PORTAIL DE L'IDENTITÉ NUMÉRIQUE

GOUVERNEMENT DE LA RÉPUBLIQUE DU BÉNIN

DOCUMENT D'INFORMATION SUR LA PKI

Table des matières

1.1 L'Infrastructure à clés publiques

1.1.1 Infrastructure à clés publiques du Bénin

- **Définition**

Une infrastructure à clés publiques, appelée encore PKI en anglais (Public Key Infrastructure) est un système de gestion de clés et de certificats, fournissant des services de sécurité basés sur la cryptographie. Elle s'appuie sur un ensemble de matériels informatiques, de cryptographie, d'applications et de procédures. Elle permet de faire le lien entre le possesseur du certificat et les informations qui y sont renseignées.

La PKI certifie des clés publiques qui permettent de chiffrer et de signer des messages ainsi que des flux de données. Elle peut s'intégrer aux différentes applications d'e-service ou métiers afin d'assurer :

- **L'authentification : l'identité de l'entité à l'origine de l'information ou d'une tentative de connexion au système, est garantie.**
- **La confidentialité : les informations échangées deviennent illisibles, de sorte que seul le destinataire ou l'expéditeur puissent les déchiffrer.**
- **La non-répudiation : l'émetteur d'une information ne peut nier en être son auteur.**
- **L'intégrité : Toute information transmise via le système de PKI ne peut être altérée.**

Pour pouvoir mettre en œuvre une gestion des certificats sûre, une vérification d'identité rigoureuse et une implémentation de solutions cryptographiques fiables sont indispensables. C'est pourquoi, la PKI du Bénin est composée d'une autorité de certification qui va délivrer et gérer les certificats pendant leur cycle de vie et d'une autorité d'enregistrement qui va appliquer les politiques d'identification et d'enregistrement des entités, définies par l'autorité de certification.

Cette infrastructure de gestion de clés fournit donc principalement des services :

- **D'enregistrement des utilisateurs de certificat**
- **D'authentification des utilisateurs aux différentes applications intégrées avec la PKI**
- **De renouvellement et de révocation des certificats, automatiquement ou via des procédures formelles**
- **De vérification de la validité des certificats.**

- De signature électronique
- De chiffrement

- Ambition du Bénin

Le Gouvernement Béninois s'est lancé dans la mise en place de plusieurs initiatives stratégiques visant spécifiquement à améliorer les opérations internes des ministères et départements gouvernementaux, ainsi que la façon dont ils fournissent leurs services aux citoyens béninois. Les améliorations doivent inclure des aspects de qualité, d'accessibilité et des interactions entre les structures gouvernementales, les entreprises et les citoyens.

Nous sommes actuellement dans un environnement mondial où l'information est au centre de toute décision. Il importe d'avoir un système d'information sécurisé et fiable. Il convient donc de protéger l'information de toute intrusion, car elle constitue un patrimoine important pour tout développement d'une administration publique ou privée, d'une entreprise, ou même d'une personne physique.

Le système PKI est un système robuste qui permet donc de faire circuler des messages entre un expéditeur et un destinataire, en garantissant que seuls ces derniers pourront y accéder.

C'est ainsi que la République du Bénin, à travers l'Agence des Services et Systèmes d'Information (ASSI), a mis en place le système national d'Infrastructure à Clés Publiques (PKI). Le système PKI est utilisé pour sécuriser entre autres, les documents de voyage (passeport électronique, carte d'identité électronique), les transactions électroniques, les documents électroniques ainsi que les services en ligne.

L'objectif à long terme est de permettre à tout citoyen ou résident ou à toute entreprise de disposer de documents électroniques nationaux fiables et de pouvoir utiliser des services en ligne (e-Gouvernement, e-Commerce, e-Banking, etc) en toute sécurité. Les actes posés via ces applications d'e-services auront la même valeur juridique que s'ils avaient été faits manuellement.

1.1.2 Présentation du Gouv CA

Le portail de l'identité numérique comporte toute l'information concernant la délivrance de certificats par l'autorité de certification du gouvernement du Bénin appelée GouvCA .

Le GouvCA est une entité qui prend en charge le processus de délivrance et de gestion des certificats électroniques, à travers leur création, leur renouvellement et leur révocation, selon les recommandations de la norme X.509. Elle fournit des

paires de clés et des certificats numériques tels que le certificat d'authentification, de signature numérique et de cryptage, permettant ainsi au souscripteur de faire des actes sécurisés en ligne. Elle garantit l'intégrité et la véracité des informations se trouvant dans les certificats.

Le GouvCA dépend et applique les politiques d'une autorité de certification racine appelée le RootCA. Le RootCA s'appuie sur les lois et règlements en vigueur en République du Bénin en matière de numérique et se trouvant principalement dans le code du numérique. Le GouvCA possède donc un certificat délivré par le RootCA.

En résumé, les utilisateurs peuvent via ce portail faire des demandes de certificats, les renouveler ou les révoquer, sous le contrôle des autorités d'enregistrement locales reconnues par l'autorité d'enregistrement principale qu'est l'ASSI.

1.1.3 Cadre légal

La PKI béninoise est fondée sur les lois et règlements se trouvant dans la loi n°2017 -20 du 20 avril 2018 portant code du numérique en République du Bénin. Le code numérique est un livret juridique qui donne toutes les dispositions légales en matière de digitalisation. Il constitue en quelque sorte « la bible » de tout projet informatique se réalisant sur le territoire national.

L'autorité d'opération du GouvCA (ANSSI) établit une déclaration des pratiques de certification qui définit la façon dont les instructions contenues dans la politique de certification (CP) sont mises en œuvre.

Le CP est un document de politique qui précise les acteurs, leurs rôles et devoirs, les usages des certifications, les niveaux d'assurance, les procédés de vérification de l'identité, les cycles de vie des certificats, les contrôles de gestion opérationnels, physiques et de sécurité, les politiques de certificats à utiliser par l'autorité de certification du Bénin pour faciliter l'interopérabilité avec d'autres domaines d'infrastructure à clé publique partenaires.

1.2 Guide du certificat

1.2.1 Définition du certificat

Un certificat est un document électronique infalsifiable attribué à une entité (personne, entreprise, matériel) par une organisation reconnue appelée autorité de certification. Il est considéré comme une carte d'identité numérique. Il comporte entre autres des informations d'identification : nom et prénom, adresse électronique, adresse du propriétaire, dates de validité, détails sur l'autorité émettrice, mais aussi des moyens de vérification de sa validité et son usage (signature, chiffrement, etc). Il confère donc à son propriétaire une identité numérique fiable.

Le certificat électronique a plusieurs appellations : certificat numérique ou encore certificat de clé publique. Il permet à un système informatique d'identifier et d'authentifier de façon sûre, toute personne ou tout appareil s'y connectant et de signer en ligne en toute sécurité. Il garantit ainsi la confidentialité, l'intégrité des données et la non-répudiation, à travers des opérations comme le chiffrement des échanges électroniques et la signature.

Le standard communément utilisé pour la création des certificats est X.509. On parle donc de certificats X.509.

La PKI du Bénin permet de délivrer des certificats avec des niveaux d'assurance divers, dépendamment de certains critères.

Type d'assurance Critères	Elevée	Substantielle	Faible
Délivrance à un humain uniquement	✓		
Délivrance de certificat à un ordinateur ou une application		✓	✓
Vérification d'identité obligatoire en présentiel	✓		
Vérification d'identité en présentiel ou à distance		✓	✓
Présentation de la carte d'identité, passeport or carte de résident	✓		
Présentation de tout type de pièce d'identité		✓	✓
Signature de formulaire de consentement	✓		
Clés générées et stockées dans un module cryptographique matériel FIPS 140-2 niveau 2 ou supérieur	✓		
Clés générées et stockées dans un		✓	

module cryptographique matériel FIPS 140-2 niveau 1 ou supérieur			
Clés générées et stockées dans un module cryptographique matériel FIPS 140-2			✓
Clés privées générées obligatoirement par le possesseur du certificat	✓		
Clés privées générées par le possesseur du certificat ou son représentant		✓	✓

1.2.2 Utilisation du certificat

Le certificat électronique est utilisé pour faire de multiples actions telles que l'authentification, la signature électronique ou le cryptage de données.

Par l'authentification, un utilisateur apporte la preuve de son identité, une fois que celle-ci a été établie au moyen de l'identification. L'authentification permet de vérifier que cet utilisateur est bien habilité à être connecté à un système informatique. Elle garantit donc la légitimité d'une entité à accéder à des ressources informatiques, en accord avec le paramétrage des accès au système. Elle peut être simple (un seul facteur de vérification comme le mot de passe) ou forte (plusieurs facteurs de vérification comme mot de passe + code envoyé par sms ou email). Dans le projet de PKI, nous utilisons l'authentification forte pour gérer les identités virtuelles émises.

La signature électronique quant à elle, va offrir des niveaux de garantie élevés en matière d'intégrité d'un document et d'authentification de la personne signataire. Elle permet de lier l'expéditeur d'un message signé, à ce message. Le destinataire du message pourra alors identifier formellement l'auteur de la signature. On va pouvoir également, être sûr que le document n'a pas été altéré entre le moment où il a été signé et le moment où il est lu. Ce mécanisme se produit en utilisant des fonctions de hachage et un chiffrement via des clés publiques et privées, afin de rentre la signature authentique, infalsifiable, non réutilisable, inaltérable et irrévocable.

Le cryptage, encore appelé chiffrement permet d'assurer la confidentialité d'un document électronique. Le texte du document va ainsi être encodé grâce à un algorithme, et devenir illisible. Une clé de chiffrement est utilisée pour chiffrer le texte et une clé de déchiffrement pour le déchiffrer. Seules les personnes en possession de la clé de déchiffrement pourront donc décoder le document.
Le cryptage est de plus en plus utilisé pour sécuriser les données, dans le monde professionnel comme personnel. En résumé, il va permettre de protéger les informations pendant leur transfert entre un client et un serveur.

1.2.3 Qui peut recevoir un certificat ?

- **Les citoyens béninois : Chaque citoyen béninois peut se faire délivrer un certificat afin de réaliser des actes d'authentification et de signature électronique. L'ANIP est la principale responsable de la délivrance de certificats aux citoyens.**
- **Les employés des entreprises : Toute entreprise enregistrée au Bénin, pourra faire délivrer à ses collaborateurs, un certificat afin de réaliser des actes d'authentification et de signature électronique. L'APIEX est la principale responsable de la délivrance de certificats aux employés.**
- **Les résidents : Chaque résident de nationalité étrangère vivant sur le territoire béninois, et en possession d'une carte de résident pourra se faire délivrer un certificat afin de réaliser des actes d'authentification et de signature électronique. La DEI est la principale responsable de la délivrance de certificats aux résidents étrangers.**
- **Les employés du gouvernement : Chaque employé du gouvernement béninois (ministères, mairies, préfectures, etc) pourra se faire délivrer un certificat afin de réaliser des actes d'authentification, de signature électronique et de chiffrement de données. L'ASSI est la principale responsable de la délivrance de certificats aux employés du gouvernement.**
- **Les ordinateurs et applications : Tout ordinateur ou application pourra se faire délivrer un certificat afin de réaliser des actes d'authentification et de chiffrement de données. L'ASSI est la principale responsable de la délivrance de certificats aux matériels et applications informatiques.**

1.2.4 Qui peut délivrer un certificat ?

Les Autorités d'Enregistrement Locales (LRA pour Local Registration Authority) sont les seuls organismes habilités à délivrer un certificat. Elles sont responsables de la délivrance et de la gestion des certificats émis. Les LRA doivent être autorisées par l'Autorité de Certification du Gouvernement (GouvCA) avant de pouvoir gérer et émettre des certificats. Toute organisation ou entreprise désirant exploiter une application via des certificats délivrés par le Gouv CA doit se faire au préalable enregistrer auprès de l'ASSI.

1.3 Nos services

1.3.1 Identité électronique (eID)

Tout citoyen béninois peut se faire délivrer une identité électronique (eID), semblable à celle fournie sur la CNI (Carte Nationale d'Identité). L'identité électronique vous permet de vous identifier et de vous authentifier dans un environnement numérique sécurisé. Elle vous permet également de signer un document ou d'opérer des transactions électroniques en toute sécurité. Toutes les informations nécessaires à la fourniture de cette identité sont stockées dans la puce de la CNI ou sur un jeton USB sécurisé.

L'identité eID ne peut être attribuée que selon des processus définis dans la déclaration des pratiques d'enregistrement propres à chaque autorité d'enregistrement et approuvées par le GouvCA.

La procédure détaillée de demande de certificats sur jeton USB est disponible à la section Obtenez votre certificat de notre site internet.

Objet du certificat	Receveurs	Conditions de délivrance	Durée de vie	Autorité d'enregistrement	Stockage du certificat	Coût
Authentification et signature électronique	Citoyen béninois	Être citoyen béninois enregistré dans la base de données du RAVIP	60 mois	ANIP	Puce du jeton USB ou de la Carte d'Identité Nationale	

NB : La délivrance de certificat sur Carte d'Identité Nationale ou jeton USB sera mise en service très bientôt.

1.3.2 Identité virtuelle ou Virtual ID

L'Identité virtuelle ou Virtual ID permet d'appliquer une signature à distance sur un document électronique. Contrairement aux certificats stockés sur la Carte Nationale d'Identité ou jeton USB sécurisé, toutes les informations liées à l'identité virtuelle sont stockées dans un système hautement sécurisé et sont hébergées dans le centre de données national du Bénin. Avec l'Identité virtuelle ou Virtual ID, vous n'avez pas besoin d'avoir de façon permanente votre

carte d'identité ou jeton USB sécurisé sur vous, pour effectuer vos transactions électroniques.

L'identité Virtual Id ne peut être attribuée que selon des processus définis dans la déclaration des pratiques d'enregistrement propres à chaque autorité d'enregistrement et approuvées par le GouvCA.

La procédure détaillée de demande de certificats virtuels est disponible à la page Obtenez votre certificat de notre site internet.

Objet du certificat	Receveurs	Conditions de délivrance	Durée de vie	Autorité d'enregistrement	Stockage du certificat	Coût
Authentification et signature électronique	Citoyen béninois	Être citoyen béninois enregistré dans la base de données du RAVIP	12 ou 24 ou 36 mois au choix	ANIP	Centre de données national	
Authentification et signature électronique	Employé	Avoir le numéro IFU de l'entreprise	12 ou 24 ou 36 mois au choix	APIEX	Centre de données national	
Authentification et signature électronique	Résident étranger	Avoir une carte de résident	12 ou 24 ou 36 mois au choix	DEI	Centre de données national	

1.3.3 Identité Mobile ou Mobile Id

L'Identité Mobile ou Mobile Id permet de vous identifier et de vous authentifier sur les services en lignes avec votre téléphone mobile. Toutes les informations liées à votre identité Mobile Id sont donc stockées dans votre téléphone mobile. Avec l'Identité Mobile ou Mobile Id, vous n'avez pas besoin d'avoir de façon permanente votre Carte d'Identité Nationale ou votre jeton USB sécurisé sur vous, pour effectuer vos transactions électroniques.

La délivrance de certificat sur téléphone mobile se fait à deux conditions :

- **Avoir un smart phone (téléphone intelligent) afin de pouvoir télécharger l'application MobileID.**
- **Avoir un compte d'identité virtuelle.**

Une fois en possession de votre identité virtuelle, vous pouvez de façon autonome, créer votre certificat dans MobileID, sans passer par une autorité d'enregistrement.

L'identité Mobile Id ne peut être attribuée que selon des processus définis dans la déclaration des pratiques d'enregistrement propres à chaque autorité d'enregistrement et approuvées par le GouvCA.

La procédure détaillée de demande de certificats sur mobile est disponible à la page Obtenez votre certificat de notre site internet.

Objet du certificat	Receveurs	Conditions de délivrance	Durée de vie	Autorité d'enregistrement	Stockage du certificat	Coût
Authentification	Citoyen béninois	Avoir une identité virtuelle	12 ou 24 mois au choix	ANIP	Téléphone mobile du propriétaire du certificat	
Authentification	Employés	Avoir une identité virtuelle	12 ou 24 mois au choix	APIEX	Téléphone mobile du propriétaire du certificat	
Authentification	Résident étranger	Avoir une identité virtuelle	12 mois	DEI	Téléphone mobile du propriétaire du certificat	