Historique des Systèmes PKI au Cameroun

Le Gouvernement du Cameroun a planifié le développement des services en ligne à travers le projet de mise en œuvre de la dématérialisation des procédures des services de l'Etat, qui consiste en la mise en ligne des services publics. Ce projet vise à rendre un meilleur service aux citoyens camerounais et à réduire sensiblement la corruption. Il s'agit également de la mise en œuvre et du développement des applications dans un environnement sécurisé. C'est l'aspect applicatif du Projet-Programme de l'e-Government. Dans le cadre de ce projet, les Services du Premier Ministre ont essentiellement pour rôle l'élaboration de la vision, de la coordination et de l'évaluation des initiatives prises par les différents départements ministériels. Le Ministère des Postes et Télécommunications est chargé de l'élaboration de la stratégie de développement et de la mise en place d'un plan directeur de déploiement de l'e-Government, tandis que l'ANTIC, en tant que bras séculier de l'Etat en matière des TIC et de la cybersécurité, a notamment les missions de conception, de suivi et de contrôle de la mise en œuvre de la politique du Gouvernement en matière de gouvernance électronique.

Afin de permettre aux citoyens Camerounais de profiter de tout ce que leur offre le cyberespace dans des conditions de sécurité avérées, le Gouvernement a fait de l'Infrastructure Nationale à Clé Publique une base technologique fondamentale pour la sécurisation de son cyberespace et l'un des axes stratégiques de réussite d'une telle initiative.

Il était du devoir du Ministère en charge des Télécommunications, en tant qu'autorité de tutelle, et agissant pour le compte du Gouvernement, de chercher des solutions idoines, afin de sécuriser le cyberespace camerounais.

1. La Convention avec l'UIT

En 2003, le Cameroun avait signé un Accord de don d'une valeur de trois cent soixante millions (360 000 000) FCFA avec l'Union Internationale des Télécommunications (UIT). Cet Accord visait à mettre en place une Infrastructure à Clé Publique. Il était entendu aux termes de cet Accord que le Cameroun, qui recevait ce don au même moment que le Rwanda et le Kyrkistan, devait servir de modèle d'un Etat sécurisé au Sommet Mondial sur la Société de l'Information, tenu en deux phases : à Genève en 2003 et à Tunis en 2005.

Malheureusement, la solution d'une société autrichienne dénommée AVANOC implémentée en décembre 2005 au Cameroun n'a pas connu le succès escompté.

L'échec cuisant et lamentable qu'a connu ce Projet a créé un climat froid entre l'UIT et le Cameroun. L'UIT a accusé le Cameroun d'être incapable de gérer ce don fabuleux et désiré par plusieurs autres pays de même niveau de développement que le nôtre.

C'est alors que le MINPOSTEL a envoyé certains commis de l'Etat se former dans le domaine de la sécurité des réseaux et des systèmes d'information. Ces derniers sont rentrés au Cameroun respectivement en 2006 et 2007.

Après cette boutade, le MINPOSTEL a continué la recherche d'une solution technologique pour sécuriser le cyberespace camerounais.

2. La Convention de partenariat avec le Consortium Mobile Money

Le 1er septembre 2008, un Accord de partenariat stratégique, visant à créer des conditions de confiance entre utilisateurs du cyberespace camerounais engagés dans des échanges électroniques, a été signé entre le Ministère des Postes et Télécommunications et le Consortium Mobile Money Cameroon SA/Coregate/HTT. Cet Accord avait pour objet la mise en place d'une autorité de certification, à titre expérimental au Cameroun.

Malheureusement, le Consortium n'ayant pas une expérience avérée dans le domaine n'avait pas pu remplir son contrat dans les délais prévus par l'Accord de partenariat. En effet, cet Accord prévoyait l'installation de la plateforme de sécurité, entre trois (03) et six (06) mois, suivi d'une exploitation de trois à cinq ans, renouvelable.

Il y a aussi eu l'avènement de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun. Les dispositions de cette loi font de l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) l'Autorité de Certification Racine et l'Autorité de Certification de l'Administration Publique au Cameroun. La loi sus-citée rend ipso-facto inopportune la mise en place d'une autorité de certification à titre expérimental.

Loin de se décourager, le Gouvernement camerounais a continué à chercher une solution de sécurisation des transactions électroniques de son cyberespace.

3. La Convention d'Accord de don avec la République de Corée

Le Ministère des Postes et Télécommunications, agissant au nom de la République du Cameroun, a entrepris cette fois des démarches nécessaires, pour transmettre à la République de Corée, devenue n°1 mondial dans le domaine des Technologies de l'Information et de la Communication, un dossier complet lui permettant de solliciter, de négocier et d'obtenir un Accord de don, d'une valeur de 2 800 000 dollars US, soit environ 1,4 milliard de FCFA. A la suite de nombreux échanges entre les experts Coréens et Camerounais, une étude de faisabilité conduite par les Coréens aboutit à la mise en œuvre d'une Infrastructure Nationale à Clé Publique.

Il convient de relever que le Projet PKI a permis à notre pays d'implémenter une Autorité de Certification Racine dénommée la CamRootCA (Cameroon Root Certification Authority) et une Autorité de Certification Gouvernementale dénommée la CamGovCA (Cameroon Government Certification Authority) au Centre PKI sis à Yaoundé, puis de sécuriser le module de paiement en ligne des taxes et droits douaniers de l'application e-GUCE du Guichet Unique des Opérations du Commerce Extérieur.

3.1. Signature de la Convention d'Accord de don (Record of Discussions)

La Convention d'Accord de don (Record of Discussions) sus-évoquée a donc été signée le 08 septembre 2010, entre la République de Corée, représentée par l'Agence Coréenne de

Coopération Internationale (KOICA) et la République du Cameroun, représentée par le Ministère des Postes et Télécommunications. Aux termes des dispositions de cette Convention, les deux (02) parties se sont engagées, chacune en ce qui la concerne, à remplir les obligations ci-dessous :

3.1.1. Engagements pris par la République de Corée

Dans le cadre de la Convention d'Accord de don sus-évoquée, la République de Corée s'est engagée à :

effectuer des survey d'implémentation du système PKI au Cameroun ;

sélectionner un PMC (Project Management Coordinator) pour coordonner les activités des entreprises impliquées dans l'exécution du Projet PKI ;

élaborer un plan directeur pour le projet ;

mener une consultation sur le plan juridique et réglementaire au Cameroun ;

fournir les équipements du système PKI en vue de l'implémentation d'une Autorité de Certification Racine et d'une Autorité de Certification Gouvernementale ;

assurer la formation du personnel choisi par la partie camerounaise et suivre la réalisation du Projet PKI ;

installer et à configurer les équipements et le système PKI fourni ;

former les camerounais en charge de la mise en œuvre du projet en Corée et au Cameroun ;

assister la partie camerounaise dans l'organisation et l'animation des séminaires au Cameroun ;

assister le Cameroun dans la maintenance du système pendant deux ans, après l'installation de la plateforme de sécurité.

3.1.2. Engagements pris par la République du Cameroun

Dans le cadre de la Convention d'Accord de don sus-évoquée, la République du Cameroun s'est engagée à :

élaborer et à publier une loi relative à la signature électronique et les textes réglementaires subséquents. A cet effet, la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun ainsi que la loi n°2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun ont

vu le jour. Ces deux lois contiennent quelques aspects relatifs à la signature électronique. Des textes réglementaires en application des lois sus-citées ont également été signés. Il s'agit notamment de :

le Décret n°2012/1318/PM du 22 mai 2012 fixant les conditions et les modalités d'octroi de l'autorisation d'exercice de l'activité de certification électronique ;

le Décret n°2012/1643/PM du 14 juin 2012 fixant les conditions et les modalités d'audit de sécurité obligatoire des réseaux de communications électroniques et des systèmes d'information ;

le Décret du Président de la République n°2012/309 du 26 juin 2012 fixant les modalités de gestion du Fonds Spécial des Activités de Sécurité Electronique ;

l'Arrêté n°00014/MINPOSTEL du 27 juin 2012 fixant les critères de qualification des certificats et les caractéristiques techniques du dispositif de création des signatures électroniques ;

mettre à la disposition du projet un bâtiment sécurisé, pour abriter les équipements du système PKI suivant les normes internationales en la matière. C'est ainsi que le bâtiment situé entre la Poste Centrale et AES-SONEL Centrale, a été mis à la disposition du Projet PKI par le MINPOSTEL ;

mettre en place une "Task Force Team", chargée du suivi de l'exécution du Projet PKI. Elle a vu le jour par décision n°00000220/MINPOSTEL du 30 juillet 2010, modifiée et complétée par la décision n°00000272/MINPOSTEL du 29 novembre 2010 ;

désigner les responsables chargés de l'exécution du Projet PKI. C'est ainsi que les responsables suivants ont été nommés. Il s'agit de messieurs :

NANA YOMBA Lucien, Coordonnateur Général chargé des affaires administratives du Projet ;

ESSIANE ELLA Justin, Coordonnateur Technique du Projet ;

NSONGAN ETUNG Joseph, Manager du Projet, chargé des affaires financières.

publier les textes relatifs aux normes et conditions d'utilisation des certificats ;

prendre en charge les droits de douane et autres taxes d'affranchissement des équipements du système PKI. Cela a été réalisé grâce à une exonération accordée par le MINFI ;

assurer le transport des équipements du port autonome de Douala jusqu'à Yaoundé ;

assurer le magasinage sécurisé des équipements ;

fournir les fonds de contrepartie pour réaliser certaines activités nécessaires à l'exécution du projet PKI au Cameroun ;

organiser des séminaires de formation et ateliers sur site au Cameroun ;

organiser une cérémonie d'inauguration officielle. Elle s'est tenue le 29 octobre 2012 ;

organiser des campagnes de promotion, de vulgarisation et de déploiement du système PKI à travers tout le territoire national.

Cette Convention est entrée en vigueur, par échange de Notes Verbales signées respectivement, le 14 octobre 2010, par le Ministère des Affaires étrangères de la République de Corée et le 28 décembre 2010, par le Ministère des Relations Extérieures de la République du Cameroun, entérinant ainsi l'Accord de don signé le 08 septembre 2010.

La réalisation du projet de mise en œuvre d'une Infrastructure Nationale à Clé Publique au Cameroun a nécessité la mobilisation d'importantes ressources humaines tant côté coréen que camerounais. Onze ingénieurs Camerounais ont été sélectionnés, pour faire partie de l'équipe technique de réalisation dudit projet. Ils ont été formés par les Coréens, pendant sept mois qu'a durée l'implémentation du système de sécurité. La répartition par administration représentée dans cette équipe technique se présente comme suit : ANTIC (07), MINPOSTEL (02) dont le Coordonnateur Technique du projet, CAMPOST (01) et GUCE (01).

Toutes les étapes sus-citées ont été réalisées avec succès par l'équipe de projet.

Le Centre PKI a été inauguré le 29 octobre 2012, au cours d'une cérémonie présidée par le Ministre des Postes et Télécommunications représentant le Premier Ministre, empêché.

Conclusion

Le Gouvernement a décerné une médaille à Monsieur le Directeur Général de l'ANTIC Dr. EBOT EBOT ENAW et lui a rétrocédé le Centre PKI pour le gérer. Aujourd'hui, outre l'application e-GUCE, l'application e-Procurement du Ministère des Marchés Publics et l'application OSCAR de la Douala International Terminal ont également été sécurisées par les ingénieurs de l'ANTIC. C'est le lieu de rappeler ici que les Institutions de l'Etat, les départements ministériels, les établissements publics administratifs et entreprises sont conviés à solliciter l'ANTIC pour faire sécuriser leurs applications.

L'on doit avoir présent à l'esprit que la sécurité coûte chère mais la réparation des dégâts aux termes d'une cyberattaque coûte encore plus chère ! ! !

Source : https://camgovca.cm/fr/accueil/historique.html