



B.P. 6170 Yaoundé-Cameroun

Tél.: +237 22 20 22 11 / Fax: +237 22 20 39 31

courriel : pki@antic.cm Web: http://www.antic.cm

QUESTIONNAIRE

(Sécurisation des applications à l'aide du système PKI)

L'Infrastructure Nationale à Clé Publique est désormais opérationnelle au Cameroun. Celle-ci vous offre l'opportunité de sécuriser vos applications qui traitent des données critiques de votre Administration ou Organisation.

Ce questionnaire permettra de partager vos compétences, votre expérience et renseignera sur les informations relatives à vos applications. Les données recueillies permettront de mieux sécuriser vos transactions électroniques critiques. Vos réponses seront gardées confidentielles et ne seront utilisées que pour le système PKI national.

Bien vouloir renseigner ce formulaire pour chaque application utilisée dans votre administration ou Organisation

Nom de l'application	
Ministère/Organisation/Institution	
Structure en charge de l'application	
Contact du responsable	
Téléphone	
Fax	
e-mail	
URL	
Adresse	

1. Introduction

1. Décrivez sommairement cette application :

2. Cette application interagit-elle avec d'autres applications existant dans votre structure?

Oui **Non**

3. Si la réponse à la question 2 ci-dessus est 'Oui', bien vouloir renseigner le tableau ci-dessous:

N°	Application	Brève description
1		
2		
3		
4		
5		

(Notez que ce tableau peut être étendu.)

4. Cette application interagit-elle avec d'autres applications hors de votre structure? **Oui** **Non**

5. Si la réponse à la question 4 ci-dessus est 'Oui', bien vouloir renseigner le tableau ci-dessous:

N°	Application	Brève description
1		
2		
3		
4		
5		

(Notez que ce tableau peut être étendu.)

6. Spécifiez les utilisateurs finaux de l'application

Personnels de votre institution **Employés de l'État en général** **Entreprises**

Grand Public **Autres, à indiquer :** _____

7. Bien vouloir indiquer le type de réseau mis en place pour offrir le service aux utilisateurs finaux.

Internet **Intranet** **Extranet** **VPN** **Autres, à indiquer :** _____

2. Environnement Technique

1. L'application est-elle de type Client-Serveur ?

Oui **Non**

2. Si la réponse à la question précédente est Oui, bien vouloir préciser le type de votre application Client-Serveur

2-tier **3-tier**

3. Indiquer le langage de programmation utilisé pour développer l'application (**préciser la version**)

Java **DotNet** **PHP** **C/C++** **WINDEV** **Visual Basic** **Pascal**

Informix **Python** **Perl** **Oracle forms** **Autres, à préciser :** _____

4. Indiquer si l'application offre des services web

Oui **Non**

5. Si la réponse à la question 4 ci-dessus est 'Oui', bien vouloir indiquer le langage utilisé pour offrir les services web

JSP **ASP** **PHP** **PERL** **Autres, à indiquer :** _____

6. L'application a-t-elle une base de données ?

Oui **Non**

7. Si la réponse à la question 6 ci-dessus est 'Oui', bien vouloir indiquer les technologies liées à la base de données pour cette application (**préciser la version**)

Oracle **Microsoft SQL** **IBM DB2** **MySQL** **Autres, à préciser :** _____

8. Si la réponse à la question 1 ci-dessus est 'Oui', bien vouloir indiquer le système d'exploitation sur lequel est installé l'application : _____

Ce système d'exploitation est :

32 bits 64 bits

La technologie utilisée est :

a. Microsoft: Windows NT Windows 2000 Server Windows 2003 Server
 Windows 2008 Server Autres, à préciser : _____

b. UNIX serveurs: AIX HPUX Linux Solaris Autres : _____

c. Autres, à préciser : _____

9. Pouvez-vous indiquer le type de serveur sur lequel est installée l'application?

Microsoft HP Sun IBM Autres, à Spécifier : _____

3. Sécurité

1. Indiquer les détails de la procédure d'identification en vue de l'enregistrement des informations des utilisateurs dans votre application

Identification hors ligne en utilisant CNI Enregistrement en ligne Identification par registre du commerce Identification par numéro de contribuable Autres, à préciser : _____

2. Existe-t-il un système de gestion des profils des utilisateurs?

Oui Non.

3. L'accès au système est-il contrôlé par le couple login/mot de passe?

Oui Non

4. L'application dispose-t-elle des moyens de retracer toutes les opérations effectuées sur le système?

Oui Non. Si oui préciser : _____

5. L'application dispose-t-elle des moyens de contrôler les accès distants au système?

Oui Non. Si oui préciser : _____

6. Indiquer si le système PKI est déployé pour sécuriser l'application

Oui Non. Si oui préciser : _____

7. Si la réponse à la question 6 ci-dessus est non, indiquer si vous envisagez déployer le système PKI? Oui Non. Si oui préciser : _____

8. Indiquer si le système a déjà été victime d'une attaque malicieuse

Oui Non. Si oui préciser : _____

9. Indiquer quel type de sécurité vous utilisez pour sécuriser votre réseau

Pare-feu DMZ Contrôle d'Accès Filtres NIDS/IPS Identifiant/Mot de passe Mot de passe à usage unique Autres, à préciser : _____

10. Quels types de problèmes de sécurité votre application rencontre-t-elle souvent?

Manque du système de contrôle d'accès Intégrité Confidentialité Virus Vers Autres, à préciser : _____

11. Quel type de sécurité votre institution offre aux serveurs?

Contrôle d'accès Smart Card Badge Système biométrique Aucun Autres, à préciser : _____

4. Organisation

1. L'application a-t-elle été développée par votre organisation en régie?

Oui Non. Si non indiquer l'entreprise qui l'a développée : _____

2. Si la réponse à la question 1 est non, disposez-vous du code source de l'application?

Oui Non

3. Si votre réponse à la question 2 est 'oui' disposez-vous des compétences internes pour modifier le code source ?

Oui Non.

4. Comment l'application est-elle maintenue?

Interne Externe. Si en Externe, bien vouloir indiquer l'organisation : _____

5. Si votre réponse à la question 4 ci-dessus est 'Externe', bien vouloir préciser si vous êtes toujours en contact avec l'organisation.

Oui Non.

6. Si votre réponse à la question 4 ci-dessus est 'Externe', bien vouloir préciser si cette organisation est une entreprise locale ou étrangère ?

Entreprise locale Entreprise étrangère.

7. Disposez-vous des documents suivants?

Documents de conception Manuels de maintenance Guide de l'utilisateur

8. Le Guichet Unique des Opérations du Commerce Extérieur(GUCE), a intégré l'Infrastructure nationale à Clé Publique dans son application (e-GUCE) pour sécuriser ses transactions en ligne. Combien jugez-vous la nécessité pour votre Administration ou Organisation d'intégrer dans vos applications, les facilités qu'offre le système PKI à savoir la signature électronique, le chiffrement, authentification forte ?

Très Urgent Urgent Pas besoin de la PKI Autres, à préciser : _____

9. Les demandeurs de vos certificats auront besoin de se rendre dans votre structure, afin de procéder à leur identification physique pour la délivrance des certificats. Dans ce cas, votre organisation deviendra une Autorité d'Enregistrement (AE). Est-il possible de désigner quelques personnes pour gérer et administrer l'Autorité d'Enregistrement de votre Administration Organisation?

Oui; Non; Si Oui, bien vouloir préciser le nombre des personnes : _____

10. Quels commentaires pouvez-vous faire pour la réussite du système PKI National?

ANNEXE 1

(Utilisation des certificats SSL)

1. Votre Administration dispose-t-elle :

a) d'un ou plusieurs site(s) web ?

Oui **Non.** Si oui indiquer l'(les) URL(s) de ce(s) site(s) web

b) d'une messagerie interne et/ou plateforme collaborative accessible via une interface Web ?

Oui **Non.** Si oui indiquer l'(les) URL(s) pour y accéder

2. Si la réponse à la question 1 est oui, indiquer le type de serveur(s) utilisé(s) pour l'hébergement :

Apache **Microsoft IIS** **NGINX** **Autres :** _____

3. Si la réponse à la question 1 est oui, indiquer le nom de l' (des) hébergeur(s)

4. Votre(vos) site(s) web traite(nt)-il(s) des données sensibles (données personnelles, secrets de fabrication, etc.) ?

Oui **Non.**

5. Comment est faite la maintenance de votre(vos) site(s) web (publications, mise à jour des outils, etc.) ?

Interne **Externe.** Si en Externe, bien vouloir indiquer le(s) prestataire(s) qui s'en charge(nt)

6. Utilisez-vous des certificats SSL pour protéger votre(vos) site(s) web/messagerie/plateforme collaborative ?

Oui **Non.** Si oui, préciser le type de certificat SSL :

Domain Validation (DV) **Organization Validation (OV)** **Extended Validation (EV)**

Autres : _____

7. Avez-vous des compétences en interne pour le déploiement d'un certificat SSL sur un serveur web ?

Oui **Non.**

ANNEXE 2

(Utilisation des moyens de cryptographie)

Les moyens de cryptographie sont un ensemble de méthodes et de principes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée.

1. Votre Structure a-t-elle recours à une exploitation des moyens de cryptographie ?

Oui **Non.**

2.

a. À quels types d'activités cette exploitation est-elle consacrée ?

Fourniture **Utilisation** **Exportation** **Importation** **Commercialisation**

b. Quels en sont les bénéficiaires ?

Administration **Grandes Entreprises** **Établissements financiers** **PME** **Professions libérales** **Etudiants** **Autres, à préciser :** _____

3. Quelles types de données sont manipulés dans ce cadre ?

Données personnelles **Données médicales** **Données financières** **Données administratives**
 Autres, à préciser : _____

4.

a. Quels sont les services cryptographiques fournis par cette prestation ?

Authentification **Intégrité** **Confidentialité** **Non-répudiation** **Horodatage** **Archivage sécurisé** **Gestion des clés cryptographiques** **Certification des clés ou de données,**
à préciser : _____

b. Quelles sont les longueurs de clés utilisées ?

64 bits **128 bits;** **256 bits;** **512 bits;** **768 bits;** **1024 bits;** **2048 bits;** **4096 bits**

c. Quelles sont les algorithmes implémentés ?

RC4 **RC5** **RSA** **DES** **3DES** **AES** **SEED** **Diffie-Hellman** **DSA** **MD5**
 SHA1 **SHA256** **Autres, à préciser :** _____

5. Quels sont les formats utilisés pour encoder la signature électronique ?

DER PEM CRT Base 64

6. Possédez-vous des références (commerciales et/ou du fabricant) de ce produit ?

Non Oui. Si oui, lesquelles ?

Merci pour votre temps et les efforts consentis./-