Réseau des Centres d'Excellence de l'UIT pour l'Afrique

Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC)

Cours en ligne

Sécurité des applications d'Internet et de Mobile Banking

Du 02 au 28 novembre 2020

PRESENTATION DE LA FORMATION

DESCRIPTION DU COURS

Titre	**Sécurité des applications d'Internet et de Mobile Banking**
Objectifs	Cet atelier a pour objectif de présenter les normes, les concepts de base et les bonnes pratiques liées à la sécurité des services électroniques bancaires. Il permettra aux participants de maitriser les risques liés aux services électroniques d'Internet et de Mobile Banking et d'identifier les solutions techniques adéquates pour remédier à ces risques tel que la certification électronique des échanges et des divers acteurs, les techniques de chiffrement, les mécanismes de signatures et d'horodatage électronique des actes faits en ligne. Cet atelier met l'accent sur : ▪ La fiabilité des documents et des preuves électroniques à valeurs probantes ; ▪ L'efficacité des diverses solutions de gestion et de conservation de ces preuves ; ▪ Les standards de signatures électroniques basiques et avancées et leurs modes et domaines d'utilisation (CMS, CAdES, S/MIME, XMLDSig, XAdES, PDF [ISO 32000-1] et PAdES [ETSI TS 102778]) ; ▪ les techniques de hachage et de chiffrement ainsi que les solutions matérielles d'authentification et de signature tel que les HSM (Hardware Security Module), les cartes à puce cryptographiques, les disques Worm, les jetons OTP d'authentification, l'authentification MFA et la biométrie. **Prérequis :** Une connaissance des bases de la sécurité est souhaitable pour tirer un meilleur profit de cette formation.
Dates	Du 02 au 28 novembre 2020
Durée	4 semaines
Date limite d'enregistrement	19 octobre 2020
Frais de formation	350 USD / 200 000 F CFA (XOF et XAF)
Code du cours	20OI24861AFR-F

RESULTATS ATTENDUS

Aux termes de l'atelier, les auditeurs seront capables de :

- connaître les enjeux techniques, économiques et juridiques et les challenges de la dématérialisation des services bancaires ;
- identifier les menaces et les risques potentiels liés aux échanges électroniques ;
- Maîtriser les solutions techniques à mettre en place pour la sécurisation des transactions électroniques (chiffrement, signature, horodatage, traitement et archivage sécurisée des documents et des preuves électroniques) ;
- recenser les différentes modalités de mise en œuvre des divers solutions techniques, en fonction des usages ;
- identifier les solutions disponibles sur le marché (cartographie des acteurs et des outils) ;
- disposer d'exemples concrets et éprouvés d'architectures fonctionnelles et techniques.

PUBLIC CIBLE

Cet atelier de formation s'adresse principalement aux profils suivants :

- Directeur des Services Informatiques (DSI) ;
- Responsable de Sécurité des Systèmes d'Information (RSSI) ;
- Consultant, experts et auditeurs en sécurité ;
- Enseignants, chercheurs et étudiants en sécurité.

FORMATEUR

NOM DU FORMATEUR	CONTACTS
Nizar BEN NEJI est un Docteur en Technologies de l'Information et de la Communication (TIC) de l'université de Carthage. Il est également un expert travaillant avec l'UIT (Union Internationale des Télécommunications), la CTO (Commonwealth Telecom Organization) et l'AICTO (Organisation Arabe des Technologies de l'Information et des Télécommunications.	nizar.benneji@fsb.rnu.tn / nizarbenneji@gmail.com

EVALUATION

- **Quiz** à la fin de chaque semaine, un quiz sera proposé, contenant des questions à choix multiples (QCM) en relation avec le cours de la semaine.
- **Etude de cas :** assignement individuel ou en groupe.

AGENDA

Semaine/ session	Activités	Exercices et interactions
Semaine 1	***Nouvelles opportunités et limites liées à la sécurité des services bancaires*** ▪ Dématérialisation des services et les éventuels risques de sécurité ▪ Fidélité à la sécurité offerte au niveau des services classiques o Authentification face à face o Vérification des pièces d'identité o Vérification du spécimen de signature o Cachet, date et signature sur chèque ▪ Etat des lieux de la sécurité des transactions électroniques à l'échelle Africain et Mondial. o Statistiques sur les cyberattaques o Etudes de cas pratiques de cyber incidents et de fraudes électroniques o Coût et dégâts engendrés par les fraudes électroniques ▪ Etat des lieux de la sécurité des services bancaires à l'échelle mondial ▪ Benchmark des solutions de banque en ligne à l'échelle mondial ▪ Services bancaires informationnels et transactionnels ▪ Limites spatiales et temporelles ▪ Interaction avec d'autres services tiers (e-commerce, e-gouvernement, ...) ***Référentiels et services de sécurité à assurer*** ▪ Référentiels et Standards de la Sécurité pour les services bancaires ▪ Services de sécurité à assurer et les divers Techniques de sécurisation : o Authentification multi facteurs, identification et autorisation ; o Confidentialité des échanges ; o Intégrité des communications et des systèmes ; o Non-répudiation des actes électroniques ; o Haute disponibilité des services électroniques ; o Pérennité et valeur probante des archives et des documents conservés o Traçabilité des événements.	**Quiz semaine 1**
Semaine 2	***Techniques d'Authentification*** ▪ Facteurs d'authentification ▪ Types d'authentification o basées sur les mots de passe o basées sur les certificats ▪ Applications d'authentification : o Authentification SSL/TLS (Simple et Mutuelle) o Authentification SSO (Single Sign On) o Authentification OTP (One Time Password) à très courte durée Authentification VPN (Site-to-site et Client-to-site) o Protocole RADIUS (Remote Authentication Dial-In User Service) o Protocole Kerberos o CHAP (Challenge-Handshake Authentication Protocol) o PAP (Password Authentication Protocol) Authentification M of N	**Quiz semaine 2**

Semaine 3	***Solutions Cryptographiques*** ▪ Hachage Cryptographique. ▪ Techniques de chiffrement et choix des algorithmes et de la taille des clés : o Symétrique (AES, DES, 3DES, ...), o Asymétrique (RSA, DSA, ECC, ...) et o Hybride (SSL/TLS, S/MIME, ...): ▪ Infrastructure à Clés Publiques (ICP) et services mis à disposition pour validation des certificats électroniques ▪ Usage des Certificats Electroniques (UIT-T X.509) ▪ Standards PKCS#1 à 15 ▪ Cas d'utilisation des certificats électroniques : o Cas du SSL/TLS : Sécurisation des protocoles sans chiffrement (HTTPS, SMTPS, IMAPS, POPS, LDAPS, FTPS) o Cas du S/MIME : Sécurisation du courrier électronique o Cas du VPN SSL : Sécurisation des liaisons site-to-site et client-to-site ***Normes et méthodologies de gestion des risques de sécurité*** ▪ Norme ISO/IEC 27005 ▪ Méthodologie EBIOS ▪ Méthodologie MEHARI ***Horodatage Electronique*** ▪ Sources de temps fiable et service NTP ▪ Prestataires de service d'horodatage ▪ Autorité d'horodatage ▪ Politique d'horodatage ▪ Requête et réponse d'horodatage ▪ Cachet électronique et contremarque de temps ▪ Domaines d'application de l'horodatage électronique	**Quiz semaine 3**
Semaine 4	***Archivage Electronique Sécurisé*** ▪ Stockage et conservation des documents et des preuves électroniques : formats et outils ▪ Service de sécurité à assurer : o Pérennité ; o Authenticité ; o Intégrité ; o Confidentialité. ▪ Architecture de base d'une solution d'archivage ▪ Panorama de solutions matérielles et progicielles : solution interne ou externalisation ***Audit et évaluation de la sécurité des services électroniques bancaires :*** ▪ Audit SSL/TLS ▪ Audit des vulnérabilités Web et Mobile ▪ Tests intrusifs / Exploits ▪ Test de montée en charge ▪ Référentiels OWASP ▪ Outillage d'évaluation et d'audit ***Autres outils et services électroniques*** ▪ Identification électronique ▪ Technologie du mobile (Mobile ID, Mobile Signature, Mobile PKI, M-payment, ...) ▪ Facturation électronique ▪ Paiement électronique ▪ Contrat et engagement électronique	**Quiz semaine 4**

	Evaluation des auditeurs et clôture de la formation.	

METHODOLOGIE

Présentations, travaux pratiques, étude de cas et échanges interactifs entre formateurs et participants.

COORDINATION DE LA FORMATION

Coordinateur de la formation :	**Coordinateur de l'UIT :**
Nom : Rodolphe Kossonou Chef du Service de la Formation Continue, ESATIC Tel. : + 225 21 218 100 Fax : + 225 51 400145 Email : rodolphe.kossonou@esatic.edu.ci	Nom : M. Emmanuel Niyikora Responsable de Programme, bureau de zone UIT pour l'Afrique de l'Ouest, Dakar Tel : +250 788312939 Email: emmanuel.niyikora@itu.int

INSCRIPTION ET PAIEMENT

Inscription sur le portail de l'ITU Académie :

L'inscription et le paiement doivent se faire en ligne sur le portail web de l'ITU Académie. Afin de pouvoir vous inscrire à un cours vous **devez** au préalable créer un compte sur le portail web d'ITU Académie à l'adresse suivante : https://academy.itu.int/index.php/user/register

Inscription à une formation :

Si vous avez déjà un compte ou que vous créez un nouveau compte, vous pouvez vous inscrire en ligne pour la formation à l'adresse suivante :
https://academy.itu.int/training-courses/full-catalogue/securite-des-applications-dinternet-et-de-mobile-banking-0

Vous pouvez également vous inscrire en trouvant le cours qui vous intéresse dans notre catalogue de formation
https://academy.itu.int/index.php/training-courses/full-catalogue

Paiement

1. **Paiement en ligne**

Les frais de participation à cette formation sont de **350 USD**. Ce montant prend en compte l'inscription, la documentation, la pause-café et le déjeuner. Il est recommandé de procéder au paiement via le système de paiement en ligne en utilisant le même lien que celui de l'inscription en ligne :
https://academy.itu.int/training-courses/full-catalogue/securite-des-applications-dinternet-et-de-mobile-banking-0

2. **Paiement par virement bancaire**

Lorsqu'il n'est pas possible d'effectuer un paiement via le système en ligne, sélectionnez l'option de paiement hors ligne ''offline'' pour générer une facture en utilisant le même lien que ci-dessus. Téléchargez la facture pour effectuer un virement sur le compte bancaire de l'UIT indiqué ci-dessous. Envoyez ensuite la preuve de paiement / la copie du bordereau de virement et la copie de la facture à Hcbmail@itu.intet mettre en copie le coordinateur du cours. **Tous les frais de transaction bancaire doivent être à la charge du payeur**. **Si les documents ci-dessus ne sont pas soumis, le candidat pourrait ne pas être inscrit à la formation**.

3. **Paiement par groupe**

Si vous souhaitez payer pour plus d'un participant par virement bancaire et que vous avez besoin d'une facture pour tous, créez un compte comme **contact institutionnel.** Les contacts institutionnels sont des utilisateurs qui

représentent une organisation. Tout étudiant peut demander à être un contact institutionnel ou à appartenir à une organisation existante.

Pour ce faire, accédez à la page de votre profil en cliquant sur le bouton **"My account"** dans le menu de l'utilisateur. Au bas de cette page, vous devriez voir deux boutons :

a. Si vous souhaitez **devenir un contact institutionnel**, cliquez sur le bouton "**Apply to be an Institutional Contact"**. Cela vous redirigera vers un petit formulaire qui vous demandera le nom de l'organisation. Une fois que vous avez renseigné le nom de l'organisation que vous souhaitez représenter, cliquez sur **"continue",** une demande est alors créée. Un responsable de l'Académie de l'UIT examinera manuellement cette demande et l'acceptera ou la refusera en conséquence.

b. Si vous souhaitez **appartenir à une organisation existante**, cliquez sur le bouton **"Request to belong to an Institutional Contact"**. Cela vous redirigera vers un petit formulaire qui vous demandera de sélectionner l'organisation à laquelle vous souhaitez appartenir à partir d'une liste d'organisations. Après avoir sélectionné la bonne organisation et cliqué sur **"continue"**, une demande sera créée. Le contact institutionnel qui représente cette organisation acceptera ou refusera manuellement votre demande d'adhésion à l'organisation.

Coordonnées bancaires de l'UIT :

Nom et addresse de la Banque :	UBS SWITZERLAND AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiaire:	Union Internationale des Télécommunications
Numero de Compte :	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Montant :	350 USD
Reference du paiement :	CoE-AFR 24861 - P.40590.1.04

4. Autres méthodes de paiement

Si pour des raisons de régulations nationales il y a des restrictions ne permettant pas d'utiliser les options de paiement 1 et 2 ci-dessus, veuillez contacter le coordinateur de l'UIT pour plus d'assistance.