisie de Clé après Révocation

Après qu'un certificat ait été révoqué autrement que lors d'une action de renouvellement ou de mise à jour, l'abonné est tenu de passer par le processus d'enregistrement initial décrit dans la section 3.2 pour obtenir un nouveau certificat. Cette procédure s'applique à tous les certificats délivrés par la GovCA du Bénin.

3.4 IDENTIFICATION ET AUTHENTIFICATION POUR LES DEMANDES DE REVOCATION

Les demandes de révocation et de suspension doivent être authentifiées. Les demandes de révocation d'un certificat peuvent être authentifiées en utilisant la clé privée associée de ce certificat, que la clé privée ait été compromise ou non. Si la clé privée n'est pas disponible pour signer une demande de révocation, l'abonné ou le demandeur autorisé peut soumettre une demande de révocation écrite (le courrier électronique est acceptable).

D'autres méthodes d'authentification peuvent être approuvées par la PA de la GovCA du Bénin et documentées par l'OA de la GovCA du Bénin ou son délégué la RA de la GovCA du Bénin dans le CPS ou par la LRA partenaire dans le RPS.

4. EXIGENCES OPÉRATIONNELLES DU CYCLE DE VIE DU CERTIFICAT

4.1 DEMANDE DE CERTIFICAT

Cette section précise les exigences relatives à la demande initiale de délivrance d'un certificat.

Le processus de demande de certificat doit fournir suffisamment d'informations pour :

- Établir l'autorisation du demandeur pour obtenir un certificat. (selon la section 3.2.3)
- Établir et enregistrer l'identité du demandeur. (selon la section 3.2.3)
- Obtenir la clé publique du demandeur et vérifier la possession par le demandeur de la clé privée pour chaque certificat requis. (selon la section **Erreur ! Source du renvoi introuvable.**)
- Vérifier toute information sur le rôle ou l'autorisation demandée pour l'inclure dans le certificat.

Ces étapes peuvent être effectuées dans l'ordre qui convient aux bureaux d'enregistrement et aux demandeurs, sans pour autant nuire à la sécurité, mais elles doivent toutes être accomplies avant la délivrance du certificat.

Les entités qui souhaitent agir en tant que LRA auprès de la GovCA du Bénin doivent remplir les conditions de demande telles que spécifiées à la section **Erreur ! Source du renvoi introuvable.**La PA de la GovCA du Bénin doit agir sur la demande et, après avoir décidé de délivrer un certificat et avoir conclu le protocole d'accord avec la LRA partenaire, devra autoriser l'OA de la GovCA du Bénin à délivrer un certificat de LRA à la LRA partenaire.

4.1.1 Soumission de la Demande de Certificat

4.1.1.1 Certificat de CA

La GovCA du Bénin ne délivre pas de certificat de CA.

Le POC de la GovCA du Bénin est chargé de la soumission des demandes de certificat de la CA subordonnée de la GovCA du Bénin à la CA racine du Bénin.

4.1.1.2 Certificat D'utilisateur

Une demande de certificat d'utilisateur (abonné) doit être soumise soit par le demandeur, soit par un bureau d'enregistrement ou un TA au nom du demandeur.

4.1.1.3 Certificat de Dispositif

Une demande de certificat de dispositif doit être présentée par le DCH du dispositif.

4.1.2 Processus D'inscription et Responsabilités

Toutes les communications entre les autorités de la PKI à l'appui du processus de demande et de délivrance du certificat doivent être authentifiées et protégées contre toute modification. Si les bases de données ou d'autres sources sont utilisées pour confirmer les attributs des abonnés, alors ces sources et les informations associées envoyées à une CA doivent exiger :

- Lorsque les informations sont obtenues par le biais d'une ou plusieurs sources d'information, une chaîne de contrôle vérifiable doit être mise en place ; et
- toutes les données reçues doivent être protégées et échangées en toute sécurité, de manière confidentielle et inviolable et protégées contre tout accès non autorisé.

Les communications peuvent être électroniques ou hors bande. Lorsque des communications électroniques sont utilisées, des mécanismes cryptographiques proportionnels à la puissance de la paire de clés publiques/privées doivent être utilisés. Les communications hors bande doivent protéger la confidentialité et l'intégrité des données.

4.2 TRAITEMENT DE DEMANDE DE CERTIFICAT

Les informations contenues dans les demandes de certificat doivent être vérifiées comme étant exactes avant la délivrance des certificats. Le CPS de la GovCA du Bénin et le RPS partenaire doivent préciser les procédures de vérification des informations contenues dans les demandes de certificat.

4.2.1 Exécution des Fonctions D'identification et D'authentification

L'identification et l'authentification d'abonné doivent répondre aux exigences spécifiées pour l'authentification d'abonné, comme indiqué aux sections **Erreur ! Source du renvoi introuvable.** et 3.3 de la présente CP.

Le CPS de la GovCA du Bénin et le RPS partenaire doivent identifier les composantes de la GovCA (par exemple, la CA ou la RA ou la LRA) qui sont responsables de l'authentification de l'identité de l'abonné dans chaque cas.

4.2.2 Approbation ou Rejet de Demandes de Certificat

Pour la GovCA du Bénin, l'OA de la GovCA du Bénin, la RA de la GovCA du Bénin ou ses délégués (par exemple, les LRA partenaires) peuvent approuver ou rejeter une demande de certificat.

En cas de rejet d'une demande de certificat, la PA de la CA racine du Bénin ou ses délégués, la GovCA du Bénin, la RA de la GovCA du Bénin ou la LRA partenaire doivent informer les abonnés du motif du rejet.

4.2.3 Délai de Traitement de Demandes de Certificat

Les demandes de certificat doivent être traitées et un certificat délivré **dans les 2 jours ouvrables** suivant la vérification d'identité.

4.3 DELIVRANCE DE CERTIFICAT

4.3.1 Actions de la CA pendant la Délivrance de Certificat

L'OA de la GovCA du Bénin, la RA de la GovCA du Bénin ou les LRA partenaires vérifient la source d'une demande de certificat avant sa délivrance. Les certificats de CA créés par la GovCA du Bénin doivent être vérifiés pour s'assurer que tous les champs et extensions sont correctement remplis.

À la réception de la demande de certificat, le bureau d'enregistrement devra :

- Vérifier l'identité du demandeur ;
- Vérifier l'autorité du demandeur et l'intégrité des informations contenues dans la demande de certificat ;
- Établir et signer un certificat si toutes les exigences relatives au certificat ont été satisfaites ; et
- Mettre le certificat à la disposition de l'abonné après avoir confirmé que celui-ci a formellement reconnu ses obligations telles que décrites dans la section **Erreur ! Source du renvoi introuvable.**.

La demande de certificat peut déjà contenir un certificat établi soit par la RA soit par l'abonné. Ce certificat ne doit pas être signé tant que toutes les vérifications et modifications éventuelles n'ont pas été effectuées à la satisfaction de la GovCA.

Toutes les informations relatives à l'autorisation et aux autres attributs reçus d'un demandeur doivent être vérifiées avant d'être incluses dans un certificat. La responsabilité de la vérification des données relatives aux abonnés potentiels doit être décrite dans le CPS de la GovCA et le RPS des LRA partenaires.

4.3.2 Notification à L'abonné par la CA de la Délivrance du Certificat

La GovCA doit informer l'abonné (ou tout autre sujet de certificat) de l'établissement d'un certificat et doit mettre le certificat à la disposition de l'abonné. Pour les certificats de dispositifs, la CA doit informer le DCH.

4.4 ACCEPTATION DE CERTIFICAT

Avant qu'un abonné ne puisse faire un usage effectif de sa clé privée, le bureau d'enregistrement de la GovCA du Bénin doit lui expliquer ses responsabilités telles que définies dans la section **Erreur ! Source du renvoi introuvable.**.

4.4.1 Conduite Constituant L'acceptation du Certificat

L'acceptation est l'action entreprise par un abonné qui déclenche ses devoirs et sa responsabilité potentielle suite à la délivrance d'un certificat. Il est de la responsabilité du bureau d'enregistrement, tout au long du processus de délivrance, de :

- Expliquer à l'abonné ses responsabilités ;
- Informer l'abonné de l'établissement d'un certificat et du contenu et de l'objet du certificat ; et
- Exiger que l'abonné indique qu'il accepte ses responsabilités.

Le processus d'acceptation du certificat est terminé lorsque l'abonné apporte le certificat dans son magasin de certificats local pour l'utiliser.

4.4.2 Publication du Certificat par la CA

Comme indiqué dans la section **Erreur ! Source du renvoi introuvable.**, tous les certificats de la CA doivent être publiés dans des répertoires.

La publication des certificats d'abonnés dans le répertoire X.500/LDAP doit être définie dans le CPS de la GovCA du Bénin et dans le RPS de la LRA partenaire.

4.4.3 Notification de la Délivrance de Certificat par la CA à d'autres Entités

Aucune disposition.

4.5 UTILISATION DE LA PAIRE DE CLES ET DU CERTIFICAT

4.5.1 Utilisation de la Clé privée et du Certificat D'abonné

Pour l'assurance élevée, moyenne et basique, les abonnés doivent protéger leurs clés privées de l'accès par d'autres parties.

Les restrictions du champ d'utilisation prévu pour une clé privée sont spécifiées par le biais d'extensions de certificat, y compris l'utilisation de la clé et les extensions d'utilisation étendue de la clé, dans le certificat associé.

4.5.2 Utilisation de la Clé publique et du Certificat par la Partie Utilisatrice

Les certificats émis par la GovCA du Bénin précisent les restrictions d'utilisation par le biais d'extensions de certificats critiques, y compris les contraintes basiques et les extensions d'utilisation de la clé. La GovCA du Bénin émet des CLR précisant le statut actuel de tous les certificats non expirés de la GovCA du Bénin (à l'exception des certificats de réponse OCSP qui incluent l'extension id-pkix-ocsp-nocheck). Le CLR doit contenir tous les certificats non expirés, mais révoqués. Il est recommandé aux parties utilisatrices de traiter et de respecter ces informations lorsqu'elles utilisent des certificats émis par la GovCA du Bénin dans une transaction.

4.6 RENOUVELLEMENT DE CERTIFICAT

Le renouvellement d'un certificat consiste à émettre un nouveau certificat avec une nouvelle période de validité et un nouveau numéro de série tout en conservant toutes les autres informations du certificat original, y compris la clé publique.

Après le renouvellement du certificat, l'ancien certificat peut être révoqué ou non, mais il ne doit pas faire l'objet d'une re-clé, d'un renouvellement ou d'une modification.

4.6.1 Circonstances de Renouvellement d'un Certificat

Les certificats d'abonnés émis dans le cadre de la présente politique ne doivent pas être renouvelés, sauf pendant la récupération de compromission de clé de la CA (voir 5.7.3). Dans ce cas, le certificat renouvelé expirera comme indiqué dans le certificat d'abonné original.

En outre, un certificat ne sera renouvelé que si la clé publique n'a pas atteint la fin de sa période de validité, si la clé privée associée n'a pas été compromise et si le nom et les attributs de l'abonné sont inchangés.

Les certificats de la CA et les certificats CSS peuvent être renouvelés tant que la durée de vie cumulée de la clé publique ne dépasse pas la durée de vie du certificat spécifiée dans la section **Erreur ! Source du renvoi introuvable.**.

La CA peut renouveler automatiquement les certificats lors de la récupération de la compromission de la clé.

4.6.2 Qui peut demander un Renouvellement ?

Pour la GovCA du Bénin, le POC de la GovCA peut demander le renouvellement du certificat de la CA subordonné de la GovCA à la CA Racine du Bénin.

L'OA de la GovCA du Bénin peut demander le renouvellement d'un certificat de rôle CSS.

4.6.3 Traitement des demandes de Renouvellement de Certificat

Pour la GovCA du Bénin, le renouvellement du certificat pour des raisons autres que la re-clé de la GovCA du Bénin doit être approuvé par la PA de la GovCA du Bénin.

4.6.4 Notification d'émission d'un Nouveau Certificat A L'abonné

La GovCA du Bénin informe l'abonné du renouvellement de son certificat et de son contenu.

4.6.5 Conduite constituant l'acceptation d'un Certificat de Renouvellement

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.6.6 Diffusion du Certificat de Renouvellement par La CA

4.6.7 Comme indiqué dans la section 2.2.1, tous les certificats de la CA doivent être diffusés dans les répertoires de la GovCA du Bénin. Notification d'émission de Certificats par la CA à d'autres entités

aucune disposition.

4.7 RE-CLE DE CERTIFICAT

La re-clé d'un certificat consiste à créer de nouveaux certificats avec une clé publique (et un numéro de série) différente tout en conservant le reste du contenu de l'ancien certificat qui décrit le sujet. Le nouveau certificat peut se voir attribuer une période de validité différente, des identificateurs de clé, spécifier un point de distribution CRL différent et/ou être signé avec une clé différente. La re-clé d'un certificat ne nécessite pas de modification du Nomdusujet et ne viole pas l'exigence d'unicité du nom.

Les abonnés de la GovCA du Bénin doivent s'identifier aux fins de la re-clé, conformément dans la section **Erreur ! Source du renvoi introuvable.**.

Après la re-clé d'un certificat, l'ancien certificat peut être révoqué ou non, mais ne doit pas être re-clé, renouvelé ou modifié.

4.7.1 Circonstances justifiant une Re-Clé de Certificat

Plus une clé est longtemps et souvent utilisée, plus elle est susceptible d'être perdue ou découverte. Il est donc important qu'un abonné obtienne périodiquement de nouvelles clés. La section 6.3.2 établit les périodes d'utilisation des clés privées tant pour les CA que pour les abonnés. Parmi les exemples de circonstances nécessitant une nouvelle clé de certificat, on peut citer : l'expiration, la perte ou la compromission, l'émission d'un nouveau jeton matériel et la défaillance du jeton matériel.

La GovCA du Bénin émettra de nouveaux certificats de LRA aux LRA-Partenaires lorsqu'une LRA-Partenaire actuellement reconnue a généré une nouvelle paire de clés et qu'un protocole d'accord valide et non expiré existe entre la PA de la GovCA du Bénin et la LRA-Partenaire.

4.7.2 Qui peut demander la Certification d'une nouvelle Clé publique ?

Les demandes de re-clé ne sont acceptées que de la part du sujet ou du DCH du certificat. En outre, l'OA de la GovCA, la RA de la GovCA du Bénin et les LRA-Partenaires peuvent initier la re-clé des certificats d'un abonné sans demande correspondante.

4.7.3 Traitement des demandes de Re-Clé de Certificats

Voir les sections **Erreur ! Source du renvoi introuvable.** et 3.3.

La période de validité associée au nouveau certificat d'une LRA émis à une LRA-Partenaire ne doit pas dépasser la période du protocole d'accord.

4.7.4 Notification de l'émission d'un Nouveau Certificat à l'abonné

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.7.5 Conduite constituant l'acceptation d'un Certificat Re-Clé

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.7.6 Diffusion du Certificat Re-Clé par la CA

Comme indiqué dans la section 2.2.1, tous les certificats de CA doivent être diffusés dans les répertoires de la GovCA du Bénin.

Aucune disposition concernant la diffusion des certificats d'abonnés n'est mentionnée dans la présente politique.

4.7.7 Notification d'émission de Certificats par la CA à d'autres Entités

Aucune disposition.

4.8 MODIFICATION DU CERTIFICAT

La modification d'un certificat consiste à créer de nouveaux certificats avec des informations du sujet (par exemple un nom ou une adresse électronique) qui diffèrent de l'ancien certificat. Par exemple, une CA peut effectuer une modification de certificat pour un abonné dont les caractéristiques ont changé (par exemple, en raison d'un mariage ou d'un divorce). Le nouveau certificat peut avoir une clé publique de sujet identique ou différente.

Après la modification du certificat, l'ancien certificat peut ou non être révoqué, mais il ne doit pas être re-clé, renouvelé ou modifié.

4.8.1 Circonstances de la Modification d'un Certificat

La GovCA peut modifier son certificat CA ou CSS dont les caractéristiques ont changé (par exemple, affirmer une nouvelle politique d'OID). Le nouveau certificat peut avoir une clé publique de sujet identique ou différente.

La GovCA peut effectuer une modification de certificat pour un abonné dont les caractéristiques ont changé (par exemple, changement de nom en raison d'un mariage). Le nouveau certificat devra avoir une clé publique différente.

4.8.2 Qui peut demander la Modification d'un Certificat ?

Les demandes de certification d'une nouvelle clé publique sont examinées comme suit :

Les abonnés disposant d'un certificat en cours de validité peuvent demander la modification du certificat. La GovCA et les bureaux d'enregistrement peuvent demander la modification du certificat au nom d'un abonné. Pour les certificats d'appareils, le DCH de l'appareil peut demander la modification du certificat.

4.8.3 Traitement des demandes de Modification de Certificat

La preuve de tous les changements d'informations sur le sujet doit être fournie aux bureaux d'enregistrement de la GovCA du Bénin et vérifiée avant l'émission du certificat modifié.

Si le nom d'une personne change (par exemple en raison d'un mariage), la preuve du changement de nom doit être fournie aux services d'enregistrement de la GovCA du Bénin afin qu'un certificat portant le nouveau nom puisse être émis. Si les autorisations ou les privilèges d'une personne changent, le bureau d'enregistrement vérifiera ces autorisations. Si les autorisations ont été réduites, l'ancien certificat doit être révoqué.

La preuve de tous les changements d'informations sur le sujet doit être fournie aux bureaux d'enregistrement et vérifiée conformément au processus initial de vérification de l'identité tel que décrit dans la section 3.2 avant que le certificat modifié ne soit émis.

La vérification de l'identité d'une demande de modification de certificat doit être effectuée selon l'un des processus suivants :

- Processus initial de vérification de l'identité tel que décrit dans la section 3.2 ; ou
- Vérification de l'identité pour le renouvellement des clés telle que décrite dans la section 3.3.

La période de validité associée au certificat modifié de la LRA émis à une LRA-Partenaire ne doit pas dépasser la période du protocole d'accord.

4.8.4 Notification de l'émission d'un Nouveau Certificat A L'abonné

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.8.5 Conduite constituant l'acceptation du Certificat modifié

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.8.6 Diffusion du Certificat modifié par La CA

Tous les certificats des CA doivent être diffusés comme indiqué dans la section **Erreur ! Source du renvoi introuvable.**.

Aucune disposition concernant la diffusion des certificats d'abonnés n'est mentionnée dans cette politique.

4.8.7 Notification d'émission de Certificats par La CA à d'autres Entités

Aucune disposition.

4.9 RÉVOCATION ET SUSPENSION DU CERTIFICAT

La GovCA doit émettre des CRL couvrant tous les certificats non expirés émis dans le cadre de cette politique, à l'exception des certificats de réponse OCSP qui incluent l'extension id-pkix-ocsp-nocheck.

La GovCA doit rendre publique une description de la manière d'obtenir des informations de révocation pour les certificats qu'elle publie, et une explication des conséquences liées à l'utilisation des informations de révocation à une date donnée. Ces informations doivent être communiquées aux abonnés lors de la demande ou de I'émission des certificats, et elles doivent être facilement accessibles à toute partie utilisatrice potentielle.

Les demandes de révocation doivent être authentifiées. Les demandes de révocation d'un certificat peuvent être authentifiées en utilisant la clé privée associée audit certificat, que la clé privée ait été compromise ou non.

L'utilisation de mesures de suspension pour les certificats d'abonnés est autorisée.

4.9.1 Circonstances de Révocation

Un certificat est révoqué lorsque la liaison entre le sujet et la clé publique du sujet définie dans un certificat n'est plus considérée comme valable.

Voici des exemples de circonstances qui invalident le lien :

- Les informations d'identification ou les éléments d'affiliation de tout nom figurant dans le certificat deviennent invalides ;
- Les attributs de privilège figurant dans le certificat de l'abonné sont réduits ;
- Il peut être démontré que l'abonné a violé les dispositions de son contrat d'abonnement ;
- Il y a des raisons de croire que la clé privée a été compromise ;
- La certification de l'objet n'est plus dans l'intérêt de la CA ; et
- l'abonné ou une autre partie autorisée (telle que définie dans le CPS ou le RPS) demande la révocation de son certificat.

Lorsque l'une des circonstances susmentionnées se produit, le certificat associé est révoqué et placé sur la CRL. Les certificats révoqués doivent figurer sur toutes les nouvelles publications de CRL jusqu'à l'expiration des certificats.

4.9.2 Qui peut demander la Révocation d'un Certificat ?

Au sein de la PKI de la GovCA, une CA peut révoquer sommairement les certificats de son domaine. Une notification écrite et une brève explication de la révocation sont ensuite fournies à l'abonné. Le registraire peut demander la révocation du certificat d'un abonné au nom de toute partie autorisée, comme spécifié dans le CPS de la GovCA ou le RPS de la LRA partenaire de la GovCA. Un abonné peut demander que son propre certificat soit révoqué. Un DCH peut demander la révocation d'un certificat relevant de son autorité. D'autres registraires autorisés peuvent demander la révocation d'un certificat d'abonné dans son domaine, comme indiqué dans le CPS ou le RPS d'une LRA partenaire.

Un certificat de la LRA partenaire peut être révoqué sur instruction de la PA, de la RA ou de l'OA de la GovCA du Bénin, ou encore sur demande authentifiée d'un agent désigné de la LRA partenaire en charge du certificat de la LRA (cet agent ou ces agents doivent être identifiés dans le protocole d'accord comme étant autorisés à faire une telle demande).

La politique définie dans cette section est conforme à l'article 321 du Code du Numérique adopté par le Gouvernement du Bénin.

4.9.3 Procédure de Demande de Révocation

Le registraire de la GovCA révoque les certificats dès réception de preuves suffisantes de la compromission ou de la perte de la clé privée correspondante de l'abonné. Une demande de révocation d'un certificat doit identifier le certificat à révoquer, expliquer la raison de la révocation et permettre l'authentification de la demande (ex. signature numérique ou manuelle).

Les situations suivantes peuvent entraîner la révocation d'un certificat :

- Lorsque l'abonné ou le DCH ne respecte pas la CP ou le RPS concernant l'utilisation du certificat ;
- Lorsque le certificat n'a pas été délivré conformément à la CP ou au RPS ; et
- les informations contenues dans le certificat ne sont plus valables ou pertinentes.

S'il est établi qu'une clé privée utilisée pour autoriser l'émission d'un ou plusieurs certificats peut avoir été compromise (ex. par exemple, un certificat de la RA ou d'une LRA partenaire), tous les certificats autorisés directement ou indirectement par cette clé privée depuis la date de la compromission réelle ou présumée doivent être révoqués ou leur émission doit être vérifiée comme étant appropriée.

4.9.4 Délai de grâce pour La Révocation d'un Certificat

Il n'y a pas de délai de grâce pour la révocation dans le cadre de cette politique. Les parties autorisées à faire une demande de révocation d'un certificat, y compris les abonnés et les DCH, doivent le faire immédiatement après avoir pris connaissance de la nécessité d'une révocation.

4.9.5 Délai accordé à la CA pour traiter la Demande de Révocation

La GovCA du Bénin révoquera les certificats aussi rapidement que possible après réception d'une demande de révocation en bonne et due forme. Les demandes de révocation seront traitées avant la publication de la CRL suivante, à l'exception des demandes validées dans les deux heures suivant l'émission de la CRL. Les demandes de révocation validées dans les deux heures suivant l'envoi d'une CRL doivent être traitées avant la publication de la CRL suivante.

4.9.6 Exigence de Vérification de la Révocation pour les Parties Utilisatrices

L'utilisation de certificats révoqués ou suspendus pourrait avoir des conséquences dommageables ou catastrophiques. La question de la fréquence d'obtention de nouvelles données de révocation est une décision qui doit être prise par la partie utilisatrice, compte tenu du risque, de la responsabilité et des conséquences de l'utilisation d'un certificat dont le statut de révocation ne peut être garanti.

4.9.7 Fréquence d'émission des Listes de Révocation

Les CRL sont émises périodiquement, même si aucune modification n'est nécessaire, afin de garantir l'actualité des informations. Les informations sur le statut des certificats peuvent être délivrées plus fréquemment que la fréquence d'émission décrite ci-dessous.

Les informations sur le statut des certificats sont publiées au plus tard lors de la prochaine mise à jour prévue. Cela facilitera la mise en cache locale des informations sur le statut du certificat pour une utilisation hors ligne ou à distance.

La GovCA doit émettre les CRL au moins une fois toutes les 6 heures avec une période de validité de 72 heures.

La politique définie dans cette section est conforme au Code du Numérique du gouvernement du Bénin.

4.9.8 Délai de Latence pour Les CRL

Les CRL doivent être publiés dans les dépôts dans les quatre heures suivant leur création. En outre, chaque CRL doit être publiée au plus tard à l'heure indiquée dans le champ nextUpdate de la CRL précédemment publiée pour la même portée.

4.9.9 Disponibilité de la Révocation/Vérification de Statut en Ligne

La GovCA du Bénin doit prendre en charge la vérification du statut et de la révocation en ligne via l'OCSP comme défini dans la RFC 6960. La latence des informations sur l'état des certificats diffusées en ligne par la GovCA du Bénin ou son CSS délégué doit être conforme ou supérieure aux exigences d'émission de CRL énoncées dans la section **Erreur ! Source du renvoi introuvable.**.

4.9.10 Exigences relatives à La Vérification en Ligne des Révocations

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.9.11 Autres formes d'annonces de Révocation disponibles

La GovCA peut également utiliser d'autres méthodes pour faire connaître les certificats qu'elle a révoqués. Toute autre méthode doit répondre aux exigences suivantes :

- La méthode alternative doit être décrite dans le CPS approuvé de la CA ;
- La méthode alternative doit fournir des services d'authentification et d'intégrité proportionnels au niveau d'assurance du certificat vérifié ; et
- la méthode alternative doit répondre aux exigences d'émission et de latence pour les CRL énoncées dans les sections **Erreur ! Source du renvoi introuvable.** et 4.9.8.

4.9.12 Exigences Spéciales liées à une Re-Clé : Une Compromission Clé

En cas de révocation d'un certificat d'abonné en raison de la compromission, réelle ou supposée, d'une clé privée, une CRL doit être émise par la GovCA dans les 6 heures suivant la notification.

4.9.13 Les Circonstances D'une Suspension

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.9.14 Qui peut faire une Demande de Suspension

Voir la section **Erreur ! Source du renvoi introuvable.**.

4.9.15 Demande de Suspension : Procédure

voir la section **Erreur ! Source du renvoi introuvable.**.

4.9.16 Limites de la Période de Suspension

aucune disposition.

4.10 SERVICES RELATIFS AU STATUT DES CERTIFICATS

4.10.1 Caractéristiques opérationnelles

La GovCA du Bénin mettra en place un service de CSS conformément à la RFC 6960.

4.10.2 Disponibilité des Services

Les mécanismes et procédures du CSS sont conçus pour garantir la disponibilité du service 24h/24, 7j/7, avec un minimum de 99 % de disponibilité globale par an et un temps d'arrêt programmé ne dépassant pas 0,5 % par an.

4.10.3 Caractéristiques facultatives

Aucune disposition.

4.11 FIN DE L'ABONNEMENT

Les certificats qui ont expiré avant ou à la fin de l'abonnement ne doivent pas être révoqués. Les certificats d'abonnés non expirés sont révoqués à la fin de la souscription.

4.12 ENTIERCEMENT ET RÉCUPÉRATION DES CLÉS

4.12.1 Entiercement et Récupération des Clés : Politique et Pratiques

Les clés privées de la GovCA ne sont jamais entiercées par un tiers.

Les clés de gestion des abonnés peuvent être sauvegardées par la GovCA pour permettre la récupération des clés. La GovCA établira des exigences de sécurité et d'authentification dans son CPS et dans le RPS de la LRA partenaire.

Les clés de signature de niveau d'assurance élevé de l'abonné ne doivent pas être sauvegardées par la GovCA du Bénin.

Les clés de signature de niveaux d'assurance basique et moyen de l'abonné peuvent être stockées en toute sécurité dans une application au nom de l'abonné. Cette mise en œuvre doit être approuvée par la PA de la GovCA du Bénin.

Les clés sauvegardées dans la base de données de la GovCA et les clés stockées dans une application au nom des abonnés et approuvées par la PA de la GovCA doivent être protégées au moins au niveau de sécurité dans lequel elles sont générées, livrées et protégées par l'abonné.

En aucun cas, une clé de signature d'un abonné ne sera détenue en fiducie par un organisme tiers externe.

4.12.2 Encapsulation et Récupération des Clés de Session : Politique et Pratiques

Non applicable.

5. LES CONTRÔLES DE GESTION, OPÉRATIONNELS ET PHYSIQUES

5.1 LES CONTRÔLES DE SÉCURITÉ PHYSIQUE

Tous les équipements de la CA, y compris les modules cryptographiques de la CA, doivent être protégés contre tout accès non autorisé en tout temps.

5.1.1 Emplacement et Construction du Site

L'emplacement et la construction des installations abritant les équipements de la GovCA du Bénin, ainsi que les sites abritant les postes de travail distants utilisés pour assurer la gestion des CA, doivent être conformes aux installations utilisées pour héberger des informations sensibles de grande valeur. L'emplacement et la construction du site, lorsqu'ils sont combinés avec d'autres mécanismes de protection physique tels que des gardes, des serrures de haute sécurité et des capteurs d'intrusion, doivent fournir une protection solide contre l'accès non autorisé aux équipements et aux archives de la GovCA du Bénin

L'infrastructure de production et de reprise après sinistre de la GovCA doit être mise en œuvre dans deux installations distinctes dotées de contrôles de gestion, opérationnels et physiques similaires.

5.1.2 Accès Physique

5.1.2.1 Accès Physique aux Équipements de La CA

Les équipements de la GovCA du Bénin et les postes de travail à distance utilisés pour assurer l'administration des CA doivent toujours être protégés contre tout accès non autorisé. Les mécanismes de sécurité doivent être proportionnels au niveau de menace dans l'environnement de ces équipements. Puisque la GovCA du Bénin doit prévoir d'émettre des certificats à tous les niveaux d'assurance, elle sera exploitée et contrôlée sur la présomption qu'elle émettra au moins un certificat de niveau d'assurance élevé.

Les exigences de sécurité physique relatives à la GovCA sont les suivantes :

- S'assurer qu'aucun accès non autorisé au matériel ne soit permis ;
- S'assurer que tous les supports amovibles et documents papier contenant des informations sensibles en texte clair sont stockés dans des conteneurs sécurisés ;
- Assurer en tout temps une surveillance manuelle ou électronique pour déceler toute intrusion non autorisée ;
- Veiller à ce qu'un registre des accès soit tenu et inspecté périodiquement ; et
- Exiger un contrôle d'accès physique effectué par deux personnes au module cryptographique et aux systèmes informatiques. Note : Le contrôle d'accès physique par deux personnes sur les serveurs hébergeant le CSS, les modules cryptographiques hébergeant les clés de signature privées du CSS et les applications de dépôt public ne sera pas possible tant que le rôle d'OA de la Gov CA du Bénin sera attribué à EDC. ~~However, two-person physical access control on the cryptographic modules hosting the CSS private signature keys will be possible while the Benin GovCA OA role is assigned to EDC.~~

Le contrôle de l'accès physique multipartite à l'équipement de la CA peut être réalisé par toute combinaison de deux rôles de confiance ou plus (voir la section **Erreur ! Source du renvoi introuvable.**), à condition que les tâches exécutées soient séparées conformément aux exigences et aux fonctions définies pour chaque rôle de confiance. Par exemple, un Auditeur et un Opérateur peuvent accéder au site abritant l'équipement de la CA pour effectuer une sauvegarde sur bande, mais seul l'Opérateur peut effectuer la sauvegarde sur bande.

Les modules cryptographiques amovibles, les informations d'activation utilisées pour accéder aux modules cryptographiques et aux autres équipements sensibles de la CA ou pour les activer doivent être placés dans des conteneurs sécurisés lorsqu'ils ne sont pas utilisés. Les données d'activation doivent être soit mémorisées, soit enregistrées et stockées d'une manière proportionnelle à la sécurité offerte par le module cryptographique et ne doivent pas être stockées avec le module cryptographique ou le matériel amovible associé aux postes de travail à distance utilisés pour assurer l'administration de la CA.

Une vérification de sécurité de l'installation abritant les équipements de la GovCA du Bénin ou encore les postes de travail à distance utilisés pour assurer l'administration des CA doit être effectuée si l'installation est laissée sans surveillance. Au minimum, le contrôle doit vérifier les points suivants :

- L'équipement est dans un état approprié au mode de fonctionnement actuel ;
- Tous les contenants de sécurité sont correctement sécurisés ;
- Les systèmes de sécurité physique (ex : serrures de portes, couvercles des évents) fonctionnent correctement ; et
- La zone est protégée contre les accès non autorisés.

L'OA de la GovCA et les personnes investies d'un rôle de confiance seront explicitement chargées d'effectuer ces contrôles. Un journal identifiant la personne effectuant un contrôle à chaque fois est tenu à jour. La dernière personne à partir doit parapher une feuille de sortie indiquant la date et l'heure, et affirmant que tous les mécanismes de protection physique nécessaires sont en place et activés.

5.1.2.2 Accès Physique aux équipements de La RA

Les équipements de la RA doivent être protégés contre tout accès non autorisé lorsque le module cryptographique est installé et activé. La RA doit mettre en œuvre des contrôles d'accès physique afin de réduire le risque d'altération des équipements même lorsque le module cryptographique n'est pas installé et activé. Ces mécanismes de sécurité doivent être proportionnels au niveau de menace dans l'environnement des équipements de la RA.

5.1.2.3 Accès Physique aux équipements du CSS

Les exigences de contrôle de l'accès physique au matériel du CSS doivent répondre aux exigences de la CA en matière d'accès physique spécifiées dans la section **Erreur ! Source du renvoi introuvable.**.

5.1.3 Alimentation électrique et climatisation

La capacité de sauvegarde de la GovCA du Bénin doit être suffisante pour verrouiller automatiquement les entrées, terminer les actions en cours et enregistrer l'état des équipements

avant que le manque de courant ou de climatisation ne provoque un arrêt. En outre, les dépôts de la GovCA du Bénin (contenant les certificats et les CRL délivrés par la GovCA du Bénin) doivent être dotés d'une alimentation électrique ininterrompue redondante et de générateurs suffisants pour un minimum de six heures de fonctionnement en l'absence d'énergie électrique commerciale.

L'installation abritant la GovCA du Bénin doit être équipée de systèmes de chauffage et de climatisation pour contrôler la température et l'humidité relative.

Les restrictions de la GovCA du Bénin lorsqu'elle est hébergée et exploitée par EDC sont les suivantes :

- Il n'est pas possible d'obtenir des alertes en dehors des heures de travail si les systèmes environnementaux sont défaillants (refroidissement/humidité) ; et
- Le centre de données d'EDC n'a pas d'autres mécanismes de contrôle d'humidité à part la climatisation.

5.1.4 Expositions À L'eau

Les équipements de la CA doivent être installés de manière à ne pas être exposés à l'eau (ex : sur des tables ou des planchers surélevés).

L'exposition à l'eau provenant des mesures de prévention et de protection contre l'incendie (ex : les systèmes de gicleurs) ne fait pas partie de cette exigence.

5.1.5 Prévention et Protection contre les Incendies

L'exposition au feu peut causer des dommages importants et instantanés au matériel de traitement de l'information et par conséquent affecter le service offert par le centre de confiance. Par conséquent, les mesures suivantes doivent être prises pour prévenir les dommages causés par l'exposition au feu.

- La prévention et la protection contre les alertes d'incendie doivent être en place à divers endroits dans le centre de données hébergeant l'infrastructure de la GovCA ;
- Le personnel doit avoir reçu une formation sur les procédures à suivre en cas d'incendie ; et
- Les mécanismes d'extinction des incendies doivent être en place.

5.1.6 Stockage de Support

Les supports de la CA doivent être stockés de manière à les protéger contre les dommages accidentels (eau, feu, électromagnétique).

5.1.7 Évacuation des déchets

Les supports et la documentation sensibles qui ne sont plus nécessaires aux opérations doivent être détruits en toute sécurité. Par exemple, les documents papier sensibles doivent être déchiquetés, brûlés ou rendus irrécupérables de quelque manière que ce soit.

5.1.8 Sauvegarde hors site

Des sauvegardes complètes du système nécessaires à la reprise après une défaillance du système doivent être effectuées selon un calendrier périodique. Les sauvegardes doivent être effectuées et stockées hors site au moins une fois par semaine. Au moins une copie de sauvegarde complète doit être stockée dans un emplacement hors site distinct de celui des équipements opérationnels de la GovCA. Seule la dernière copie de sauvegarde complète doit être conservée. La sauvegarde doit être stockée dans un site doté de contrôles physiques et procéduraux correspondant à ceux de la GovCA du Bénin opérationnelle.

5.2 CONTRÔLES PROCÉDURAUX

5.2.1 Les Rôles de Confiance

Un rôle de confiance est un rôle dont le titulaire exerce des fonctions qui peuvent entrainer des problèmes de sécurité si elles ne sont pas exécutées correctement, que ce soit accidentellement ou intentionnellement. Les personnes choisies pour remplir ces rôles doivent être extraordinairement responsables, sinon l'intégrité de la CA est affaiblie. Les fonctions exercées dans ces rôles constituent la base de la confiance pour toutes les utilisations de la GovCA du Bénin.

Deux approches sont adoptées pour augmenter la probabilité que ces rôles puissent être remplis avec succès. La première consiste à s'assurer que la personne qui remplit le rôle est digne de confiance et correctement formée. La seconde répartit les fonctions entre plusieurs personnes, de sorte que toute activité malveillante entrainerait une collusion.

Les exigences de cette politique sont définies en termes de quatre rôles relevant de l'OA de la GovCA du Bénin :

- Administrateur de système - autorisé à installer, configurer et maintenir le système d'exploitation, le réseau, la VM et les utilitaires ; autorisé à effectuer la sauvegarde et la récupération de système ; à établir et maintenir les comptes du système ; à configurer les systèmes d'exploitation et les paramètres d'audit des logiciels non-CA ; et générer des clés de composants ;
- Administrateur de la CA - Relevant de l'autorité d'exploitation de la CA, les administrateurs de la CA sont autorisés à installer, à configurer et à gérer le logiciel de la CA, du CSS et du référentiel ainsi que les modules cryptographiques ;
- Autorité d'enregistrement - autorisée à demander ou à approuver l'émission et la révocation des certificats ; et
- Agent de conformité en matière de sécurité - Relevant de l'autorité d'exploitation de la CA, le rôle d'agent de conformité en matière de sécurité SCO est autorisé à examiner, à maintenir et à archiver les journaux de vérification. Le rôle du SCO ne doit pas être confondu avec celui de l'auditeur de conformité, qui n'est pas considéré comme un rôle de confiance.

Les rôles requis pour chaque niveau d'assurance sont identifiés à la section **Erreur ! Source du renvoi introuvable.**. La séparation des tâches doit être conforme à la section **Erreur ! Source du renvoi introuvable.** et aux exigences relatives au contrôle par deux personnes à la section

Erreur ! Source du renvoi introuvable., quels que soient les titres et les numéros des rôles de confiance.

Les restrictions affectant la GovCA du Bénin lorsqu'elle est hébergée et exploitée par EDC : La même personne de Rôle de Confiance EDC peut se voir attribuer le rôle d'Administrateur du Système et le rôle d'Administrateur de la CA.

5.2.2 Nombre de personnes requises par Tâche

Deux personnes ou plus sont requises pour la GovCA et les CSS qui opèrent au niveau d'assurance élevée pour les tâches suivantes :

- La génération de clés de la CA et du CSS ; et
- l'activation de la clé de signature de la CA et du CSS~~; and~~.
- ~~CA and CSS private key backup.~~

Lorsqu'un contrôle multipartite de l'accès logique est requis, au moins un des participants doit être un administrateur de la CA. Tous les participants doivent exercer un rôle de confiance tel que défini dans la section **Erreur ! Source du renvoi introuvable.**.

L'accès physique aux CA ne constitue pas une tâche telle que définie dans la présente section. Par conséquent, le contrôle de l'accès physique à deux personnes peut être effectué selon les exigences de la section **Erreur ! Source du renvoi introuvable.**.

5.2.3 Identification et Authentification pour Chaque Rôle

Une personne jouant un rôle de confiance doit s'identifier et s'authentifier avant d'être autorisée à effectuer toute action décrite ci-dessus pour ce rôle ou cette identité.

5.2.4 Rôles exigeant la séparation des responsabilités

La séparation des rôles, lorsqu'elle est requise comme indiqué ci-dessous, peut être effectuée soit par les équipements de la CA, soit par des procédures, ou au moyen des deux.

La GovCA du Bénin opère au niveau d'assurance élevée.

Les différents membres du personnel seront spécifiquement désignés pour les quatre rôles définis à la section **Erreur ! Source du renvoi introuvable.** ci-dessus. Ces agents ne peuvent assumer qu'un seul des rôles d'administrateur du système, d'administrateur de la CA et de SCO. Les agents désignés comme RA peuvent également assumer le rôle d'administrateur de la CA. Un SCO ne doit assumer aucun autre rôle. Les logiciels et le matériel de la CA, du SCO et de la RA doivent identifier et authentifier ses utilisateurs et doivent faire respecter ces rôles.

Les restrictions applicables à la GovCA du Bénin lorsqu'elle est hébergée et exploitée par l'EDC : La même personne de confiance d'EDC peut se voir attribuer le rôle d'administrateur du système et le rôle d'administrateur de la CA.

5.3 CONTRÔLES DU PERSONNEL

5.3.1 Antécédents, Qualifications, Expérience et Exigences sécuritaires

La PA et l'OA de la GovCA du Bénin sont chargées du fonctionnement de la GovCA et doivent en répondre.

Toutes les personnes remplissant des rôles de confiance seront sélectionnées sur la base de la loyauté, de la fiabilité et de l'intégrité. En ce qui concerne la GovCA du Bénin, toutes les personnes remplissant des Rôles de Confiance doivent être des citoyens du Bénin (sauf lorsque le rôle de l'OA de la GovCA du Bénin est assumé par EDC) et avoir passé avec succès la procédure de vérification des antécédents du Gouvernement du Bénin et l'« Enquête de moralité » du Gouvernement du Bénin. Le personnel de l'OA de la GovCA du Bénin agissant en Rôles de Confiance est soumis à un accord de confidentialité.

Note : Les politiques internes d'EDC s'appliquent aux agents d'EDC auxquels des rôles de confiance ont été attribués lorsque le rôle d'OA de la GovCA du Bénin est assigné à EDC.

5.3.2 Procédures de Vérification des Antécédents

Le personnel de l'OA de la GovCA du Bénin exerçant des rôles de confiance doit, au minimum, se soumettre aux procédures de vérification des antécédents du gouvernement du Bénin.

Le personnel de la GovCA du Bénin exerçant des rôles de confiance doit, au minimum, faire l'objet d'une enquête d'antécédents couvrant les domaines suivants :

- L'emploi ;
- La formation ;
- Lieu de résidence ;
- Le respect de la loi ; et
- Références.

La période d'enquête doit couvrir au moins **les cinq dernières années** pour chaque domaine, à l'exception du contrôle du lieu de résidence qui doit couvrir au moins **les trois dernières années**. Indépendamment de la date d'obtention, le diplôme d'études le plus élevé doit être contrôlé.

L'adjudication de l'enquête sur les antécédents sera effectuée par une autorité d'adjudication compétente selon une procédure conforme à la politique et aux procédures d'embauche du gouvernement du Bénin, ou un niveau équivalent d'enquête et d'adjudication.

La vérification des antécédents sera actualisée **tous les dix ans**.

Le personnel de l'OA de la GovCA du Bénin exerçant des rôles de confiance est soumis à une clause de confidentialité qui doit être signée par le demandeur et stockée en toute sécurité par l'OA de la GovCA du Bénin.

Note : La procédure de vérification interne des antécédents au sein d'EDC s'applique aux agents d'EDC auxquels sont attribués des rôles de confiance lorsque le rôle d'OA de la GovCA du Bénin est assigné à EDC.

5.3.3 Exigences en matière de Formation

Tout le personnel exerçant des fonctions en rapport avec les opérations de la GovCA du Bénin doit recevoir une formation complète sur toutes les tâches opérationnelles qu'il est censé accomplir, y compris les politiques et procédures de sécurité et d'exploitation, le traitement et le compte rendu des incidents et les procédures de reprise après sinistre et de continuité des activités.

En outre, le personnel exerçant des fonctions en rapport avec les opérations de la GovCA du Bénin doit recevoir une formation complète ou démontrer ses compétences dans les domaines suivants :

- Les principes et les mécanismes de sécurité applicables à la CA/RA ; et
- Toutes les versions du logiciel de PKI en service sur le système de la CA.

Il convient de conserver les documents identifiant tout le personnel ayant reçu une formation et le niveau de formation suivi. Lorsqu'une compétence a été démontrée en lieu et place d'une formation, des documents justificatifs sont conservés.

Note : Les exigences de formation interne de l'EDC s'appliquent aux agents d'EDC qui se voient attribuer des rôles de confiance lorsque le rôle d'OA de la GovCA du Bénin est assigné à EDC.

5.3.4 Fréquence et Exigences du Recyclage

Les personnes en charge des rôles de la PKI doivent être informées des changements dans le fonctionnement de la GovCA du Bénin. Tout changement important dans le fonctionnement doit faire l'objet d'un plan de formation (sensibilisation) et l'exécution de ce plan doit être documentée. Des exemples de tels changements sont la mise à niveau des logiciels ou du matériel de la GovCA du Bénin, les changements apportés aux systèmes de sécurité automatisés et la délocalisation de l'équipement.

Des documents doivent être conservés pour identifier tout le personnel qui a reçu une formation et le niveau de formation suivi.

Note : La fréquence et les exigences de recyclage interne au sein d'EDC s'appliquent aux agents d'EDC affectés à des rôles de confiance lorsque le rôle d'OA de la CA racine du Bénin est assigné à EDC.

5.3.5 Périodicité et Séquence de Rotation des Postes

La GovCA ne procède pas à la rotation des postes.

Cependant, l'OA de la GovCA du Bénin veille à ce qu'une formation appropriée et un transfert de connaissances soient effectués avant qu'un agent exerçant un rôle de confiance ne soit remplacé par une nouvelle personne afin d'assurer la continuité et l'intégrité des services de la GovCA.

Note : Les politiques internes de l'EDC concernant la fréquence et la séquence de la rotation des postes s'appliquent aux agents d'EDC auxquels des rôles de confiance ont été attribués lorsque le rôle d'OA de la GovCA du Bénin est assigné à EDC.

5.3.6 Sanctions pour Les Actions non autorisées

La PA et l'OA de la GovCA du Bénin prennent les mesures appropriées lorsque le personnel a effectué des actions impliquant la GovCA du Bénin ou son dépôt, des actions non autorisées dans la présente CP, le CPS de la GovCA du Bénin, le RPS de la LRA partenaire ou d'autres procédures publiées par la PA et l'OA de la GovCA du Bénin.

Note : Les politiques internes de l'EDC s'appliquent aux agents d'EDC auxquels des rôles de confiance ont été attribués lorsque le rôle d'OA de la GovCA du Bénin est assigné à EDC.

5.3.7 Exigences relatives au personnel contractuel

Le personnel contractuel employé pour exécuter des fonctions relatives à la CA racine du Bénin ou à une CA partenaire doit répondre aux exigences en matière de personnel énoncées dans la CP de la GovCA du Bénin ou la CP, CPS et RPS de la LRA partenaire, selon le cas.

Note : Les politiques internes de l'EDC s'appliquent aux agents d'EDC auxquels des rôles de confiance ont été attribués lorsque le rôle d'OA de la GovCA du Bénin est assigné à EDC.

5.3.8 Documentation mise à La Disposition du Personnel

En ce qui concerne la GovCA du Bénin, une documentation complète permettant de définir les tâches et les procédures pour chaque rôle de confiance doit être fournie au personnel remplissant ce rôle.

5.4 LES PROCÉDURES D'ENREGISTREMENT DES AUDITS

Des fichiers journaux d'audit sont générés pour tous les événements relatifs à la sécurité de la GovCA du Bénin. Pour les CA fonctionnant dans un environnement de machine virtuelle (VME), des journaux d'audit doivent être générés pour tous les événements applicables à la fois sur la machine virtuelle (VM) et le noyau d'isolation (c'est-à-dire l'hyperviseur).

Dans la mesure du possible, les journaux d'audit de sécurité doivent être automatiquement collectés. Lorsque cela n'est pas possible, un journal, un formulaire papier ou un autre mécanisme physique doit être utilisé. Tous les journaux d'audit de sécurité, électroniques et non électroniques, sont conservés et mis à disposition lors des audits de conformité.

5.4.1 Critères de Collecte des Événements

Un message de n'importe quelle source reçu par la GovCA du Bénin demandant une action liée à l'état opérationnel de la CA est un événement vérifiable. Au minimum, chaque enregistrement d'audit doit comprendre les éléments suivants (enregistrés automatiquement ou manuellement pour chaque événement vérifiable) :

- Le type de l'évènement ;
- La date et l'heure de l'événement ;
- Un indicateur de réussite ou d'échec, si nécessaire ; et
- l'identité de l'entité et/ou de l'opérateur qui a causé l'événement.

Les exigences détaillées en matière d'audit sont énumérées dans le tableau ci-dessous en fonction du niveau d'assurance. La GovCA du Bénin doit enregistrer les événements identifiés dans le tableau pour le niveau d'assurance élevé.

Toutes les capacités d'audit de sécurité du système d'exploitation de la GovCA du Bénin et des applications de la CA requises par la présente CP doivent être activées. En conséquence, la plupart des événements identifiés dans le tableau seront automatiquement enregistrés. Lorsque les événements ne peuvent pas être enregistrés automatiquement, la CA doit mettre en œuvre des procédures manuelles pour satisfaire à cette exigence.

La GovCA est gérée au niveau d'assurance élevé.

Tableau 4 – Critères de Collecte des Événements

Événement à auditer
SECURITY AUDIT
Any changes to the Audit parameters, e.g. audit frequency, type of event audited
Any attempt to delete or modify the Audit logs
Obtaining a third-party time-stamp
IDENTIFICATION AND AUTHENTICATION
Successful and unsuccessful attempts to assume a role
The value of maximum authentication attempts is changed
The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An Administrator changes the type of authenticator, e.g. from password to biometrics
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION

Événement à auditer
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component private keys
All access to certificate subject private keys retained within the CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
All changes to the trusted public keys, including additions and deletions
SECRET KEY STORAGE
The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION
All certificate requests
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL
The approval or rejection of a certificate status change request
CA CONFIGURATION
Any security-relevant changes to the configuration of the CA
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile

Événement à auditer
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of the Operating System
Installation of the CA
Installing hardware cryptographic modules
Removing hardware cryptographic modules
Destruction of cryptographic modules
System Startup
Logon Attempts to CA Applications
Receipt of Hardware/Software
Attempts to set passwords
Attempts to modify passwords
Backing up CA internal database
Restoring CA internal database
File manipulation (e.g. creation, renaming, moving)
Posting of any material to a repository
Access to CA internal database
All certificate compromise notification requests

Événement à auditer
Loading tokens with certificates
Shipment of Tokens
Zeroizing tokens
Re-key of the CA
Configuration changes to the CA server involving:
Hardware
Software
Operating System
Patches
PHYSICAL ACCESS / SITE SECURITY
Personnel Access to room housing CA
Access to the CA server
Known or suspected violations of physical security
ANOMALIES
Software Error conditions
Software check integrity failures
Receipt of improper messages
Misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures

Événement à auditer
Violations of Certificate Policy
Violations of Certification Practice Statement
Violations of Registration Practice Statement
Resetting Operating System clock

5.4.2 Fréquence de Traitement des Données

Les systèmes de la GovCA du Bénin doivent être surveillés en permanence afin de fournir des alertes en temps réel sur les événements sécuritaires et opérationnels pour examen par le personnel autorisé de l'OA de la GovCA du Bénin.

5.4.3 Période de Conservation des données d'audit sur La Sécurité

Les données relatives à l'audit de sécurité sont conservées selon le calendrier suivant :

- 3 mois au minimum sur le serveur
- 6 mois au minimum sur le serveur de sauvegarde
- 10 ans au minimum dans les archives

La personne qui supprime les journaux d'audit du système de la GovCA du Bénin doit être un agent officiel différent des personnes qui, en combinaison, sont en charge de la clé de signature de la GovCA.

5.4.4 Protection des données d'audit sur La Sécurité

La configuration et les procédures du système de la GovCA du Bénin doivent être conjointement mises en œuvre pour s'assurer de ce que :

- Seul le personnel affecté aux rôles de confiance dispose d'un accès en lecture aux journaux ;
- Seules les personnes autorisées peuvent archiver les journaux d'audit ; et
- Les journaux d'audit ne sont pas modifiés.

L'entité qui effectue l'archivage du journal d'audit n'a pas besoin d'avoir un accès de modification, mais des procédures doivent être mises en œuvre pour protéger les données archivées contre la destruction avant la fin de la période de conservation du journal d'audit (notez que la suppression nécessite un accès de modification).

Le lieu de stockage hors site des journaux d'audit doit être un lieu sûr et sécurisé, séparé de l'endroit où les données ont été générées.

5.4.5 Procédures de Sauvegarde des Données de l'audit sur La Sécurité

Les journaux d'audit sont sauvegardés **quotidiennement** et une copie est envoyée vers un site externe.

Les résumés des examens des journaux d'audit sont sauvegardés **au moins une fois par mois**. Une copie des résumés des journaux d'audit est envoyée hors site **tous les mois**.

5.4.6 Système de Collecte des Audits sur la Sécurité (Interne et Externe)

Le système de collecte des journaux d'audit peut être ou non externe au système de la GovCA du Bénin. Les processus d'audit automatisés sont lancés au démarrage du système (ou de l'application) et ne s'arrêtent qu'à l'arrêt du système (ou de l'application). S'il s'avère qu'un système d'audit automatisé a échoué et que l'intégrité du système ou la confidentialité des informations protégées par le système est menacée, alors l'OA de la GovCA du Bénin déterminera s'il faut suspendre le fonctionnement de la GovCA du Bénin jusqu'à ce que le problème soit résolu.

5.4.7 Notification au sujet causant un événement

Cette CP n'impose aucune obligation d'informer la personne, l'organisation, le dispositif ou l'application qui a causé l'événement lorsqu'un audit a été réalisé.

5.4.8 Évaluations de la vulnérabilité

Au moins une fois tous les 6 mois, le personnel de la GovCA du Bénin doit évaluer si le système de la CA ou ses composants ont été attaqués ou violés.

Le personnel de la GovCA du Bénin doit effectuer des évaluations de routine pour détecter les preuves d'activités malveillantes.

En outre, des évaluations de vulnérabilité doivent être systématiquement effectuées après des modifications ou des mises à niveau du système.

Les données d'audit de sécurité doivent être examinées par le SCO de la GovCA du Bénin pour détecter des événements tels que des échecs répétés, des demandes d'informations privilégiées, des tentatives d'accès aux fichiers du système et des réponses non authentifiées. Le SCO de la GovCA du Bénin doit contrôler la continuité des données d'audit de sécurité.

5.5 ARCHIVAGE DES DOSSIERS

Les archives de la GovCA du Bénin doivent être suffisamment détaillées pour permettre de vérifier le bon fonctionnement de la GovCA du Bénin ainsi que la validité de tout certificat (y compris ceux qui ont été révoqués ou qui ont expiré) délivré par la GovCA du Bénin.

Les politiques définies dans cette section sont conformes aux articles 301 et 302 du Code du Numérique du Gouvernement du Bénin.

Note : Les dossiers de la GovCA du Bénin ne seront pas archivés par EDC lorsque ce dernier agit en tant qu'OA de la GovCA du Bénin.

5.5.1 Types de documents et d'événements archivés

Au minimum, les données suivantes de la CA, du CSS et de la RA doivent être enregistrées pour être archivées conformément à chaque niveau d'assurance :

Tableau 5 – Types de documents et d'événements archivés

Données à archiver
CA accreditation (e.g. MOA and LOA)
Certificate Policy
Certification Practice Statement
Registration Practice Statement
GovCA architecture and design documents
Contractual obligations
Other agreements concerning operations of the CA
System and equipment configuration
Modifications and updates to system or configuration
Certificate issuance, revocation, rekey and modification requests
Subscriber identity authentication data as per Section 3.2.3
Documentation of receipt and acceptance of certificates (if applicable)
Subscriber Agreements
Documentation of receipt of tokens
All certificates issued or published
Record of CA Re-key
All CRLs issued and/or published
Other data or applications to verify archive contents
Compliance Auditor reports
Any changes to the Audit parameters, e.g. audit frequency, type of event audited
Any attempt to delete or modify the Audit logs
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
All access to certificate subject private keys retained within the CA for key recovery purposes
All changes to the trusted public keys, including additions and deletions
The export of private and secret keys (keys used for a single session or message are excluded)

Données à archiver
The approval or rejection of a certificate status change request
Appointment of an individual to a Trusted Role
Destruction of cryptographic modules
All certificate compromise notifications
Remedial action taken as a result of violations of physical security
Violations of Certificate Policy
Violations of Certification Practice Statement
Violations of Registration Practice Statement

5.5.2 Durée de Conservation des archives

La durée minimale de conservation des données d'archives de la GovCA est de **10 ans**.

Cette durée minimale de conservation de ces archives est destinée uniquement à faciliter le fonctionnement de la GovCA du Bénin.

5.5.3 Protection des Archives

Aucun utilisateur non autorisé ne peut écrire dans l'archive ou la supprimer. En ce qui concerne la GovCA du Bénin, les documents archivés peuvent être déplacés sur un autre support lorsque l'OA de la GovCA du Bénin l'autorise. Le contenu de l'archive ne sera pas divulgué, sauf en conformité avec les sections **Erreur ! Source du renvoi introuvable.** et **Erreur ! Source du renvoi introuvable.**. Les archives des transactions individuelles peuvent être divulguées à la demande de tout abonné impliqué dans la transaction ou de ses agents légalement reconnus. Les supports d'archives doivent être stockés dans une installation de stockage sûre et sécurisée, séparée de la GovCA du Bénin opérationnelle elle-même.

Si le support original ne peut pas conserver les données pendant la période requise, un mécanisme permettant de transférer périodiquement les données archivées sur de nouveaux supports est défini par le site d'archivage.

Les applications nécessaires au traitement des données d'archives seront également conservées pendant une période déterminée par la PA de la GovCA du Bénin pour la GovCA du Bénin.

Préalablement au terme de la période de conservation des archives, l'OA de la CA racine du Bénin mettra les données archivées et les applications nécessaires à la lecture des archives à la disposition d'un centre d'archivage agréé par la PA de la CA racine du Bénin, qui conservera les applications nécessaires à la lecture de ces données archivées.

5.5.4 Procédures de Sauvegarde des archives

Le CPS de la GovCA du Bénin ou un document de référence devra décrire comment les archives sont sauvegardées et gérer.

5.5.5 Exigences relatives à l'horodatage des Registres

Les archives de la CA seront automatiquement horodatées lors de leur création. Le CPS doit décrire comment les horloges du système utilisées pour l'horodatage sont maintenues en synchronisation avec un système de temps standard faisant autorité.

5.5.6 Système de Collecte d'archives (Interne ou Externe)

Les données d'archives sont collectées dans les meilleurs délais, conformément aux descriptions figurant dans le CPS.

5.5.7 Procédures d'obtention et de vérification des Informations contenues dans Les Archives

Les procédures détaillant les modalités de création, de vérification, de conditionnement, de transmission et de stockage des informations d'archives sont publiées dans le CPS de la GovCA du Bénin.

Le contenu des archives ne doit pas être divulgué, sauf si cela est déterminé par la PA de la GovCA du Bénin pour la GovCA du Bénin ou si la loi l'exige. Les archives des transactions individuelles peuvent être divulguées à la demande de tout abonné impliqué dans la transaction ou de ses agents légalement reconnus.

Les politiques définies dans cette section sont en conformité avec les articles 301 et 302 du Code du Numérique adopté par le Gouvernement du Bénin.

5.6 CHANGEMENT DE CLÉS

Afin de minimiser le risque de compromission de la clé privée de signature d'une CA, cette clé peut être changée ; à partir de ce moment, seule la nouvelle clé sera utilisée à des fins de signature de certificats. L'ancienne clé publique, toujours valide, sera disponible pour vérifier les anciennes signatures jusqu'à ce que tous les certificats signés à l'aide de la clé privée associée aient également expiré. Si l'ancienne clé privée est utilisée pour signer les CRL qui couvrent les certificats signés avec cette clé, alors l'ancienne clé doit être conservée et protégée.

Après qu'une CA a effectué un changement de clé, elle peut continuer à délivrer des CRL signées avec l'ancienne clé jusqu'à ce que tous les certificats signés avec cette clé aient expiré. Une fois que tous les certificats signés avec cette ancienne clé ont été révoqués, il est possible que la CA émette une CRL finale à long terme signée avec l'ancienne clé, avec une échéance nextUpdate au-delà de la période de validité de tous les certificats émis. Cette CRL finale sera disponible pour toutes les parties utilisatrices jusqu'à ce que la période de validité de tous les certificats délivrés soit écoulée. Une fois que la dernière CRL a été délivrée, l'ancienne clé privée de signature de la CA peut être détruite.

En ce qui concerne la GovCA du Bénin, les procédures de changement de clé nécessiteront qu'une nouvelle clé publique soit signée par la CA racine du Bénin.

La GovCA du Bénin subordonnée à la CA racine du Bénin doit être en mesure de continuer à interagir avec la CA racine du Bénin après que la GovCA du Bénin aura effectué une reconduction clé.

5.7 COMPROMISSION ET REPRISE APRÈS SINISTRE

L'OA de la GovCA du Bénin élaborera des procédures de reprise après sinistre permettant un retour aux opérations des services critiques dans les plus brefs délais.

Les procédures de reprise après sinistre seront testées par l'OA de la GovCA du Bénin au moins une fois par trimestre.

Les politiques définies dans cette section sont conformes aux articles 309 et 310 du Code du Numérique adopté par le gouvernement du Bénin.

5.7.1 Procédures de Traitement des Incidents et des Compromissions

La PA de la GovCA du Bénin, la PA de la CA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin doivent être avisés si l'un des cas suivants se produit :

- Présomption ou détection d'une compromission des systèmes de la CA ;
- Tentatives physiques ou électroniques de piratage des systèmes de la CA ;
- Attaques par déni de service sur les composants de la CA ; et
- Tout incident empêchant la CA d'émettre une CRL dans les 24 heures suivant l'heure spécifiée dans le champ nextUpdate de sa CRL actuellement valide.

L'OA de la GovCA du Bénin rétablira les capacités opérationnelles le plus rapidement possible, conformément aux procédures définies dans le CPS applicable.

En cas d'incident tel que décrit ci-dessus, la PA de la GovCA du Bénin doit aviser la PA de la CA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin dans les 24 heures suivant la découverte de l'incident, avec une analyse préliminaire des mesures correctives.

Dans les 10 jours ouvrables suivant la résolution de l'incident, la PA de la GovCA du Bénin doit afficher sur sa page web publique un avis identifiant l'incident et en informer la PA de la CA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin, comme le stipulent les articles 301 et 302 du Code du Numérique N° 2017-20 du gouvernement du Bénin. L'avis public comprend les éléments suivants :

- Quels composants de la CA ont été touchés par l'incident ;
- L'interprétation que la CA a faite de l'incident ;
- Qui est touché par l'incident ;
- Quand l'incident a été découvert ;
- Une liste complète de tous les certificats qui ont été délivrés par erreur ou qui n'étaient pas conformes à la CP, au CPS et au RPS, selon le cas, à la suite de l'incident ; et
- Une déclaration selon laquelle l'incident a été entièrement résolu.

La notification fournie directement à la PA de la GovCA du Bénin doit également inclure les mesures détaillées prises pour remédier à l'incident.

Les politiques définies dans cette section sont conformes aux articles 309 et 310 du Code du Numérique du Gouvernement du Bénin.

5.7.2 Les Ressources informatiques, les logiciels et/ou les données sont corrompus

Lorsque des ressources informatiques, des logiciels et/ou des données sont corrompus, la GovCA du Bénin doit réagir comme suit :

- Avant de relancer le système, assurez-vous que son intégrité a été rétablie ;
- Si les clés de signature de la CA ne sont pas détruites, le fonctionnement de la CA doit être rétabli, en donnant la priorité à la capacité de générer des informations sur l'état des certificats dans le cadre du calendrier d'émission des CRL spécifié dans la section **Erreur ! Source du renvoi introuvable.**, au **Erreur ! Source du renvoi introuvable.** ; et
- si les clés de signature de la CA sont détruites, le fonctionnement de la CA doit être rétabli le plus rapidement possible, en donnant la priorité à la génération d'une nouvelle paire de clés de la CA.

Dans le cas d'un incident tel que décrit ci-dessus, la PA de la GovCA du Bénin doit afficher un avis sur sa page web identifiant l'incident et fournir une notification à la PA de la CA racine du Bénin et à l'Organe de contrôle du Gouvernement du Bénin. Voir la section 0 pour le contenu de l'avis.

5.7.3 Procédures de Compromission des Clés privées d'une Entité

Si les clés de signature de la GovCA du Bénin sont compromises ou perdues (de sorte que la compromission soit envisageable même si elle n'est pas certaine) :

- La PA de la CA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin doivent être notifiés par la PA de la GovCA du Bénin afin que la CA racine du Bénin puisse émettre des CRL révoquant le certificat de la CA subordonnée émis à la GovCA compromise ;
- Une nouvelle paire de clés de la GovCA du Bénin doit être générée conformément aux procédures définies dans le CPS de la GovCA du Bénin ; et
- Les nouveaux certificats de la GovCA du Bénin seront émis par la CA racine du Bénin conformément à la CP et au CPS de la CA racine du Bénin et de la GovCA.

L'OA de la GovCA du Bénin doit également enquêter et faire un rapport à la PA de la GovCA du Bénin, à la PA de la CA racine du Bénin et à l'Organe de contrôle du gouvernement du Bénin, sur les causes de la compromission ou de la perte et sur les mesures prises pour éviter qu'elle ne se reproduise.

La PA de la GovCA du Bénin doit afficher un avis sur sa page web décrivant la compromission. Voir la section 0 pour le contenu de l'avis.

5.7.4 Capacités de continuité des activités après Un Désastre

Le référentiel de la GovCA du Bénin et les systèmes CSS doivent être déployés de manière à assurer une disponibilité 24 heures sur 24, 365 jours par an. L'OA de la GovCA du Bénin doit mettre en œuvre des fonctionnalités permettant d'assurer des niveaux élevés de fiabilité pour le référentiel et le CSS.

L'OA de la GovCA du Bénin exploite un site de secours, dont le but est d'assurer la continuité des opérations en cas de défaillance du site principal. Les opérations de la GovCA du Bénin doivent être conçues pour reprendre le service complet dans les six (6) heures suivant la défaillance du système primaire.

L'OA de la GovCA du Bénin informe dès que possible et de manière sécurisée la PA de la GovCA du Bénin, qui à son tour devra informer la PA de la CA racine du Bénin, et l'Organe de contrôle du gouvernement du Bénin en cas de sinistre lorsque l'installation de la GovCA du Bénin est physiquement endommagée et que toutes les copies des clés de signature de la GovCA du Bénin sont détruites.

Les parties utilisatrices peuvent décider de leur propre chef de continuer à utiliser les certificats signés avec la clé privée détruite en attendant le rétablissement du fonctionnement de la GovCA du Bénin avec de nouveaux certificats.

5.8 CESSATION DE LA CA

Avant de mettre fin à la GovCA du Bénin, la PA de la GovCA du Bénin doit informer la PA de la CA racine du Bénin, l'Autorité Nationale de Politique du Gouvernement du Bénin et l'Organe de Contrôle du Gouvernement du Bénin, les LRA partenaires et les abonnés au moins deux mois avant la cessation.

En cas de cessation des activités de la GovCA du Bénin, les certificats signés par la GovCA du Bénin seront révoqués et la PA de la GovCA du Bénin avisera la PA de la CA racine du Bénin que les activités de la GovCA du Bénin ont pris fin afin qu'elle puisse révoquer les certificats de CA subordonnés qu'elle a émis à la GovCA du Bénin. En cas de cessation des activités de la GovCA du Bénin, les certificats signés par la GovCA du Bénin seront révoqués et la PA de la GovCA du Bénin avisera la PA de la CA racine du Bénin que les activités de la GovCA du Bénin ont pris fin afin qu'elle puisse révoquer les certificats de CA subordonnés qu'elle a émis à la GovCA du Bénin. Avant la cessation des activités de la GovCA du Bénin, l'OA de la GovCA du Bénin doit fournir toutes les données archivées à une installation d'archivage. Tous les certificats émis qui n'ont pas expiré seront révoqués et une CRL finale à long terme avec une nextUpdate dépassant la période de validité de tous les certificats émis sera générée. Cette CRL finale sera accessible à toutes les parties utilisatrices jusqu'à ce que la période de validité de tous les certificats émis soit écoulée. Une fois que la dernière CRL a été émise, la (les) clé(s) de signature privée de la GovCA du Bénin sera (seront) détruite(s).

Les politiques définies dans cette section sont conformes à l'article 315 du Code du Numérique N° 2017-20 adopté par le gouvernement du Bénin.

6. CONTRÔLES TECHNIQUES DE SÉCURITÉ

6.1 GENERATION ET INSTALLATION DE PAIRES DE CLES

6.1.1 Génération de paires de Clés

6.1.1.1 Génération de paires de Clés de CA et de CSS

Le matériel de codage cryptographique utilisé pour signer les certificats, les CLR ou les informations sur l'état des certificats par la GovCA et le CSS du Bénin doit être généré dans les modules cryptographiques validés FIPS 140-2 de Niveau 3.

Un contrôle multipartite est nécessaire pour la génération des paires de clés de la CA et du CSS pour la GovCA du Bénin, comme indiqué dans la section **Erreur ! Source du renvoi introuvable.**.

La génération de paires de clés de la CA doit créer une piste d'audit vérifiable attestant que les exigences de sécurité des procédures ont été respectées. Pour tous les niveaux d'assurance, la documentation de la procédure doit être suffisamment détaillée pour montrer que la séparation appropriée des rôles a été utilisée.

Un auditeur indépendant doit valider l'exécution des procédures de génération de clés, soit en assistant à la génération de clés, soit en examinant le registre signé et documenté de la génération de clés.

6.1.1.2 Génération de paires de Clés d'abonné

La génération de la paire de clés d'abonné peut être effectuée par l'abonné, la CA ou la RA. Si la CA ou la RA génère des paires de clés d'abonné, les exigences relatives à la fourniture de paires de clés spécifiées dans la section **Erreur ! Source du renvoi introuvable.** doivent également être respectées.

Pour le niveau d'assurance moyen, la génération de la clé doit être effectuée à l'aide d'une méthode logicielle ou matérielle approuvée FIPS 140-2 de Niveau 1 ou supérieur ou d'une norme internationale équivalente.

Pour le niveau d'assurance élevé, la génération de la clé doit être effectuée à l'aide d'une méthode matérielle approuvée FIPS 140-2 de Niveau 2 ou supérieur ou d'une norme internationale équivalente.

Il n'y a pas de disposition FIPS 140-2 ou équivalente pour le niveau d'assurance de basique.

6.1.2 Livraison de la Clé A L'abonné

Si les abonnés génèrent leurs propres paires de clés, il n'est pas nécessaire de fournir des clés privées et cette section ne s'applique pas.

Des applications de confiance gérées par l'OA de la GovCA du Bénin (OA de la GovCA) peuvent être utilisées pour stocker de manière sécurisée les paires de clés d'assurance basique ou moyenne pour le compte des abonnés. Dans ce cas, la clé peut être délivrée par la CA ou la RA aux applications de confiance pour un stockage sécurisé en utilisant des données d'activation connues uniquement des abonnés.

Lorsque les CA ou les RA génèrent des clés au nom de l'abonné, la clé privée doit alors être délivrée de manière sécurisée à l'abonné ou à une application de confiance utilisée par les abonnés pour protéger leurs clés.

Les clés privées peuvent être délivrées par voie électronique ou sur un module cryptographique matériel. Dans tous les cas, les exigences suivantes doivent être respectées :

- Toute personne qui génère une clé privée de signature pour un abonné ne doit conserver aucune copie de la clé après la remise de la clé privée à l'abonné ou à une application de confiance approuvée ;
- La clé privée doit être protégée contre l'activation, la compromission ou la modification pendant le processus de livraison ;
- L'abonné doit accuser réception de la (des) clé(s) privée(s) ;
- La livraison doit être effectuée de manière à ce que les bons jetons et les bonnes données d'activation soient fournis aux bons abonnés.
    - Pour les modules matériels, la responsabilité de l'emplacement et de l'état du module doit être maintenue jusqu'à ce que l'abonné en accepte la possession ;
    - Pour la livraison électronique de clés privées, le matériel doit être crypté à l'aide d'un algorithme cryptographique et la taille de la clé doit être au moins aussi forte que la clé privée. Les données d'activation doivent être transmises par un canal sécurisé distinct ; et
    - Pour les applications de clés partagées, les identités organisationnelles et les dispositifs de réseau, voir également la section 3.2.

La GovCA du Bénin doit tenir un registre d'accusés de réception du jeton par l'abonné. Ces informations peuvent être conservées dans les fichiers journaux d'audit de la CA et de la RA. Pour les certificats d'assurance élevée, il peut être demandé aux abonnés de signer un accusé de réception.

6.1.3 Livraison de la Clé publique à l'émetteur du Certificat

Les exigences suivantes s'appliquent :

- Lorsque les paires de clés sont générées par l'abonné ou la RA, la clé publique et l'identité de l'abonné doivent être livrées de manière sécurisée à la CA pour l'émission du certificat ; et
- le mécanisme de livraison lie l'identité vérifiée de l'abonné à la clé publique. Si la cryptographie est utilisée pour réaliser cette liaison, elle doit être au moins aussi forte que les clés publiques de l'abonné soumises pour signature.

6.1.4 Livraison de Clés publiques de la CA aux Parties Utilisatrices

Lorsque la GovCA met à jour sa paire de clés de signature, elle distribue la nouvelle clé publique de manière sécurisée. La nouvelle clé publique sera distribuée sous forme de certificat de la CA subordonnée obtenu de la CA Racine du Bénin.

6.1.5 Taille Des Clés

La GovCA du Bénin doit utiliser des clés de signature d'au moins 4096 bits pour la RSA.

La GovCA du Bénin doit utiliser l'algorithme de hachage SHA-256, SHA-384 ou SHA-512 lorsqu'elle génère des signatures numériques.

Les CSS doivent signer les réponses en utilisant le même algorithme de signature, la même taille de clé et le même algorithme de hachage que ceux utilisés par la CA pour signer les CLR.

Les certificats d'entité finale doivent contenir des clés publiques d'au moins 2048 bits pour la RSA.

Les certificats d'entité finale qui expirent après le 31/12/2030 doivent contenir des clés publiques d'au moins 3072 bits pour la RSA ;

L'utilisation du TLS ou d'un autre protocole offrant une sécurité similaire pour satisfaire à l'une des exigences de la présente CP doit exiger au minimum un AES (128 bits) ou équivalent pour la clé symétrique et au moins un RSA de 2048 bits ou équivalent pour les clés asymétriques.

L'utilisation du TLS ou d'un autre protocole offrant une sécurité similaire pour satisfaire à l'une des exigences de la présente CP doit exiger au minimum un AES (128 bits) ou équivalent pour la clé symétrique et au moins un RSA de 3072 bits ou équivalent pour les clés asymétriques après le 31/12/2030.

6.1.6 Génération des paramètres de la Clé publique et Contrôle de la Qualité

Aucune disposition.

6.1.7 Objectifs d'utilisation de Clé

Les clés publiques qui sont liées dans des certificats doivent être certifiées pour la signature ou le cryptage, mais pas les deux, sauf dans les cas spécifiés ci-dessous. L'utilisation d'une clé spécifique est déterminée par l'extension d'utilisation de la clé dans le certificat X.509.

Les certificats d'abonnés doivent affirmer l'utilisation des clés en fonction de l'application prévue de la paire de clés. En particulier, les certificats à utiliser pour les signatures numériques (y compris l'authentification) doivent définir les bits de signature numérique et/ou de non-répudiation. Les certificats à utiliser pour le chiffrement de clés ou de données doivent définir le bit de chiffrement de la clé.

Les certificats de niveau d'assurance basique et moyen peuvent comporter une seule clé à utiliser pour le chiffrement et la signature. Ces certificats à double usage doivent être générés et gérés conformément aux exigences de leurs certificats de signature respectifs, sauf indication contraire dans la présente CP. Ces certificats à double usage ne doivent jamais faire valoir le bit d'utilisation de la clé de non-répudiation et ne doivent pas être utilisés pour authentifier des données qui seront vérifiées sur la base du certificat à double usage à une date ultérieure. Les entités sont encouragées, à tous les niveaux d'assurance, à délivrer aux abonnés deux paires de clés, l'une pour la gestion des clés et l'autre pour la signature numérique et l'authentification.

Pour les certificats d'abonnés, l'extension Extended Key Usage doit être présente et ne doit pas contenir de ExtendedKeyUsage {2.5.29.37.0}. Les OID de l'extension Extended Key Usage doivent être compatibles avec les bits d'utilisation de la clé affirmée.

6.2 PROTECTION DES CLÉS PRIVÉES

6.2.1 Normes standards pour le module cryptographique

La norme appropriée pour les modules cryptographiques est la norme FIPS PUB 140-2, sécurité requise pour les modules cryptographiques.

Les modules cryptographiques doivent être validés au niveau FIPS 140-2 identifié dans cette section en outre, la PA de la GovCA du Bénin se réserve le droit d'examiner la documentation technique associée à tout module cryptographique dont l'utilisation est envisagée par la GovCA du Bénin.

Le tableau ci-dessous résume les exigences minimales pour les modules cryptographiques ; des niveaux plus élevés peuvent être utilisés.

Tableau 6 – Exigences minimales de la norme FIPS 140-2 pour les modules cryptographiques

Niveau d'Assurance	CA, CMS and CSS	Abonné	RA
Basic	Level 2 (hardware or software)	No FIPS 140-2 requirement	Level 1 or better (hardware or software)
Medium	Level 2 (hardware)	Level 1 or better (hardware or software)	Level 2 or better (hardware or software)
High	Level 3 (hardware) The Benin GovCA is operated at the High Assurance level	Level 3 for the NID cards Level 2 or better for the other Subscriber cryptographic modules (hardware)	Level 2 or better (hardware or software)

6.2.2 Contrôle multi-personne à clé privée

L'utilisation des clés privées de signature de la GovCA du Bénin et du CSS nécessite l'intervention de plusieurs personnes, comme indiqué à la section **Erreur ! Source du renvoi introuvable.** de la présente CP.

6.2.3 Entiercement de Clé privée

6.2.3.1 Entiercement de la clé de signature privée de la GovCA du Bénin

En aucune circonstance, la clé de signature de la GovCA du Bénin et les clés de signature CSS utilisées pour signer les certificats, les CRL ou les réponses sur l'état des certificats OCSP ne peuvent être entiercées par un tiers.

6.2.3.2 Entiercement des clés de cryptage de la CA

La GovCA du Bénin ne doit exercer aucune fonction de récupération de clés de cryptage impliquant des clés de cryptage délivrées aux CA.

6.2.3.3 Entiercement des clés de signature privées de l'abonné

Les clés de signature privées de l'abonné ne doivent pas être entiercées par un tiers.

6.2.3.4 Entiercement des clés privées de cryptage et à double usage de l'abonné

Les clés de gestion de la clé d'abonné ne doivent pas être entiercées par un tiers.

6.2.4 Sauvegarde de clé privée

6.2.4.1 Sauvegarde de la clé de signature privée de la GovCA du Bénin

Les clés de signature privées de la GovCA du Bénin doivent être sauvegardées sous le contrôle de plusieurs personnes, comme indiqué dans la section **Erreur ! Source du renvoi introuvable.**.

Une sauvegarde des clés de signature privées de la GovCA du Bénin est nécessaire pour faciliter la reprise après sinistre. Les clés de signature privées de la GovCA du Bénin doivent être sauvegardées sous le contrôle de plusieurs personnes.

Au moins une copie de la clé de signature privée de la GovCA du Bénin doit être stockée hors site. Toutes les copies de la clé de signature privée de la CA doivent être comptabilisées et protégées de la même manière que l'original.

6.2.4.2 Sauvegarde de la clé de signature privée de l'abonné

Au niveau des assurances de base ou moyenne, les clés de signature privées de l'abonné peuvent être sauvegardées ou copiées, mais doivent être détenues par l'abonné ou sous le contrôle d'une application de confiance approuvée par la PA de la GovCA du Bénin et gérée par l'OA de la GovCA du Bénin.

Au niveau de la Haute Assurance, les clés de signature privées de l'abonné ne doivent pas être sauvegardées ou copiées, mais doivent être détenues par l'abonné ou sous le contrôle d'une application de confiance approuvée par la PA de la GovCA du Bénin.

Les clés de signature privée sauvegardées de l'abonné ne doivent pas être stockées sous forme de texte intégral en dehors du module cryptographique. Le stockage doit assurer des contrôles de sécurité compatibles avec la protection assurée par le module cryptographique de l'abonné.

6.2.4.3 Sauvegarde des clés privées de gestion des clés de l'abonné

Les clés de gestion des clés d'abonnés peuvent être sauvegardées pour permettre la récupération des clés comme décrit dans la section **Erreur ! Source du renvoi introuvable.**.

Les clés de gestion des clés privées sauvegardées de l'abonné ne doivent pas être stockées en texte intégral en dehors du module cryptographique. Le stockage doit garantir des contrôles de sécurité compatibles avec la protection assurée par le module cryptographique de l'abonné.

6.2.4.4 Sauvegarde de la clé privée du CSS

Les clés privées CSS peuvent être sauvegardées. Si elles sont sauvegardées, toutes les copies doivent être comptabilisées et protégées de la même manière que l'original.

6.2.4.5 Sauvegarde des clés privées du dispositif

Les clés privées du dispositif peuvent être sauvegardées ou copiées, mais doivent être conservées sous le contrôle du DCH du dispositif ou d'un autre administrateur autorisé. Les clés privées sauvegardées ne doivent pas être stockées en texte intégral en dehors du module cryptographique. Le stockage doit garantir des contrôles de sécurité compatibles avec la protection assurée par le module cryptographique du dispositif.

6.2.5 Archives de clé privée

Les clés privées de l'abonné peuvent être archivées conformément aux dispositions des sections **Erreur ! Source du renvoi introuvable.** et **Erreur ! Source du renvoi introuvable.**.

6.2.6 Entrée de clé privée dans le module cryptographique

Les clés privées de la GovCA du Bénin peuvent être exportées du module cryptographique uniquement pour effectuer les procédures de sauvegarde des clés de la CA comme décrit dans la section **Erreur ! Source du renvoi introuvable.**. En aucune circonstance, la clé privée de la CA ne doit exister en texte intégral en dehors du module cryptographique.

Toutes les autres clés doivent être générées par et dans un module cryptographique. Dans le cas où une clé privée doit être transférée d'un module cryptographique à un autre, la clé privée doit être cryptée pendant le transfert ; les clés privées ne doivent jamais exister en texte intégral en dehors des limites du module cryptographique.

Les clés privées ou symétriques utilisées pour crypter d'autres clés privées en vue du transfert doivent être protégées contre toute divulgation.

6.2.7 Stockage de clé privée sur module cryptographique

Les clés privées sont stockées sur des modules cryptographiques conformément à la section **Erreur ! Source du renvoi introuvable.**.

6.2.8 Méthode d'activation des clés privées

Pour la clé de signature de la GovCA et du CSS du Bénin, l'activation nécessite un contrôle multipartite comme indiqué dans la section **Erreur ! Source du renvoi introuvable.**. Les moyens acceptables d'authentification au module cryptographique comprennent, sans toutefois s'y limiter, les phrases de passe, les codes PIN ou les biométries. Lorsque des phrases de passe ou des codes PIN sont utilisés, ils doivent comporter au moins douze (12) caractères.

L'abonné doit être authentifié auprès du module cryptographique avant l'activation de toute clé privée. Les moyens d'authentification acceptables comprennent, sans s'y limiter, les phrases de passe, les codes PIN ou les biométries. Lorsque des phrases de passe ou des codes PIN sont utilisés, ils doivent comporter un minimum de caractères conformément au tableau suivant.

Tableau 7 – Nombre minimum de caractères requis pour activer les clés privées de l'abonné

Niveau d'Assurance	Nombre de Caractères Minimum
Basic	Software cryptographic module: 5 characters

Niveau d'Assurance	Nombre de Caractères Minimum
	Hardware cryptographic module: 4 characters
Medium	Software cryptographic module: 5 characters Hardware cryptographic module: 5 characters
High	Hardware cryptographic module: 5 characters

La saisie des données d'activation doit être protégée contre la divulgation (c'est-à-dire que les données ne doivent pas être affichées pendant leur saisie).

6.2.9 Méthodes de désactivation de clé privée

Les modules cryptographiques qui ont été activés ne doivent pas être disponibles pour un accès non autorisé. Après utilisation, le module cryptographique doit être désactivé, par exemple via une procédure de déconnexion manuelle, ou automatiquement après une période d'inactivité telle que définie dans la CPS de la GovCA du Bénin et la RPS de la LRA partenaire. Les modules cryptographiques du dispositif de la CA doivent être retirés et stockés dans un conteneur sécurisé lorsqu'ils ne sont pas utilisés.

6.2.10 Méthode de destruction des clés de signature privées

Les personnes occupant des rôles de confiance doivent détruire les clés de signature privées de la CA, la RA et du serveur CSS lorsqu'elles ne sont plus utiles. Les clés de signature privées des abonnés sont détruites lorsqu'elles ne sont plus nécessaires, ou lorsque les certificats auxquels elles correspondent expirent ou sont révoqués. Pour les modules cryptographiques logiciels, il peut s'agir de l'écrasement des données. Pour les modules cryptographiques du dispositif matériel, il s'agira probablement d'exécuter une commande de "mise à zéro". La destruction physique du dispositif n'est pas nécessaire.

6.3 AUTRES ASPECTS DE LA GESTION DE PAIRES DE CLÉ

6.3.1 Archives à clé publique

La clé publique est archivée comme faisant partie de l'archive des certificats.

6.3.2 Périodes d'utilisation des clés publiques et privées

La GovCA du Bénin limite l'utilisation de ses clés privées à un maximum de 123 mois pour les certificats d'abonnés et la signature des CRL.

Les certificats CSS de haute assurance qui fournissent un statut de révocation ont une période de validité maximale de **1 an**.

Les certificats CSS d'assurance moyenne qui fournissent un statut de révocation ont une période de validité maximale de **2 ans**.

Les certificats d'assurance de base CSS qui fournissent un statut de révocation ont une période de validité maximale de **3 ans**.

Les clés privées de signature des abonnés et les certificats stockés sur les cartes NID ont une durée de validité maximale de **5 ans**.

Les clés privées et les certificats de signature de tous les autres abonnés ont une durée de validité maximale de **3 ans**.

Les certificats de gestion de clé d'abonné ont une durée de validité maximale de 3 ans ; l'utilisation des clés privées de gestion de clé d'abonné est sans restriction.

La GovCA ne doit délivrer de certificats d'abonnés dont la date d'expiration est supérieure à celle de ses propres certificats et clés publiques.

6.4 DONNÉES D'ACTIVATION

6.4.1 Génération et Installation des Données d'Activation

Les données d'activation utilisées pour déverrouiller les clés privées de la GovCA, de la RA, du CMS, du CSS ou de l'abonné du Bénin, conjointement avec tout autre contrôle d'accès, doivent avoir un niveau de résistance approprié pour les clés ou les données à protéger. Si les données d'activation doivent être transmises, elles doivent l'être par un canal protégé de manière appropriée, et distinct dans le temps et dans l'espace du module cryptographique associé.

6.4.2 Protection des Données d'Activation

Les données utilisées pour déverrouiller les clés privées sont protégées contre toute divulgation par une combinaison de mécanismes de contrôle d'accès cryptographique et physique. Les données d'activation sont :

- Mémorisée
- De nature biométrique, ou
- enregistrée et sécurisée au niveau d'assurance associé à l'activation du module cryptographique, et ne doit pas être stocké avec le module cryptographique.

Le mécanisme de protection comprend un dispositif permettant de verrouiller temporairement le compte ou de mettre fin à l'application après un nombre prédéterminé de tentatives de connexion infructueuses, comme indiqué dans la CPS.

6.4.3 Autres Aspects des Données d'Activation

Les modules cryptographiques qui stockent les clés des abonnés doivent prévoir un mécanisme de verrouillage des clés privées.

6.5 LES CONTRÔLES DE SÉCURITÉ INFORMATIQUE

6.5.1 Exigences techniques spécifiques en matière de sécurité informatique

Pour la GovCA du Bénin, les fonctions de sécurité informatique énumérées ci-dessous sont requises. Ces fonctions peuvent être assurées par le système d'exploitation ou par une

combinaison de système d'exploitation, de logiciels et de protections physiques. La GovCA du Bénin et ses parties auxiliaires doivent inclure les fonctionnalités suivantes :

- Exiger des identifiants authentifiés ;
- Fournir un contrôle d'accès discrétionnaire ;
- Fournir une capacité d'audit de sécurité ;
- Restreindre le contrôle d'accès aux services de la GovCA du Bénin et aux rôles PKI ;
- Appliquer la séparation des taches pour les rôles du PKI ;
- Exiger l'identification et l'authentification des rôles du PKI et des identités associées ;
- Exiger la séparation ou interdire la réutilisation des objets pour la mémoire vive de la GovCA du Bénin ;
- Exiger l'utilisation de la cryptographie pour la session de communication et la sécurité de la base de données ;
- Archiver l'historique de la GovCA du Bénin et les données d'audit ;
- Exiger l'autotest des services liés à la sécurité de la GovCA du Bénin ;
- Exiger un moyen fiable pour l'identification des rôles de la PKI et des identités associées ;
- Exiger un mécanisme de récupération des clés et du système de la CA racine du Bénin ; et
- Appliquer les limites d'intégrité de domaine pour les processus critiques de sécurité.

Pour les parties de la GovCA du Bénin qui fonctionnent dans un VME, les fonctions de sécurité suivantes concernent également l'hyperviseur :

- Exiger des identifiants authentifiés ;
- Fournir un contrôle d'accès discrétionnaire ;
- Fournir une capacité d'audit de sécurité ;
- Appliquer la séparation des taches pour les rôles du PKI ;
- Exiger la séparation ou interdire la réutilisation des objets pour la mémoire vive de la CA ;
- Exiger l'utilisation de la cryptographie pour la session de communication et la sécurité de la base de données ;
- Archiver l'historique de la CA et les données d'audit ;
- Exiger l'autotest des services liés à la sécurité de la GovCA du Bénin ; et
- Appliquer les limites d'intégrité de domaine pour les processus critiques de sécurité.

Pour les CSS, les fonctions de sécurité informatique énumérées ci-dessous sont requises (dans une VME, ces fonctions sont applicables à la fois au VM et à l'hyperviseur) :

- Authentifier l'identité des utilisateurs avant d'autoriser l'accès au système ou aux applications ;
- Gérer les privilèges des utilisateurs afin de les limiter aux rôles qui leur sont assignés ;
- Appliquer les limites d'intégrité de domaine pour les processus critiques de sécurité ; et
- Prendre en charge la récupération après une défaillance de la clé ou du système.

Pour bureaux éloignés utilisés pour administrer les CA, les fonctions de sécurité informatique énumérées ci-dessous sont requises :

- Authentifier l'identité des utilisateurs avant d'autoriser l'accès au système ou aux applications ;
- Gérer les privilèges des utilisateurs afin de les limiter aux rôles qui leur sont assignés ;
- Créer et archiver les enregistrements de vérification pour toutes les transactions ; (voir la Section **Erreur ! Source du renvoi introuvable.**)
- Appliquer les limites d'intégrité de domaine pour les processus critiques de sécurité ; et
- Prendre en charge de la récupération après une défaillance de la clé ou du système.

Toutes les communications entre toute personne jouant un rôle de confiance de la PKI et la CA doivent être authentifiées et protégées contre toute modification.

6.5.2 Évaluation de la sécurité informatique

Aucune stipulation.

6.6 CONTRÔLES TECHNIQUES DU CYCLE DE VIE

6.6.1 Contrôles de développement du système

Les contrôles de développement du système pour la GovCA du Bénin sont les suivants :

- Pour le logiciel commercial standard, le logiciel doit être conçu et développé selon une méthodologie de développement formelle et documentée.
- Pour le dispositif et le logiciel développés spécifiquement pour une CA donnée, le demandeur doit démontrer que les exigences de sécurité ont été satisfaites par une combinaison de vérification et de validation de logiciel, d'une approche de développement structurée et d'un environnement de développement contrôlé.
- Lorsqu'un logiciel libre a été utilisé, le demandeur doit démontrer que les exigences de sécurité ont été satisfaites par la vérification et la validation du logiciel et par une gestion structurée du développement et du cycle de vie.

Le dispositif et le logiciel acquis pour faire fonctionner la CA doivent être achetés et expédiés de manière à réduire la probabilité qu'un élément particulier ait été altéré.

- Le logiciel et dispositif matériel de la CA, y compris l'hyperviseur VME, doivent être consacrés à l'exploitation et au soutien de la GovCA (c.-à-d. les systèmes et services dédiés à la délivrance et à la gestion des certificats). Aucune autre application, dispositif

matériel, connexion réseau ni composant logiciel ne faisant pas partie des activités de la CA ne doivent être installés. Dans une VME, un seul hyperviseur peut prendre en charge plusieurs CA et leurs systèmes de soutien, à condition que tous les systèmes aient des contrôles de sécurité comparables et soient dédiés au soutien de la CA.

- Dans une VME, tous les systèmes de la VM doivent fonctionner dans la même zone de sécurité que la CA.
- Il faut prendre les précautions nécessaires pour empêcher le chargement de logiciel malveillant sur l'équipement de la CA. Lors de la première utilisation, le dispositif matériel et le logiciel doivent être analysés premièrement à la recherche de codes malveillants et périodiquement par la suite.
- Les mises à jour du dispositif matériel et du logiciel doivent être achetées ou développées de la même manière que le matériel d'origine et être installées par un personnel de confiance et formé de façon spécifique.

6.6.2 Contrôles de gestion de la sécurité

La configuration du système de la GovCA du Bénin ainsi que les modifications et les mises à jour éventuelles doivent être documentées et contrôlées. Un mécanisme de détection des modifications non autorisées du logiciel ou de la configuration du système de la GovCA du Bénin doit être mis en place. Une méthodologie formelle de gestion de la configuration doit être utilisée pour l'installation et la maintenance continue du système de la GovCA du Bénin. Lors de son premier chargement le logiciel de la GovCA du Bénin doit être vérifié comme étant celui fourni par le vendeur, sans modifications, et être la version destinée à être utilisée.

6.6.3 Contrôles de sécurité du cycle de vie

Aucune stipulation.

6.7 CONTRÔLES DE SÉCURITÉ DU RÉSEAU

La GovCA, les RA, les CMS, les registres, les bureaux à distance utilisés pour administrer les CA et les services CSS doivent employer des contrôles de sécurité de réseau appropriés. Les équipements de réseau doivent désactiver les ports et services de réseau inutilisés. Tout logiciel de réseau présent doit être nécessaire au fonctionnement de l'équipement. La GovCA doit établir une liaison avec un poste de travail distant utilisé afin de gérer la CA, uniquement après une authentification réussie du poste de travail à distance à un niveau d'assurance correspondant à celui de la CA.

6.8 HORODATAGE

Les temps indiqués doivent être exacts à trois minutes près et être exprimés en temps universel coordonné (UTC). Des procédures électroniques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les ajustements de l'horloge sont des éléments vérifiables, voire la section **Erreur ! Source du renvoi introuvable.**.

Les politiques définies dans cette section sont conformes à l'article 300 du Code du Numérique du Gouvernement du Bénin.

7. CERTIFICATS ET PROFILS CRL

7.1 PROFIL DE CERTIFICAT

7.1.1 Numéros de version

LA GovCA du Bénin doit émettre des certificats X.509 v3 (remplir le champ de la version avec le nombre entier "2").

7.1.2 Extensions de Certificats

L'utilisation des extensions de certificats standards doit être conforme à la RFC 5280.

Les certificats délivrés par la GovCA du Bénin ne doivent pas inclure les extensions privées critiques.

Les certificats d'abonnés délivrés par la GovCA du Bénin peuvent inclure des extensions privées critiques tant que l'interopérabilité au sein de la communauté d'utilisation n'est pas compromise.

7.1.3 Identificateurs d'Objets d'Algorithme

Les certificats délivrés par la GovCA du Bénin doivent identifier l'algorithme de signature en utilisant l'un des OID suivants :

Tableau 8 – Identificateurs d'Objets d'Algorithme de Signature

Identificateur de l'algorithme de Signature	OID
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }

Lorsque les certificats sont signés en utilisant la RSA avec un tampon PSS, l'OID est indépendant de l'algorithme de hachage ; l'algorithme de hachage est spécifié comme un paramètre. Les signatures RSA avec tamponnement PSS peuvent être utilisées avec les algorithmes de hachage et les OID spécifiés ci-dessous :

Tableau 9 – RSA with PSS padding Hash Algorithm OIDs

Identificateur de l'algorithme de Signature	OID
id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Les certificats délivrés par la GovCA du Bénin doivent identifier l'algorithme cryptographique associé à la clé publique concernée en utilisant l'un des OID suivants :

Tableau 10 – Algorithme cryptographique associé à la clé publique du sujet

Identificateur de l'algorithme de Signature	OID
id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dhpublicnumber	{ iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1 }

7.1.4 Formulaires de nom

Au besoin, tel qu'indiqué à la section 3.1.1, les champs d'objet et émetteur du certificat de base doivent être remplis avec un nom distinctif X.500. Les noms distinctifs doivent être composés de types d'attributs standards, tels que ceux identifiés dans RFC 5280.

7.1.5 Contraintes liées aux noms

Les CA peuvent faire valoir des contraintes de nom dans les certificats de la CA.

7.1.6 Identificateur d'objet de politique de certification

Tous les certificats délivrés par la GovCA du Bénin doivent comporter une extension des politiques de certification affirmant le ou les OID appropriés au niveau d'assurance avec lequel ils ont été délivrés Voir la section 1.2 pour les OID spécifiques.

7.1.7 Utilisation de l'extension des Contraintes de Politique

Les CA peuvent imposer des contraintes de politique dans les certificats des CA. Lorsque cette extension apparaît, au moins l'un des éléments suivants doit être présent : requireExplicitPolicy ou inhibitPolicyMapping. Lorsqu'elle est présente, cette extension doit être marquée comme non-critique*, pour prendre en charge les applications existantes qui ne peuvent pas traiter les PolicyConstraints. Pour les certificats de la CA subordonnés inhibitPolicyMappings, les skip certs seront définis à 0.

7.1.8 Syntaxe et sémantique des Qualificatifs de Politique

Les certificats délivrés par la GovCA du Bénin peuvent contenir des qualificatifs de politique identifiés dans RFC 5280.

7.1.9 P Traitement de la sémantique pour l'extension de la politique de certification des certificats d'importance critique

Les certificats délivrés par la GovCA du Bénin ne doivent pas comporter d'extension des politiques de certificats critiques.

7.2 PROFIL DE LA CRL

7.2.1 Numéros de version

La GovCA du Bénin émettra la version deux (2) des CRL X.509.

7.2.2 Extensions d'Entrée des CRL

La GovCA du Bénin doit indiquer dans la CPS l'utilisation de toutes les extensions supportées par la CA, ses RA et ses entités finales.

7.3 PROFIL OCSP

Les CSS opérant dans le cadre de cette politique doivent signer les réponses en utilisant les algorithmes désignés pour la signature des CRL.

7.3.1 Numéro(s) de version

Les CSS opérant dans le cadre de cette politique doivent utiliser la version 1 de l'OCSP.

7.3.2 Extensions de l'OCSP

L'OA de la GovCA du Bénin doit définir un profil OCSP qui documente toutes extensions relevées et leur niveau d'importance critique. Tous les logiciels PKI doivent traiter correctement toutes les extensions OCSP identifiées dans le profil OCSP. La GovCA doit indiquer dans sa CPS l'utilisation de toutes les extensions supportées par la CA, les RA et les entités finales.

8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

La GovCA-OA du Bénin doit disposer d'un mécanisme d'audit de conformité pour s'assurer que les exigences de la présente et le CPS de la GovCA du Bénin sont mises en œuvre et appliquées.

Cette spécification n'impose aucune méthode d'évaluation particulière.

Les politiques définies dans cette section sont conformes aux articles 317 et 319 du Code du Numérique du Gouvernement du Bénin.

8.1 FRÉQUENCE DE L'AUDITS DE CONFORMITÉ

Au moins une fois par an, la GovCA du Bénin, les CMS, les CSS et les RA doivent faire objet périodique d'un audit de conformité.

La GovCA du Bénin a le droit d'exiger des audits de conformité ou des inspections périodiques et apériodiques des opérations de la RA et de la LRA afin de confirmer que les entités subordonnées opèrent conformément aux pratiques et procédures de sécurité décrites dans leur CPS respectif et dans le RPS partenaire approuvé. La PA de la GovCA du Bénin doit indiquer la raison de tout audit de conformité apériodique.

Le CA-PA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin ont le droit d'exiger des audits de conformité ou des inspections périodiques et apériodiques des opérations de la GovCA afin de confirmer que la PKI opère conformément aux pratiques et procédures de sécurité décrites dans la présent CP et la CPS de la GovCA du Bénin, la CA CP racine du Bénin et le Code du Numérique du gouvernement du Bénin. La CA-PA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin doivent indiquer le motif de tout audit de conformité apériodique.

8.2 IDENTITÉ/QUALIFICATIONS DE L'AUDITEUR

L'auditeur de conformité doit démontrer sa compétence dans le domaine des audits de conformité. Au moment de l'audit, l'auditeur de conformité de la GovCA du Bénin doit avoir une connaissance approfondie des exigences que la PA de la GovCA du Bénin impose à la délivrance et à la gestion des certificats de la GovCA du Bénin. L'auditeur de conformité doit effectuer ces audits de conformité dans le cadre d'une activité commerciale régulière et continue.

Pour le gouvernement du Bénin, en plus des exigences précédentes, l'auditeur doit être un auditeur de système d'information certifié (CISA), de préférence un spécialiste expérimenté en sécurité informatique, et un spécialiste en matière de PKI qui peut apporter sa contribution concernant les risques acceptables, les stratégies d'atténuation et les meilleures pratiques du secteur.

NB : L'auditeur de conformité n'a pas besoin de détenir une certification CISA lorsque la GovCA est hébergée par l'EDC.

8.3 RELATION ENTRE L'AUDITEUR ET LA PARTIE AUDITÉE

Pour la GovCA du Bénin, l'auditeur de conformité doit soit être un cabinet privé, un indépendant de l'entité auditée, soit être suffisamment détaché de l'OA de la GovCA et des partenaires LRA afin de fournir une évaluation impartiale et indépendante. Un exemple de cette hypothèse peut être un inspecteur général d'un ministère ou d'une agence du gouvernement du Bénin. Pour des

raisons d'objectivité et d'indépendance, l'auditeur de conformité peut ne pas avoir servi l'entité dans la mise en place ou le maintien de la structure de la GovCA du Bénin, des CPS de la GovCA du Bénin ou des RPS de la LRA Partenaire.

Le CA-PA racine du Bénin et l'Organe de Contrôle du Gouvernement du Bénin doivent déterminer si un auditeur de conformité répond à cette exigence.

Si l'auditeur sélectionné ou le rapport de conformité produit par l'auditeur de conformité ne satisfait pas pleinement le CA-PA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin, la PA de la GovCA du Bénin pourrait avoir à refaire son audit de CA.

8.4 SUJETS COUVERTS PAR L'AUDIT DE CONFORMITÉ

The compliance audit of the Benin GovCA shall verify that:

- L'OA de la GovCA du Bénin est en train d'appliquer toutes les dispositions d'une CPS approuvée par la PA de la GovCA du Bénin en accord avec cette présente CP.
- L'OA de la GovCA du Bénin est en train d'appliquer les dispositions pertinentes des protocoles d'accord (MOA) conclus entre la PA de la GovCA du Bénin et la CA-PA de la racine du Bénin ;
- La RA de la GovCA du Bénin est en train d'appliquer toutes les dispositions d'une CPS approuvée par la PA de la GovCA du Bénin en accord avec cette CP ;
- La GovCA-OA du Bénin est en train d'appliquer les dispositions pertinentes du Code du Numérique du gouvernement du Bénin ; et
- La LRA partenaire du Bénin est en train d'appliquer toutes les dispositions d'un RPS approuvé par la PA de la GovCA du Bénin en accord avec cette PC.

Les composantes autres que les CA peuvent être contrôlées dans leur intégralité ou en utilisant un échantillon représentatif. Si l'auditeur de conformité utilise l'échantillonnage statistique, toutes les composantes de la PKI, les gestionnaires des composantes de la PKI et les opérateurs doivent être pris en compte dans l'échantillon. Les échantillons doivent varier sur une base annuelle.

Un audit de conformité complet pour la GovCA du Bénin couvre tous les aspects dans le cadre du champ d'application identifié ci-dessus.

8.5 LES MESURES PRISES A LA SUITE D'UNE CARENCE

Lorsque l'auditeur de conformité constate la non-conformité entre la conception, l'exploitation ou la maintenance de la GovCA du Bénin et les exigences de la présente CP, des protocoles d'accord (MOA) ou de la CPS et RPS applicables, les actions suivantes doivent être effectuées :

- L'auditeur de conformité doit documenter la non-conformité et en fournir une copie à l'OA de la GovCA du Bénin ;
- L'OA de la GovCA du Bénin fournira une copie de la documentation relative aux non-conformités à la PA de la GovCA du Bénin, à la RA de la GovCA du Bénin, à la CA-PA racine du Bénin et à l'Organe de contrôle du gouvernement du Bénin **dans les 3 jours ouvrables** suivant la fin de l'exercice d'audit.

- L'OA de la GovCA du Bénin et la RA de la GovCA du Bénin feront part des conclusions et des mesures correctives à la PA de la GovCA du Bénin, et cette dernière fournira les conclusions et les informations relative à la mesure corrective à la CA-PA racine du Bénin et à l'Organe de contrôle du gouvernement du Bénin.
- L'OA de la GovCA du Bénin détermine quelles autres notifications ou actions sont nécessaires pour satisfaire aux exigences de la présente CP, de la CPS et des MOA, puis procède à ces notifications et prend des mesures sans délai.
- La RA de la GovCA du Bénin détermine quelles autres notifications ou actions sont nécessaires pour répondre aux exigences du (des) RPS de la LRA partenaire, puis procède à ces notifications et prend des mesures sans délai.
- En fonction de la nature et de la gravité de la discordance, et de la rapidité avec laquelle elle peut être corrigée, la PA de la GovCA du Bénin peut demander à l'OA de la GovCA du Bénin et à la RA de la GovCA du Bénin de prendre si nécessaire des mesures supplémentaires, y compris l'arrêt temporaire des activités de la GovCA du Bénin ou l'arrêt de la délivrance et de la gestion des certificats par une LRA partenaire.
- En cas de non-conformité à la CP de la CA racine du Bénin, à la CP de la GovCA du Bénin, à la CPS de la GovCA du Bénin, à la RPS de la LRA partenaire ou au Code du Numérique du gouvernement du Bénin, l'Organe de contrôle du gouvernement du Bénin peut retirer la licence de la GovCA du Bénin et le statut de "qualifié".

Lorsque la PA de la GovCA du Bénin, la PA de la CA racine du Bénin et l'Organe de contrôle du gouvernement du Bénin reçoivent un rapport d'insuffisance d'audit de la part de l'OA de la GovCA du Bénin, la PA de la GovCA du Bénin et la CA-PA racine du Bénin, de concert avec l'Autorité nationale de la politique de certification du Bénin, sont autorisés à :

- Demander à la LRA partenaire et si nécessaire à la CA-OA du Bénin de prendre des mesures supplémentaires pour protéger le niveau de confiance dans l'infrastructure ;
- Arrêter l'émission de certificats par la LRA partenaire ; et
- Obliger la LRA partenaire à informer immédiatement les détenteurs de certificats qu'elle a émis, de leur non-conformité aux dispositions de la CP de la GovCA du Bénin et du Code du Numérique du gouvernement du Bénin.

Lorsque l'Organe de contrôle du gouvernement du Bénin demande à la LRA partenaire de corriger une violation des exigences de la CP de la GovCA du Bénin, de la CPS de la GovCA et de la RPS de la LRA partenaire et des stipulations du Code du Numérique du gouvernement du Bénin et que le partenaire n'agit pas en conséquence après un délai raisonnable fixé par l'Organe de contrôle du gouvernement du Bénin, ce dernier a la possibilité, en tenant compte de l'étendue, de la durée et des conséquences de la violation, de retirer le statut "qualifié" de la LRA partenaire, et d'informer la PA de la GovCA du Bénin pour qu'il révoque le certificat de la LRA et délivre un nouveau CRL. L'Organe de contrôle du gouvernement du Bénin doit également informer la LRA partenaire du retrait de son statut de "qualifié".

Les politiques définies dans cette section sont conformes aux articles 320 et 321 du Code du Numérique du Gouvernement du Bénin.

8.6 COMMUNICATION DU RÉSULTAT

Sur une base annuelle, la PA de la GovCA du Bénin soumet un dossier d'examen annuel à la CA-PA racine du Bénin et à l'Organe de contrôle du gouvernement du Bénin **dans les 3 jours** suivant la réception du rapport de conformité par l'auditeur. Ce dossier doit comprendre une déclaration de la PA de la GovCA du Bénin selon laquelle toutes les composantes de la PKI ont été auditées ; y compris toutes les composantes qui peuvent être gérées et exploitées séparément, comme les services de la LRA partenaire. Le dossier doit identifier les versions de la CP, de la CPS et de la RPS de la LRA partenaire utilisées au cours de l'évaluation. En outre, les résultats sont communiqués au besoin, comme indiqué à la section **Erreur ! Source du renvoi introuvable.** ci-dessus.

9. AUTRES AFFAIRES ET QUESTIONS JURIDIQUES

Les détails concernant les affaires et les questions juridiques de la GovCA sont présentés dans des documents séparés.

9.1 TARIFS

La PA de la GovCA du Bénin se réserve le droit de facturer une redevance à chaque organisme autorisé à agir en tant que LRA et autorisé à délivrer des certificats et aux abonnés afin de soutenir les opérations de la GovCA du Bénin.

Les frais de certificat sont publiés sur le site web officiel de la GovCA. (http://govca.bj)

9.1.1 Frais d'Émission/de Renouvellement de Certificat

La GovCA peut facturer des frais pour l'émission de certificats conformément à la liste de prix respective pour les services de certificats numériques publiée sur le site web officiel de la GovCA (http://govca.bj) ou mise à disposition sur requête du demandeur.

9.1.2 Droits d'accès au certificat

L'accès aux certificats délivrés par la GovCA est gratuit.

9.1.3 Frais de révocation ou d'accès aux informations sur le statut

Des frais peuvent être perçus pour l'utilisation du service CSS.

9.1.4 Tarifs pour autres services

Des frais peuvent être perçus pour l'utilisation du service de l'Autorité d'Horodatage (TSA).

9.1.5 Politique de Remboursement

Aucune stipulation.

9.2 RESPONSABILITÉ FINANCIÈRE

Cette CP ne contient aucune limite sur l'utilisation des certificats émis par la GovCA du Bénin. Les entités qui agissent en tant que parties utilisatrices doivent plutôt déterminer au besoin les limites financières qu'elles souhaitent imposer pour les certificats utilisés afin de conclure une transaction.

9.2.1 Couverture d'assurance

Aucune stipulation.

9.2.2 Autres Actifs

Aucune stipulation.

9.2.3 Couverture d'assurance/garantie pour les entités finales

Aucune stipulation.

9.3 CONFIDENTIALITÉ DES INFORMATIONS COMMERCIALES

Les informations de la GovCA du Bénin qui ne nécessitent pas de protection sont rendues publiques. L'accès du public aux informations organisationnelles est déterminé par l'organisation concernée.

L'accès de la PA de la GovCA du Bénin aux données de la LRA partenaire sera abordé dans le protocole d'accord avec cette LRA partenaire.

9.3.1 Portée de la confidentialité des informations

Les informations confidentielles de la GovCA comprennent, entre autres, les données sur les abonnés, les informations sur les parties utilisatrices, les informations sur les transactions commerciales, le plan d'affaires de la GovCA et les informations sur les ventes de la GovCA.

9.3.2 Informations ne relevant pas de la catégorie des informations confidentielles

Toute information qui est publique ne doit pas être confidentielle.

9.3.3 Responsabilité pour la protection des informations confidentielles

La GovCA du Bénin est chargée de prendre toutes les mesures nécessaires pour protéger les informations identifiées comme confidentielles afin de se conformer aux lois et règlements du Bénin**.**

9.4 CONFIDENTIALITÉ DES INFORMATIONS PERSONNELLES

Sans préjudice des dispositions du Livre V, l'OA de la GovCA du Bénin, la RA de la GovCA du Bénin ou une LRA partenaire qui délivre des certificats ne peut recueillir des données à caractère personnel que directement auprès de la personne concernée, avec le consentement explicite de celle-ci, et uniquement dans la mesure où cela est nécessaire à la remise et à la conservation du certificat.

Les données qui leur sont transmises, en particulier les données à caractère personnel, ne peuvent être collectées ou traitées à d'autres fins sans le consentement préalable et explicite de la personne concernée. Les LRA partenaires ne peuvent détenir, accéder et utiliser ces données que dans la mesure strictement nécessaire à l'exécution de leurs services.

Lorsque le titulaire du certificat utilise un pseudonyme et que la nécessité d'enquêtes policières ou judiciaires l'exige, l'OA de la GovCA du Bénin, la RA de la GovCA du Bénin ou la LRA partenaire qui a délivré le certificat communique à l'autorité compétente, à la police ou à l'autorité judiciaire, toute donnée et/ou information relative à l'identité du titulaire.

Les politiques définies dans cette section sont conformes à l'article 307 du Code du Numérique du Gouvernement du Bénin.

9.4.1 Privacy Plan

L'OA de la GovCA du Bénin, la RA de la GovCA du Bénin et la LRA partenaire doivent effectuer une évaluation des impacts sur la confidentialité. Si cela est jugé nécessaire, l'OA de la GovCA du Bénin, la RA de la GovCA du Bénin et la LRA partenaire disposent d'un plan de protection de confidentialité afin de protéger les informations d'identification personnelle contre

toute divulgation non autorisée. Le gouvernement du Bénin approuve les plans de protection de confidentialité.

NB : L'évaluation d'impact sur la confidentialité doit être effectuée par le personnel du gouvernement du Bénin. Le personnel d'EDC affecté au rôle de la CA-OA racine du Bénin ne procédera pas à une évaluation de l'impact sur la confidentialité tant que la CA racine du Bénin est hébergée et exploitée par EDC.

9.4.2 Informations considérées comme confidentielles

L'OA de la GovCA du Bénin, la RA de la GovCA du Bénin et la LRA partenaire doivent protéger toutes les informations d'identification personnelle des abonnés contre toute divulgation non autorisée. La GovCA du Bénin doit également protéger les informations d'identification personnelle pour les besoins du MOA contre toute divulgation non autorisée. Le contenu des archives gérées par l'OA de la GovCA du Bénin ne sera pas divulgué, sauf si la loi l'exige.

La collecte d'informations personnellement identifiables (PII) est limitée au minimum nécessaire pour valider l'identité de l'abonné. Il peut s'agir d'attributs qui relient la preuve d'identité à des sources faisant autorité. L'OA de la GovCA du Bénin, la RA de la GovCA du Bénin et la LRA partenaire doivent informer explicitement l'abonné de l'objectif de la collecte et de la conservation des PII nécessaires à la vérification de l'identité et des conséquences de la non-communication de ces informations. Les PII collectées à des fins de vérification de l'identité ne doivent pas être utilisées à d'autres fins.

9.4.3 Informations considérées comme non confidentielles

Les informations figurant dans les certificats de la GovCA du Bénin ne sont pas soumises aux protections décrites dans la section 9.4.2.

Les certificats qui contiennent le Numéro Personnel d'Identification (NPI) ou l'Identifiant Fiscal Unique (IFU) ou le numéro de résident du Bénin dans le champ sujet ou l'extension du nom alternatif du sujet ne doivent pas être distribués via des répertoires accessibles au public (exemple LDAP, HTTP).

9.4.4 Responsabilité de la protection des informations confidentielles

Les informations sensibles doivent être conservées en toute sécurité et ne peuvent être divulguées que conformément aux autres dispositions de la section **Erreur ! Source du renvoi introuvable.**.

Toutes les informations recueillies dans le cadre du processus de vérification de l'identité sont protégées afin de garantir la confidentialité et l'intégrité. Si la GovCA du Bénin met fin à ses activités, il lui incombe d'éliminer ou de détruire les informations sensibles, y compris les PII, de manière sûre, et de maintenir sa protection contre tout accès non autorisé jusqu'à leur destruction.

9.4.5 Avis et consentement pour l'utilisation des Informations confidentielles

L'OA de la GovCA du Bénin, la RA de la GovCA du Bénin et la LRA partenaire ne sont pas tenus de fournir un avis ou d'obtenir le consentement de l'abonné afin de divulguer des informations confidentielles conformément aux dispositions de l'article **Erreur ! Source du renvoi introuvable.**.

9.4.6 Divulgation en vertu de Procédure Judiciaire/Administratif

L'OA de la GovCA du Bénin, la RA de la GovCA du Bénin et la LRA partenaire ne doivent pas divulguer d'informations confidentielles à un tiers, sauf si cela est autorisé par la présente politique, requis par la loi, une règle ou un règlement du gouvernement, ou une décision d'un tribunal compétent.

9.4.7 Autres Circonstances de Divulgation d'Information

Aucune stipulation.

9.5 DROITS DE PROPRIÉTÉ INTELLECTUELLE

La GovCA du Bénin ne violera pas sciemment les droits de propriété intellectuelle détenus par des tiers.

9.6 REPRÉSENTATIONS ET GARANTIES

Les obligations décrites ci-dessous concernent la GovCA du Bénin, qui interagit avec la CA racine du Bénin. Les obligations qui s'appliquent à la GovCA du Bénin concernent ses activités d'émettrices de certificats. En outre, les obligations se focalisent sur les obligations de la GovCA du Bénin qui affectent l'interopérabilité avec la CA racine du Bénin. Ainsi, lorsque les obligations comprennent, par exemple, un examen (ou un audit) par la PA de la GovCA du Bénin ou un autre organisme du fonctionnement de la GovCA du Bénin, l'objectif de cet examen concerne l'interopérabilité en utilisant la CA racine du Bénin, et la question de savoir si la GovCA du Bénin se conforme au protocole d'accord (MOA).

9.6.1 Représentations et Garanties de la CA

Les certificats de la GovCA du Bénin sont délivrés et révoqués à l'unique discrétion de la PA de la GovCA du Bénin. Tout examen effectué par la GovCa-CP du Bénin est à l'usage de la GovCa-CP du Bénin et de la CA-PA racine du Bénin afin de déterminer si l'interopérabilité est possible ou non et, si possible, dans quelle mesure la politique de certification de la GovCa du Bénin correspond à la politique de la CA racine du Bénin.

9.6.2 Représentations et Garanties de la RA

Une RA de la GovCA du Bénin et une LRA partenaire exerçant des fonctions d'enregistrement telles décrites dans la présente politique doit se conformer aux stipulations de cette politique, et se conformer à une CPS et éventuellement à un RPS approuvé par la GovCA PA du Bénin afin d'être utilisé avec cette politique. Une RA de la GovCA du Bénin ou une LRA partenaire qui est jugée avoir agi d'une manière incompatible avec ces obligations est sujette à la révocation des responsabilités de la RA ou de la LRA.

Une GovCA RA du Bénin ou une LRA partenaire soutenant cette politique doit se conformer aux stipulations du présent document, notamment :

- Maintenir ses opérations en conformité avec les exigences de la CPS approuvée et, s'il y a lieu, de la RPS.

- N'inclure que des informations valables et appropriées dans les demandes de certificat, et conserver la preuve qu'une diligence raisonnable a été exercée pour valider les informations contenues dans le certificat.
- Veiller à ce que des obligations soient imposées aux abonnés conformément à la section **Erreur ! Source du renvoi introuvable.**, et que les abonnés soient informés des conséquences du non-respect de ces obligations.

9.6.3 Représentations et garanties de l'abonné

Pour un niveau d'assurance élevé, un abonné est tenu de signer un document contenant les exigences auxquelles il doit satisfaire en ce qui concerne la protection de la clé privée et l'utilisation du certificat avant de se voir délivrer le certificat. Pour les niveaux d'assurance de base et moyen, l'abonné ou le DCH doit reconnaître ses obligations en matière de protection de la clé privée et de l'utilisation du certificat avant de recevoir le certificat.

Les abonnés ou le DCH de la GovCA du Bénin s'engagent à :

- Se présenter de manière précise dans toutes les communications avec les autorités de la PKI ;
- Protéger leurs clés privées en tout temps, conformément à la présente politique, comme le stipulent leurs accords d'acceptation de certificats et leurs procédures locales ;
- Aviser rapidement la GovCA du Bénin en cas de suspicion de perte ou de compromission de leurs clés privées. Cette notification doit être faite directement ou indirectement par le biais de mécanismes compatibles avec les CPS de la GovCA du Bénin et les RPS de la LRA partenaire ;
- Lorsqu'un certificat est expiré ou a été révoqué, l'abonné doit cesser d'utiliser les certificats expirés ou révoqués ; et
- Respecter toutes les conditions et restrictions imposées sur l'utilisation de leurs clés et certificats privés.

Les politiques de cette section sont conformes à l'article 316 du Code du Numérique du Gouvernement du Bénin.

9.6.4 Représentations et garanties des parties utilisatrices

Aucune.

9.6.5 Représentations et garanties des autres participants

Aucune.

9.7 RENONCIATION AUX GARANTIES

La GovCA du Bénin ne peut pas renoncer aux responsabilités décrites dans la présente CP.

9.8 LIMITES DE RESPONSABILITÉ

La GovCA ne peut être tenu responsable des dommages causés aux abonnés, aux parties utilisatrices ou à toute autre partie, résultant de ou liés à l'utilisation de certificats qui sont

révoqués, expirés, utilisés à des fins non autorisées, altérés, compromis ou faisant l'objet de fausses déclarations, d'actes trompeurs ou d'omissions.

9.9 INDEMNITÉS

Aucune stipulation.

9.10 CONDITION ET RÉSILIATION

9.10.1 CONDITION

Ce CP devient effectif lorsqu'il est approuvé par la PA de la GovCA du Bénin et la PA de la CA Racine du Bénin. La présente CP ne présente aucune condition particulière.

9.10.2 Résiliation

La résiliation de la présente CP est laissée à la discrétion de la PA de la GovCA du Bénin.

9.10.3 Date d'Effet de la Résiliation et de la Survie

Les exigences de la présente CP restent en vigueur jusqu'à la fin de la période d'archivage du dernier certificat délivré.

9.11 LES NOTIFICATIONS INDIVIDUELLES ET LES COMMUNICATIONS AVEC LES PARTICIPANTS

La PA de la GovCA du Bénin doit établir des procédures appropriées pour les communications avec sa RA de la GovCA ou sa LRA partenaire et la CA Racine du Bénin par le biais de contrats ou de protocoles d'accord, selon le cas.

Toute modification prévue de l'infrastructure susceptible d'affecter l'environnement opérationnel de la GovCA du Bénin doit être communiquée à la PA de la GovCA du Bénin et à la RA de la GovCA du Bénin ou à la LRA partenaire au moins deux semaines avant la mise en application, et tous les nouveaux artefacts (par exemple les nouveaux profils de certificats) produits à la suite de la modification doivent être fournis à la CA-PA racine du Bénin dans les 24 heures suivant la mise en application.

Pour toutes les autres communications, aucune stipulation.

9.12 AMENDEMENTS

9.12.1 Procédure d'Amendement

La PA de la GovCA du Bénin doit réexaminer la présente CP au moins une fois par an. Les corrections, mises à jour ou suggestions de modifications de cette CP doivent être communiquées à la CA-PA du Bénin et à l'Organe de contrôle du gouvernement du Bénin. Cette communication doit comprendre une description du changement, une justification du changement et les coordonnées de la personne qui demande le changement.

9.12.2 Mécanisme et Période de Notification

Les modifications proposées dans cette CP seront distribuées par voie électronique aux membres et observateurs de la PA de la GovCA du Bénin conformément à la présente CP.

9.12.3 Circonstances selon lesquelles l'OID doit être modifié

Les OID seront modifiés si la PA de la GovCA du Bénin détermine qu'une modification de la CP réduit le niveau d'assurance fourni.

9.13 CLAUSES DE RÈGLEMENT DE LITIGES

La PA de la GovCA du Bénin doit faciliter le règlement entre les entités lorsque des conflits surviennent à la suite de l'utilisation des certificats délivrés dans le cadre de cette politique.

9.14 LOI REGISSANT

La conception, la validité, l'exécution et la période d'effet des certificats délivrés en vertu de la présente CP à toutes fins doivent être régies par la législation (loi, jurisprudence ou règlement) du gouvernement du Bénin.

En cas de litige avec la GovCA du Bénin, la résolution se fera selon les termes du protocole d'accord (MOA).

9.15 RESPECT DE LA LOI REGISSANT

Le gouvernement du Bénin est tenu de se conformer à la loi en vigueur.

9.16 AUTRES PROVISIONS

S'il est déterminé qu'une section de la présente CP est incorrecte ou invalide, les autres sections de la présente CP restent en vigueur jusqu'à la mise à jour de la CP.

10. ACRONYMES ET DÉFINITIONS

10.1 LISTE DES DÉFINITIONS

Authority Revocation List : Il s'agit d'une liste des certificats croisés et des certificats racines des autorités de certification révoqués.

Activation Data : Ce sont les valeurs de données, autres que les clés, qui sont nécessaires au fonctionnement des modules cryptographiques et qui doivent être protégées (par exemple, un code PIN, une phrase de passe ou un partage de clé détenu manuellement)

Applicant : L'abonné est parfois aussi appelé "demandeur" après avoir fait une demande de certificat auprès d'une autorité de certification, mais ceci avant que la procédure de délivrance du certificat ne soit terminée.

Archive : Espace de Stockage à long terme, disposé physiquement dans un emplacement distinct.

Audit : Analyse et examen indépendants des dossiers et des activités afin d'évaluer la qualité des contrôles du système, de garantir la conformité avec les politiques et les procédures opérationnelles établies et de recommander les modifications nécessaires des contrôles, des politiques ou des procédures.

Bénin GovCA-OA : L'OA de la GovCA du Bénin est l'organisation choisie par la PA de la GovCA du Bénin pour être responsable du fonctionnement de la GovCA du Bénin.

Bénin GovCA-PA : La GovCA du Bénin est un organisme du gouvernement du Bénin chargé de définir, de mettre en œuvre et d'administrer les décisions politiques concernant les utilisations de la GovCA du Bénin.

CA Certificate : Un certificat pour une clé publique d'une CA, délivré par une autre CA.

CA Private Signing Key : La clé privée correspond à une clé publique figurant dans un certificat de la CA et est utilisée pour signer les certificats PKI.

Certificate : Il s'agit d'un enregistrement informatique ou un message électronique qui : identifie l'autorité de certification émettrice ainsi que le nom ou l'identité de l'abonné, contient la clé publique de l'abonné, énumère une période de validité, est signé numériquement par une CA et a le sens donné dans la présente CP et les normes applicables. Un certificat comprend non seulement les informations réelles qu'il contient, mais aussi tous les documents qui y sont expressément mentionnés ou incorporés.

Certificate Revocation List (CRL) : Une liste des certificats révoqués avant l'expiration de leur période de validité

Certification Authority (CA) : Une entité qui crée, émet, gère et révoque des certificats

Certificate Policy (CP) : C'est un ensemble de règles qui indiquent l'applicabilité d'un certificat à une communauté particulière et/ou à une catégorie d'application avec des exigences de sécurité communes. Par exemple, une CP donnée peut indiquer l'applicabilité d'un type de certificat à l'authentification de parties effectuant des transactions interentreprises pour le commerce de biens ou de services dans une fourchette de prix donnée.

Certification Practice Statement (CPS) : C'est une déclaration des pratiques qu'une CA emploie pour émettre, gérer, révoquer et renouveler ou recomposer les certificats.

Cross-Certificate : Il s'agit d'un certificat utilisé pour établir une relation de confiance entre deux Autorités de Certification.

Cryptographic module : C'est soit un logiciel, un dispositif ou un utilitaire qui génère des paires de clés, stocke des informations cryptographiques et/ou exécute des fonctions cryptographiques.

Digital Signature, Digitally Sign : C'est la transformation d'un document électronique par une personne utilisant une clé privée et une clé publique de chiffrement afin qu'une autre personne possédant le document transformé et la clé publique correspondante puisse déterminer avec précision si la transformation a été créée à l'aide de la clé privée correspondant à la clé publique et si le document a été modifié depuis que la transformation a été effectuée.

Distinguished Name (DN) : C'est l'identifiant unique d'un abonné pour qu'il puisse être localisé dans un répertoire selon la norme ITU/CCITT X.500 (par exemple, le DN d'un abonné peut contenir les attributs suivants : nom commun (cn), adresse électronique (mail), nom de l'organisation (o), unité organisationnelle (ou), localité (l), département (st) et pays (c).

End Entity : Un abonné et/ou une partie utilisatrice autorisée.

Issue Certificates, Issuance : L'acte effectué par une CA pour créer une liste de certificats dont la CA est "l'émettrice ", et pour informer le demandeur du contenu et du fait que le certificat est prêt et disponible pour acceptation.

Issuing Certification Authority (Issuing CA) : Dans le contexte d'un certificat particulier, la CA émettrice est la CA qui a délivré le certificat d'entité finale.

Key Generation : Le processus de création d'une paire de clés.

Key Pair : Il s'agit de deux clés mathématiquement liées (une clé privée et la clé publique correspondante), avec les propriétés suivantes :

- Une Clé peut crypter une communication uniquement capable d'être décryptée par l'autre Clé
- L'obtention ou la découverte d'une clé à partir de l'autre est irréalisable par calcul, en supposant des circonstances probables, notamment la disponibilité de texte crypté par l'une des clés.

Key Recovery Policy : Une politique de récupération de clé est une forme spécialisée de politique administrative axée sur la protection et la récupération de clés privées de gestion de clés (c'est-à-dire les clés de décryptage) gardées sous séquestre. Une politique de récupération de clés aborde tous les aspects associés au stockage et à la récupération des certificats de gestion de clés.

Key Recovery Practices Statement (KRPS) : Un énoncé des pratiques qu'un système de récupération de clés emploie pour protéger et récupérer les clés privées de gestion de clés, conformément à des exigences spécifiques (c'est-à-dire les exigences spécifiées dans le KRP).

Lightweight Directory Access Protocol (LDAP) : Un protocole client-serveur utilisé pour accéder aux services d'annuaire sur un réseau informatique.

Memorandum of Agreement (MOA) : Il s'agit d'un accord entre la CA-PA racine du Bénin et un partenaire (par exemple, la PA de la GovCA du Bénin) permettant l'interopérabilité entre la CA partenaire et la CA racine du Bénin.

Multi-Person Control : Surveillance et contrôle continus du matériel de contrôle positif à tout moment par un minimum de deux personnes autorisées, chacune étant capable de détecter les procédures incorrectes et/ou non autorisées en ce qui concerne la tâche à accomplir et chacune étant familiarisée avec les exigences de sécurité et de sûreté établies.

Object Identifier (OID) : L'identifiant alphanumérique ou numérique unique enregistré selon la norme d'enregistrement ISO pour faire référence à un objet ou à une classe d'objet spécifique. Dans la présente CP, ils sont utilisés pour identifier de manière unique les certificats délivrés en vertu de la présente CP et les algorithmes cryptographiques pris en charge.

Online Certificate Status Protocol (OCSP) : Protocole utilisé pour valider en temps réel le statut d'un certificat. Un répondeur OCSP est utilisé pour répondre aux demandes de statut de certificat et peut émettre une des trois réponses : Valide, Invalide ou Inconnu. Un répondeur OCSP répond aux demandes de statut de certificat en fonction des CRL qui lui sont fournies par les CA.

Operational Period : La durée de validité effective d'un certificat, qui commence au début de la période de validité et se termine à la première des deux dates suivantes :

- La fin de la période de validité indiquée dans le certificat, ou
- La date de révocation du certificat.

Partner CA : Il s'agit d'une CA qui agit au nom d'un partenaire (la GovCA du Bénin, par exemple), et qui est sous le contrôle opérationnel d'un partenaire. Le partenaire peut être une organisation, une société ou une communauté d'intérêts. Pour le gouvernement du Bénin, un partenaire peut être un ministère ou une agence, un élément subordonné d'un ministère ou une entité organisationnelle indépendante telle qu'une organisation du secteur privé qui est autorisée à faire partie de la PKI du gouvernement du Bénin et à recevoir un certificat croisé ou un certificat CA subordonné de la part de la GovCA du Bénin.

PKI Certificate : Il s'agit d'un certificat délivré en vertu de la présente CP.

Private Key : La clé sensible de la paire de clés est protégée par l'abonné et gardée secrète. La clé privée crée des signatures numériques ou décrypte des données préalablement chiffrées à l'aide de la clé publique correspondante.

Public Key : Il s'agit de la clé non sensible de la paire de clés divulguée par l'abonné qui détient la clé privée correspondante. La clé publique vérifie les signatures numériques créées à l'aide de la clé privée correspondante, ou chiffre les données destinées au décryptage avec la clé privée correspondante.

Public Key Cryptography : C'est un type de cryptographie également connu sous le nom de cryptographie asymétrique. Cette cryptographie utilise une paire de clés plutôt qu'une clé unique pour sécuriser l'authentification et/ou la confidentialité des données.

Public Key Infrastructure (PKI) : Il s'agit de l'architecture, la technologie, les pratiques et les procédures qui soutiennent le fonctionnement d'un système de sécurité utilisant des certificats et la cryptographie à clé publique.

Registration Authority (RA) : Il s'agit d'une personne, une organisation ou un processus chargé de vérifier l'identité d'un abonné ou d'un DCH.

Relying Party : Il s'agit du bénéficiaire d'un certificat qui agit sur la base de ce certificat et/ou de toute signature numérique vérifiée à l'aide de ce certificat.

Repository : Il s'agit d'un système en ligne géré par une CA pour le stockage et la récupération des certificats et d'autres informations relatives aux certificats, y compris les informations relatives à la validité ou à la révocation des certificats.

Revoke (a certificate) : C'est le fait d'invalider un certificat de manière permanente à partir d'un moment précis. La révocation comprend l'inscription du certificat dans un ensemble de certificats révoqués ou dans un autre répertoire ou base de données de certificats révoqués (par exemple, l'inclusion dans une CRL). Le système empêche également les utilisateurs d'accéder aux certificats révoqués une fois qu'ils sont connectés à l'infrastructure centrale.

Request For Comments (RFC) : Séries de documents utilisés comme principal moyen de communication des informations sur l'internet. Certains RFC sont désignés par l'IAB comme étant des normes standards d'Internet. La plupart des RFC documentent les spécifications des protocoles tels que Telnet et FTP.

Subject Certification Authority : Dans le contexte d'un certificat CA spécifique, la CA concernée est la CA dont la clé publique est certifiée dans le certificat (voir aussi l'Autorité de certification émettrice).

Subject Name : C'est le champ spécifique dans un certificat contenant le DN de l'abonné.

Subordinate CA : Dans une PKI hiérarchique, une CA dont la clé de signature de certificat est certifiée par une autre CA et dont les activités sont limitées par cette autre CA. (Voir CA hiérarchique).

Subscriber : Un titulaire de certificat qui se fait délivrer un certificat.

Subscriber Agreement : Un accord entre une CA et un abonné qui établit les droits et les responsabilités des parties concernant la délivrance et la gestion des certificats.

Token un module cryptographique composé d'un objet matériel (par exemple une « carte à puce »), souvent avec une mémoire et une micro puce.

Trusted Agent : Entité autorisée à agir en tant que représentant d'une entité pour confirmer l'identification de l'abonné pendant le processus d'enregistrement. Les agents de confiance n'ont pas d'interfaces automatisées avec les autorités de certification.

Trusted Role : L'exécution de ces rôles exige le respect de la politique et des procédures pour prévenir l'introduction de problèmes de sécurité. Les fonctions des Rôles de confiance constituent la base de la confiance pour l'ensemble du système PKI.

Validity Period : C'est la durée de validité prévue d'un certificat, qui commence à la date de délivrance (date « Valable du » ou « d'Activation ») et se termine à la première des deux dates suivantes : la date d'expiration indiquée dans le certificat (date "Valable jusqu'au" ou "d'Expiration") ou la date de révocation indiquée dans la liste de révocation spécifiée comme point de distribution de la CRL dans le certificat.

Virtual Machine Environment (VME) : Une émulation d'un système informatique (dans ce cas, une CA) qui fournit la fonctionnalité d'une machine physique dans un environnement indépendant de la plate-forme. Elle se compose d'un hôte (machine virtuelle) et d'un noyau d'isolation (hyperviseur) et fournit les fonctionnalités nécessaires à l'exécution de systèmes d'exploitation entiers.

X.500 : Une série de normes de réseaux informatiques couvrant les services d'annuaires électroniques. Ces services comprennent le Directory Access Protocol (DAP), le Directory System Protocol (DSP), le Directory Information Shadowing Protocol (DISP) et le Directory Operational Bindings Management Protocol (DOP).

X.509 : Une norme de l'Union internationale des télécommunications - Secteur de la normalisation des télécommunications (ITU-T) pour l'infrastructure à clé publique qui spécifie les formats standards pour les certificats de clé publique et la validation du chemin de certification.

10.2 LIST OF ACRONYMS

AES	Advanced Encryption Standard
ANIP	Agence Nationale d'Identification des Personnes
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARL	Authority Revocation List
ASSI	Agence des Services et Systèmes d'Information
CA	Certification Authority
CISA	Certified Information System Auditor
CITE	Community Interoperability Test Environment
CMS	Card Management System
CNSN	Conseil National de Sécurité du Numérique
COI	Communities of Interest
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSS	Certificate Status Server
DCH	Designated Certificate Holder
DN	Distinguished Name
DS	Document Signer
EC	Elliptic Curve
EDC	Entrust Datacard Corporation
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IFU	Identifiant Fiscal Unique
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
LDAP	Lightweight Directory Application Protocol
MOA	Memorandum of Agreement
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
NCPA	National Certification Policy Authority

NPI	Numéro Personnel d'Identification
PA	Policy Authority
PII	Personally Identifiable Information
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PoC	Point of Contact
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
RKGC	Root Key Generation Ceremony
RPS	Registration Practice Statement
SCO	Security Compliance Officer
TA	Trusted Agent
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VM	Virtual Machine
VME	Virtual Machine Environment

11. ANNEXE A - DEMANDE D'ENREGISTREMENT DE L'AUTORITÉ LOCALE PARTENAIRE

11.1 INTRODUCTION

11.1.1 Objectifs

Cette annexe fournit un cadre général pour le processus utilisé pour soumettre une demande afin de devenir une autorité locale d'enregistrement partenaire (Partner-LRA).

Cette annexe est destinée au personnel impliqué dans les activités de contrôle et d'approbation des demandes des LRA partenaires. Les demandes d'information peuvent être adressées à la PA de la GovCA du Bénin. Voir la section **Erreur ! Source du renvoi introuvable.** pour les coordonnées de la PA de la GovCA du Bénin.

11.1.2 Principes généraux

Les certificats de la LRA partenaire délivrés par la GovCA du Bénin sont délivrés et révoqués à la discrétion de la PA de la GovCA du Bénin. Lorsque la GovCA du Bénin délivre un certificat LRA partenaire à un partenaire, il le fait à sa propre discrétion au profit du gouvernement du Bénin. Toute information soumise à la PA de la GovCA du Bénin par une LRA partenaire requérante est à la disposition de la PA de la GovCA du Bénin pour déterminer si un certificat de la LRA partenaire peut être délivré et souhaitable et sera traité comme un droit de propriété conformément aux accords de non-divulgation applicables.

En vue d'aider à déterminer si la PA de la GovCA du Bénin examinera une demande, une LRA requérante partenaire doit soumettre une analyse de rentabilité à la PA de la GovCA du Bénin pour approbation. L'analyse de rentabilisation doit décrire comment le gouvernement du Bénin bénéficiera de la délivrance d'un certificat LRA partenaire au demandeur.

11.2 PROCESSUS DE CANDIDATURE ET D'ÉVALUATION

Le processus de candidature et d'évaluation est conçu pour établir une relation de confiance mutuelle entre la GovCA du Bénin et la LRA partenaire requérante. Cette section identifie les étapes nécessaires à exécuter par les différentes parties impliquées dans le processus de demande. Cette section précise les conditions préalables qui doivent être remplies avant qu'une LRA partenaire requérante ne soumette une demande de certificat de LRA partenaire. À tout moment au cours du processus d'évaluation, la PA de la GovCA du Bénin peut informer le demandeur, s'il est déterminé, que la demande a été rejetée :

- La GovCa et le gouvernement du Bénin ne tirent pas suffisamment profit de l'interopérabilité avec la LRA partenaire requérante ;
- Il existe des assez risques ou des problèmes de sécurité en ce qui concerne l'interopérabilité avec l'ALE partenaire candidate ; et
- Les politiques, le processus et les procédures de la LRA partenaire requérante ne s'alignent pas avec la GovCA du Bénin.

Le dossier de candidature de la LRA partenaire requérante doit comprendre les réponses à toutes les sections et tous les documents demandés doivent être joints, sauf indication contraire. Le

dossier de candidature sera examiné par la PA de la GovCA du Bénin et sa subordonnée, la RA de la GovCA du Bénin.

Après avoir examiné toutes les contributions, si la décision est de poursuivre, la LRA partenaire requérante passera à la phase suivante. Cette phase comprend :

- Présentation de l'analyse de rentabilité à la PA de la GovCA du Bénin et à la RA de la GovCA du Bénin ;
- Analyse de la déclaration de pratique d'enregistrement (RPS) de la LRA partenaire du demandeur ;
- Examen et essais techniques ;
- Revue d'audit ;
- Vote de la PA de la GovCA du Bénin sur la délivrance d'un certificat LRA à la LRA partenaire ;
- Négociation d'un Protocole d'Accord ; et
- Délivrance d'un certificat LRA à la LRA partenaire agréé.

NB : Si la demande initiale n'est pas approuvée, la LRA partenaire requérante sera informée des raisons pour lesquelles la demande a été rejetée.

11.2.1 Évaluation de la Méthodologie

La LRA partenaire requérante doit disposer d'une procédure officielle documentée. La PA de la GovCA du Bénin doit examiner les processus de la LRA partenaire requérante concernant l'émission et la gestion des certificats d'abonnés. Ce processus doit être documenté dans la RPS de la LRA partenaire. Au minimum, la RPS doit traiter les sections 3 et 4 de la GovCA CP du Bénin, les tests (interopérabilité et sécurité), les MOA, les demandes de nouveaux membres, la surveillance et la gouvernance continues des relations entre les LRA. L'examen déterminera si les processus de la LRA partenaire requérante fournissent le degré d'assurance dans l'intégrité de la communauté de la GovCA du Bénin pour justifier la participation à la communauté de confiance.

11.2.2 Évaluation de la déclaration de Procédure d'Enregistrement

La revue de la déclaration de procédure d'enregistrement est l'analyse de la RPS présentée par la LRA partenaire requérante et qui assure la conformité avec la CP de la GovCA du Bénin. La LRA partenaire requérante doit soumettre sa RPS à l'examen par la CA-PA de la racine du Bénin et son délégué la RA de la GovCA du Bénin. La CA-PA et la RA du Bénin vont comparer le RPS de la LRA partenaire requérante avec la CP de la GovCA du Bénin afin de s'assurer que l'environnement opérationnel et les exigences de délivrance et de gestion des certificats sont comparables à l'environnement opérationnel et aux exigences de délivrance et de gestion des certificats de la GovCA du Bénin.

11.2.3 Examen et Essai techniques

L'examen et l'essai technique comprennent :

- Les tests d'interopérabilité technique ; et

- Démonstration des capacités opérationnelles.

Pour les tests d'interopérabilité technique, la LRA partenaire requérante doit démontrer que sa solution d'émission et de gestion des certificats est techniquement compatible avec la GovCA du Bénin. La solution d'émission et de gestion des certificats de la LRA partenaire requérante et la conformité ou l'interopérabilité de la solution de la LRA partenaire requérante avec la GovCA du Bénin seront examinées. L'objectif est de déterminer si l'émission et la gestion des certificats d'abonnés peuvent être couronnées de succès ;

L'environnement de test d'interopérabilité de la communauté de la GovCA du Bénin (Benin GovCA CITE) est établi afin de fournir à la communauté de la GovCA du Bénin un environnement de test pour (a) identifier et résoudre les problèmes, et (b) assurer une fonctionnalité adéquate, avant le déploiement dans l'environnement de production. Il est configuré comme un double de l'infrastructure de production de la GovCA Bénin. Le personnel représentant la LRA partenaire requérante travaille avec l'OA de la GovCA du Bénin pour effectuer les tests d'interopérabilité technique.

La LRA partenaire requérante doit établir un banc d'essai qui reflète son environnement opérationnel et le configurer conformément à la GovCA CITE du Bénin. Tous les coûts encourus par la LRA partenaire requérante qui résultent de l'établissement d'un banc d'essai et de la participation aux essais d'interopérabilité technique sont à la charge de cette dernière. La LRA partenaire requérante doit maintenir le banc d'essai et la connectivité avec la GovCA CITE du Bénin après l'achèvement du processus de demande afin de fournir un environnement pour tester les correctifs du référentiel et les nouvelles applications avant le déploiement dans l'environnement de production. Les tests d'interopérabilité technique doivent au moins démontrer que :

- Les communications en réseau utilisent avec succès tous les protocoles requis ;
- La demande d'émission et de gestion du certificat est correctement construite par la GovCA du Bénin et échangée et reconnue par la LRA partenaire requérante ; et
- Une transaction test pour la délivrance et la gestion d'un certificat peut être validée avec succès.

11.2.4 Revue d'Audit

Le RPS de la LRA partenaire requérante doit démontrer que son service d'émission et de gestion des certificats fonctionne conformément à la CP de la GovCA du Bénin. Pour ce faire, la LRA partenaire requérante doit se soumettre à un audit indépendant qui détermine ce qui suit :

- Le RPS de la LRA partenaire requérante répond de manière adéquate aux exigences applicables de la CP de la GovCA du Bénin ; et
- Les opérations et la gestion de la LRA partenaire requérante mettent correctement en œuvre le RPS.

La PA de la GovCA du Bénin, la RA de la GovCA du Bénin et l'Organe de contrôle du gouvernement du Bénin examineront la lettre d'opinion d'audit pour confirmer que la LRA partenaire requérante est exploitée et gérée conformément à son RPS.

11.2.5 Vote de la PA de la GovCA du Bénin sur l'émission d'un certificat de la LRA partenaire

La PA de la GovCA du Bénin et la RA de la GovCA du Bénin examinent les informations et les contributions recueillies au cours des étapes précédentes. Une fois ce processus terminé, la CA-PA racine du Bénin votera sur la question de savoir s'il faut délivrer un certificat LRA partenaire au demandeur. Si la décision est d'approuver la délivrance d'un certificat LRA partenaire, la LRA partenaire requérante et la CA-PA du Bénin signent un protocole d'accord (MOA).

11.2.6 Négociation d'un Protocole d'Accord (MOA)

Les relations entre le gouvernement du Bénin et une la LRA partenaire sont régies par le protocole d'accord qui doit être signé par un fonctionnaire autorisé à engager la LRA partenaire requérante et par la PA de la GovCA du Bénin.

La PA de la GovCA du Bénin fournira un modèle de protocole d'accord adapté au type de certificat LRA souhaité par la LRA partenaire du demandeur et qui servira de point de départ aux négociations. Le protocole d'accord ne sera signé qu'une fois que toutes les questions auront été résolues à la satisfaction de la PA de la GovCA du Bénin.

Une copie du protocole d'accord entièrement exécuté sera fournie à l'OA de la GovCA du Bénin et à la LRA partenaire requérante pour archivage.

11.2.7 Émission du certificat de la LRA Partenaire

La PA de la GovCA du Bénin fournit une feuille de travail à la LRA partenaire du demandeur afin obtenir des informations techniques et sur le POC pour l'émission du certificat de la LRA. Ces informations sont utilisées pour remplir les demandes de certificat de la LRA. Après un examen satisfaisant des données techniques, les certificats LRA produits sont délivrés et affichés dans les référentiels appropriés.

11.3 LISTE DE CONTRÔLE DES CONDITIONS PREALABLES A LA DEMANDE DE CERTIFICAT DE LA LRA PARTENAIRE

Une LRA partenaire souhaitant obtenir un certificat LRA de la part de la GovCA du Bénin doit répondre aux critères énumérés ci-dessous afin que sa demande soit prise en compte :

Tableau 11 – Liste de contrôle des conditions préalables à la demande de certificat de la LRA partenaire

Prérequis	Oui/Non
Démontrer pourquoi il est avantageux pour le gouvernement du Bénin de délivrer un certificat LRA à la LRA partenaire qui en fait la demande	
La LRA partenaire requérante peut avoir un sponsor du gouvernement du Bénin qui bénéficiera de l'interopérabilité avec la communauté PKI que la GovCA soutient. Le sponsor doit déclarer son intention de faire confiance et d'accepter les certificats de la communauté PKI représentée par la LRA partenaire requérante une	

fois qu'elle aura été approuvée et de maintenir le parrainage tout au long du processus de demande/approbation.	
Identifier les OID de la politique de la GovCA du Bénin avec lesquels la LRA partenaire du demandeur demande l'autorisation d'émettre et de gérer.	
Fournir une déclaration de pratique d'enregistrement (RPS) qui démontre comment les certificats seront délivrés et gérés et comment la LRA partenaire se conformera aux politiques définies dans la CP de la GovCA du Bénin. La PA de la GovCA du Bénin se chargera de déterminer en dernier ressort la comparabilité.	
Soumettre une copie de la charte de LRA partenaire décrivant l'adhésion, la résolution des conflits, l'autorité et les relations organisationnelles.	
Fournir une description de l'architecture de la LRA partenaire requérante.	
Fournir la preuve des connaissances, des compétences et des aptitudes de la LRA partenaire du demandeur en matière de délivrance et de gestion des certificats X.509, en incluant les CV du personnel clé, en identifiant les rôles, l'expérience et l'expertise, le nombre d'années passées dans le domaine, etc.	
Soumettez un dossier de candidature dûment rempli en utilisant le modèle qui se trouve dans la section **Erreur ! Source du renvoi introuvable.** ci-dessous.	

11.4 DEMANDE DE CERTIFICAT LRA AUPRÈS DE LA GOVCA DU BENIN

1. Coordonnées des personnes à contacter

   Veuillez signer et envoyer une copie électronique de cette section par courriel à info-assi@presidence.bj.

2. Informations sur l'organisation
   a. Nom de l'organisme demandeur
   b. Adresse de l'organisme demandeur

3. Coordonnées du point focal du demandeur (POC)
   a. Représentant de l'organisation POC (nom et titre, adresse postale, numéro de téléphone du service, adresse électronique de service)
   b. PoC technique (nom et titre, adresse postale, numéro de téléphone du service, adresse électronique du service)
4. Avantages pour le gouvernement du Bénin

Décrire l'analyse de rentabilité qui permettra au gouvernement du Bénin de délivrer un certificat LRA au demandeur.

5. Politiques de certification souhaitées par la LRA de la GovCA du Bénin
    a. Basique
    b. Moyen
    c. Élevé
6. Aperçu du service de la LRA requérante

    Fournir des informations sur les exigences de la LRA, sa communauté d'utilisation et le bénéfice attendu pour le gouvernement du Bénin.

Tableau 12 – Aperçu des services offerts par le demandeur et la LRA

Informations requises sur la LRA partenaire du Demandeur	Réponse du demandeur
Les documents de gouvernance suivants doivent être identifiés ici et soumis avec la demande : • Charte • Processus et procédures de résolution des conflits	
Quelle autorité permet à la LRA partenaire requérante de parler et d'agir au nom de ses abonnés cibles ?	
Décrire la nature de la relation entre les abonnés cibles et la GovCA du Bénin	
Décrivez les parties utilisatrices qui s'attendent à bénéficier de l'utilisation de ces certificats d'abonnés.	
Décrire la relation entre la LRA partenaire et son parrain du Gouvernement du Bénin, s'il y en existe.	

7. Informations sur l'architecture du service LRA du demandeur

    Fournir des informations sur l'architecture du service de votre LRA :

Tableau 13 – Informations sur l'architecture de service de la LRA requérante

Informations requises sur l'Architecture	Réponse du demandeur
Fournir une liste des applications LRA sous le contrôle de la LRA partenaire requérante qui seront utilisées pour émettre et gérer les certificats (ex : le portail PKI du gouvernement du Bénin, l'application LRA personnalisée qui sera développée par la LRA partenaire, le service de gestion des utilisateurs, le serveur d'inscription natif Windows, etc.)	
Fournir une liste des types de certificats devant être émis et gérés par la LRA partenaire (ex : authentification des abonnés de haute assurance, authentification informatique de moyenne assurance, certificats TLS de moyenne assurance, etc.)	
Fournir une liste des opérations de gestion des certificats à effectuer par la LRA partenaire (ex : émission, révocation, nouvelle clé, suspension, modification).	
Joindre un diagramme d'architecture logique décrivant le service de la LRA dans l'environnement de LRA partenaire requérante et la manière dont il sera intégré à la GovCA du Bénin (ex, Entrust Java Toolkit, Entrust CA Gateway, TrustedX API, etc.)	
Joindre un diagramme de réseau détaillé décrivant l'ensemble des composantes des services de la LRA partenaire requérante, leurs relations et la protection du réseau en place.	
Fournir toute information supplémentaire qui pourrait être utile au gouvernement du Bénin pour l'évaluation de cette demande.	

8. Sponsor Partenaire du Gouvernement du Bénin

   Fournir le nom et les coordonnées d'un sponsor de la LRA partenaire du gouvernement du Bénin.

   a. Nom et titre du sponsor :
   b. Ministère ou organisme parrain :

c. Adresse électronique :
d. Numéro de téléphone :

9. Statut de la société
   Fournir la preuve du statut social de l'entité responsable du service de la LRA partenaire et de sa capacité financière à gérer les risques associés à l'exploitation d'un service LRA. La nature et l'autonomie du statut d'entreprise et de la capacité financière seront déterminées au cas par cas à la discrétion de la PA de la GovCA du Bénin.

10. Connaissances, Compétences et Aptitudes
    Fournir à ses abonnés la preuve de connaissances, de compétences et de capacités de la LRA partenaire requérante dans l'émission et la gestion des certificats X.509 de la GovCA du Bénin. Inclure les curriculums vitae du personnel clé, en identifiant les rôles, l'expérience et l'expertise, le nombre d'années sur le terrain, etc.

11. Signature
    La demande doit être signée et datée numériquement par un haut cadre (un dirigeant ou un cadre) autorisé à parler au nom de l'organisation qui gère le service la LRA Partner et par un représentant autorisé de l'agence de parrainage.

Demandeur	Sponsor
Les informations ci-dessus sont, pour autant que je sache et que je croie, vraies et exactes.	J'affirme que je suis un représentant autorisé de mon agence et j'accepte de parrainer le candidat figurant sur la liste.
Nom :	Nom :
Titre :	Titre :
Signature :	Signature :
Date :	Date :

11.5 RESPONSABILITÉS DE PARRAINAGE DE LA LRA DE LA GOVCA DU BENIN

Vous trouverez ci-dessous les responsabilités d'un ministère ou d'une agence du gouvernement du Bénin ou d'un partenaire qui parraine une LRA partenaire requérante auprès de la GovCA du Bénin.

Responsabilités du Sponsor :

- La déclaration de parrainage doit émaner d'un membre de la GovCA du Bénin, en règle avec la GovCA du Bénin, et être présentée par l'intermédiaire de son représentant désigné ;
- La déclaration doit provenir d'une organisation qui tirera un avantage important de l'émission d'un certificat LRA à la LRA partenaire du demandeur (avec une affirmation de l'adhésion du CIO) ;

- La déclaration doit décrire une attente raisonnable de bénéfice pour le gouvernement du Bénin qui justifie l'effort et l'engagement initial et continu de ressources pour établir et maintenir le certificat LRA du demandeur ;
- Des sponsors supplémentaires et des déclarations du même ou d'autres ministères, agences ou partenaires sont acceptables et encouragés ;
- Le sponsor principal doit rester directement impliqué dans le processus d'évaluation des candidats
- Le sponsor principal doit réaffirmer son parrainage à la fin du processus d'évaluation (avant l'approbation par la PA du dossier de candidature de la LRA partenaire).