BCEAO
BANQUE CENTRALE DES ÉTATS DE L'AFRIQUE DE L'OUEST

Dakar, le 15 septembre 2021

Avis N°2

Publication de réponses aux questions formulées dans le cadre de l'Appel d'Offres N°AO/Z00/DBA/033/08/2021 relatif à la fourniture d'Infrastructure de Gestion de Clés Publiques (PKI)

Questions	Réponses
Combien d'utilisateurs/d'appareils allez-vous sécuriser ? Signature d'e-mails ? Authentification Wi-Fi ? Accès VPN ? Gestion des appareils mobiles ? Pour quelles fonctions principales avez-vous besoin de la solution PKI ?	La mise en place de l'infrastructure à clés publiques devra permettre de fédérer les autorités de certification existantes. Il est attendu que la solution proposée réponde aux besoins suivants : - La sécurisation de la messagerie ; - La sécurisation des applications WEB: par l'émission de certificats ssl/tls. - L'authentification au réseau : Les postes de travail et utilisateurs utilisent des certificats pour s'authentifier sur le réseau. Le besoin est estimé à 3500 certificats à minima. - L'authentification des équipements réseaux. Le besoin est évalué pour au moins 100 équipements réseau. - L'authentification des participants (banques primaires...) pour au moins 1200 certificats. - L'authentification pour l'établissement de VPN pour 350 certificats à minima. La solution proposée devra être évolutive (adaptation aux besoins futurs) et flexible (intégration\interfaçage API) tout en répondant aux exigences fonctionnelles décrites.
Y a-t-il une relation d'approbation entre les différentes forêts ?	Il n'est pas prévu de relation d'approbation entre les différentes forêts.

Avenue Abdoulaye FADIGA
BP 3108 – Dakar - Sénégal

Tél. (221) 33 839 05 00 / Fax. (221) 33 823 93 35
courrier.bceao@bceao.int - www.bceao.int

Combien d'utilisateurs doivent être authentifiés ? (veuillez noter qu'un siège d'utilisateur peut être utilisé pour authentifier l'utilisateur sur plusieurs appareils)	Le nombre d'utilisateurs peut être réparti comme suit : - un Siège avec près de 800 utilisateurs ; - huit Agences Principales avec en moyenne 235 utilisateurs par agence ; - dix-sept Agences Auxiliaires avec en moyenne 100 utilisateurs par agence ; - deux sites spécifiques avec en moyenne 100 utilisateurs par agence ; - une représentation avec moins de 10 utilisateurs.
Combien d'appareils doivent être authentifiés ? (les sièges de l'appareil s'authentifient sur l'appareil uniquement)	Le nombre d'appareils à authentifier est de 3000 au minimum.
Combien d'autorités de certification racine privées sont nécessaires ?(conception PKI	Le nombre d'autorités de certification racine est laissé à l'appréciation du soumissionnaire.
Combien d'autorités de certification émettrices intermédiaires sont nécessaires ?	Le nombre d'autorités de certification racine est laissé à l'appréciation du soumissionnaire tout en considérant les besoins exprimés.
Souhaitez-vous que nous fournissons le matériel HSM ?	Selon l'architecture proposée, le soumissionnaire est appelé à inclure dans son offre l'acquisition de matériels ou composants nécessaires à la mise en place de ladite architecture.
Incluons-nous la reprise après sinistre ?	L'infrastructure à mettre en place doit être hautement disponible, donc permettre une reprise après sinistre.
Combien d'heures/jours de formation et de services professionnels sont nécessaires?	Les détails de la formation sont laissés à l'appréciation du soumissionnaire tout en respectant les spécifications de l'appel d'offres.
Est-ce que la PKI demandée doit générer également des certificats sur carte à puce ou tokens cryptographiques matériels ?	Cette fonctionnalité pourrait être proposée en option.
Les autorités de certifications LWPKI, ZOM-CA, SICA-CA et RASP-PKI sont-elles indépendantes les unes par rapport aux autres ? Existe t'il un lien hiérarchique entre elles ?	Seules les autorités LWPKI et RASP-PKI sont dépendantes. La LWPKI étant l'autorité de certification racine. Les autres sont des autorités de certifications indépendantes.

Que signifie SFD ?	SFD (Systèmes Financiers Décentralisés) c'est à dire Etablissements de microfinance ou de micro-crédits.
Comment est sécurisée la messagerie interne ? Chaque utilisateur de la messagerie a-t-il un certificat ou seul le serveur SMTP en utilise 1 ?	Le certificat est installé au niveau du serveur. Les utilisateurs ne disposent pas de certificat.
" En termes de PKI, la Banque dispose aujourd'hui ... d'un (1) certificat délivré par Digicert décrit ci-après : "Est-ce le même certificat digicert qui est utilisé pour sécuriser la messagerie et les applications web ?"	Faire une proposition qui couvre les besoins spécifiés.
Où et comment sont stockées les clés privées des Autorités CA ?	Elles sont stockées en local.
Que signifie Enterprise CA ?	Autorité de certification d'entreprise, elle est adossée à un domaine Active Directory. Il s'agit d'une terminologie Microsoft.
Que signifie Self Root CA ?	Certificat auto-signé
Est-t-il nécessaire que le HSM hors ligne soit suffisamment compact pour être stocké dans un coffre-fort ?	Le choix est laissé au soumissionnaire de proposer la meilleure solution. Il peut proposer des fonctionnalités en option.
Puisque nous n'avons pas une idée sur les exigences de scalabilité et de performances requises pour l'infrastructure existante/future, auriez-vous besoin que les performances du HSM supporte le passage de 400+ à 8000+ signatures RSA-2048 avec seulement une mise à niveau de la licence ?	Le choix est laissé au soumissionnaire de proposer la meilleure solution. Il peut proposer des fonctionnalités en option.
Exigez-vous que le logiciel CA soit certifié ou en cours de certification CC/FIPS ?	La certification CC/FIPS pourrait être proposée en option.
Tous les logiciels et matériels doivent être fournis, sans s'y limiter, les éléments	Une architecture virtualisée serait plus adaptée, la banque disposant déjà d'un datacenter pouvant

suivants : ● RACK avec serrure biométrique ; ● SERVEURS pour les CA en ligne avec virtualisation ; ● HSM pour les CA hors ligne ; ● HSMs réseau ; ● NTP ; ● LAPTOPS pour CAs hors ligne ; ● Stations d'administration ; ● Coffre-fort pour le stockage sécurisé sur site/hors site ; ● Sacs de preuves inviolables (Tamper evident bags) ; ● Clés USB FIPS.	accueillir les machines virtuelles.
Les contrôles suivants sont-ils mis en place ? Le cas contraire, faudrait-il que le soumissionnaire les inclût dans l'offre ? ● Système HVAC ● Coupure de courant ● Exposition à l'eau ● Prévention et protection contre l'incendie ● Élimination sécurisée des déchets ● Accès sécurisé à la salle PKI ● Sauvegarde hors site	Le présent cahier de charges ne couvre pas les contrôles physiques au centre de données.
Les équipements de sécurité (tels que l'anti-virus, les pare-feu, IPS, WAF, … etc) seront-ils fournis par la BCEAO ?	Le présent cahier de charges ne couvre pas l'acquisition des équipements de sécurité cités.
Combien d'utilisateurs auront besoin d'un Digital ID ? Combien de certificats SSL privés devront être émis ? Souhaitez-vous acquérir un certificat SSL public ? Le cas échéant, combien ? Avez-vous besoin d'un portail unique où vous pouvez gérer les certificats PKI	La BCEAO dispose actuellement d'une centaine d'applications. Il n'est pas prévu une acquisition de certificat SSL public.

publique, d'entreprise émanant du même éditeur ainsi que la PKI de Microsoft ?	
Quelle est la PKI actuellement déployée ? (Editeur/Version)	Les autorités de certification existantes sont déployées avec Microsoft ADCS (2016/2019)
Quel est le plan de migration prévu pour la PKI actuelle ? ● Migration progressive et réémission de tous les certificats actuellement déployés ? ● Co-habitation des deux PKI et réémission à l'expiration du certificat sur la nouvelle PKI ?	Il est prévu une migration progressive et une réémission de tous les certificats actuellement déployés.
Pour l'intégration aux systèmes de paiement : ● Quels sont les cas d'utilisation actuels/prévus ? ● Quelle est la procédure actuelle pour la génération et la mise à jour des clés ? ● Quelle est la procédure prévue pour la génération et la mise à jour des clés ? Délivrance et gestion des certificats : ● Exigez-vous que le logiciel de l'AC supporte les protocoles suivants SCEP, EST, CMP pour l'émission et la gestion des certificats ?	Il s’agira de générer des certificats aux utilisateurs pour le chiffrage des flux échangés.
Exigez-vous que la gestion des	Faire une proposition

utilisateurs se fasse à l'aide d'une interface Web ? Souhaitez-vous restreindre l'accès au portail de gestion des utilisateurs par le biais de l'authentification sécurisée via des certificats X.509 ?	
Exigez-vous que la PKI dispose d'un portail libre-service et supporte les actions suivantes : - Auto-inscription (self-enrollment) des utilisateurs ; - Délivrance de Digital IDs ; - Révocation de certificats.	Faire une proposition
Exigez-vous un service qui scanne votre réseau pour détecter tous les certificats de serveur public/privé et vous avertir lorsque ces certificats sont sur le point d'expirer ?	Faire une proposition

Exigez-vous que le logiciel CA prenne en charge l'intégration avec les fournisseurs MDM suivants : - Microsoft Intune ; - VMWare AirWatch ; - MobileIron ; - SAP Afaria ; - SOTI MobiControl ; - BlackBerry ; - IBM MobileFirst Protect (MaaS360).	La comptabilité avec les solutions MDM serait un atout important.
Exigez-vous un client de bureau qui offre les fonctionnalités suivantes : - Stockage sécurisé des clés privées et des certificats ; - Stockage de l'historique des clés de chiffrement de l'utilisateur final ; - Signature/chiffrement des fichiers ; - Suppression sécurisée ; - Fonctionne sur Mac OS et Windows.	Non
Exigez-vous un plugin pour Outlook afin d'effectuer un chiffrement de bout en bout /une signature numérique des courriels ?	Non
Exigez-vous que les utilisateurs finaux aient accès à leurs profils numériques à distance et en toute sécurité ?	Non

Exigez-vous que le logiciel de l'AC génère des politiques de certificats pour garantir que les actions de certification sont conformes aux politiques organisationnelles ? Exigez-vous que le logiciel de CA offre la possibilité de sauvegarder et de récupérer l'historique de toutes les clés de chiffrement privées d'un utilisateur final ?	oui
Exigez-vous un enregistrement automatique (Auto-Enrollment) des clés et des certificats sur les clients Desktop Windows?	Oui
Exigez-vous que le logiciel de l'AC supporte les commandes en masse (bulk commands) pour l'enregistrement des utilisateurs, l'activation des certificats, la révocation, ...etc ?	Oui
Exigez-vous un serveur OCSP pour valider le statut de révocation des certificats en temps réel ?	Oui
Afin de faciliter le dépannage (troubleshooting) et le support, Exigez-vous que le logiciel de l'AC et le HSM proviennent du même fournisseur ?	Il est préférable que cela provienne du même fournisseur tout en garantissant le meilleur rapport qualité-prix