CNFCPP	**FICHE PROGRAMME D'UNE ACTION DE FORMATION**	Réf: **FORM.FINC.02** Version : 00 Date d'application : 20/04/09

Thème : Sécurité des applications Internet et Mobile Banking: E-Banking et M-Banking

Population cible : Responsables des Systèmes d'Information ;
Consultant, Experts et Auditeurs en sécurité.

Objectifs de le formation :	**Objectifs pédagogiques :**
Cet atelier a pour objectif de présenter les normes, les concepts de base et les bonnes pratiques liées à la sécurité des transactions électroniques bancaires. Il permettra aux participants de maitriser les risques liés aux services électroniques et identifier les solutions techniques adéquates pour remédier à ces risques tel que la certification électronique, les techniques de chiffrement, les mécanismes de signatures et d'horodatage électronique des transactions. Cet atelier met l'accent sur la fiabilité des documents et des preuves électroniques à valeurs probantes et les divers 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 divers techniques de hachage et de chiffrement ainsi que les solutions matériels tel que les HSM (Hardware Security Module), les cartes à puce intelligentes, les disques Worm et les jetons d'authentification.	Connaissance basique des systèmes et des réseaux informatiques.

Jours	**Contenus/ Concepts clés à aborder**	**Méthodes et Moyens Pédagogiques**	**Durée (Heures)**	
			Théorie	**Pratique**
J1	Accueil, enregistrement et ouverture du séminaire <u>Introduction</u> (1) ▪ Dématérialisation des services et les éventuels risques de sécurité ▪ Etat des lieux de la sécurité des transactions électroniques à l'échelle Africain et Mondial. o Statistiques sur les cybers attaques o Etudes de cas pratiques de cyber incidents et de fraudes électroniques o Coût et dégâts engendrés par les fraudes électroniques Référentiels et Standards de la Sécurité	Exposés, travaux pratiques et échanges interactifs.	**3**	**3**

	Introduction (2) ▪ Services de sécurité à assurer et les divers Techniques de sécurisation: o Authentification, Identification et autorisation; o Confidentialité des échanges; o Intégrité des communications; o Non-répudiation des actes; o Haute disponibilité des services électroniques; o Traçabilité des événements.			
J2	. Techniques d'Authentification (1) ▪ Facteurs d'authentification ▪ Types d'authentification o basés sur les mots de passe o basés 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 o Authentification VPN (Site-to-site et Client-to-site) Techniques d'Authentification (2) o Protocole RADIUS (Remote Authentication Dial-In User Service) o Protocole Kerberos o CHAP (Challenge-Handshake Authentication Protocol) o PAP (Password Authentication Protocol) o Authentification M parmi N	Exposés, travaux pratiques et échanges interactifs.	**3**	**3**
J3	Solutions Cryptographiques (1) ▪ 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	Exposés, travaux pratiques et échanges interactifs.	**3**	**3**

	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 <u>Solutions Cryptographiques</u> (2) ▪ Signature Electronique: Principe de base, Attributs, Types et Durée de vie des signatures électroniques. ▪ Politique de Signature ▪ Signature électronique multiple: o Hiérarchique; o Co-signature. ▪ Formats des signatures électroniques: o CMS (Cryptographic Message Syntax); o CAdES (CMS Advanced Electronic Signatures); o S/MIME (Secure Multipurpose Internet Mail Extensions); o XMLDSig (XML Digital Signature); o XAdES (XML Advanced Electronic Signature); o PDF[ISO 32000-1] (PDF Signature); o PAdES [ETSI TS 102778]) (PDF Advanced Electronic Signature). ▪ Scellement des données (Cachet serveur) ▪ Cas d'utilisation des signatures électroniques: o Signature des formulaires Web o Signature des documents XML o Signature des documents PDF o Signature des courriers électroniques			
J4	<u>Horodatage Electronique</u> ▪ Source 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	Exposés, travaux pratiques et échanges interactifs.	**3**	**3**

	électronique <u>Archivage Electronique Sécurisé</u> ▪ 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 des solutions matérielles et logicielles			
J5	<u>Autres outils et services électroniques</u> ▪ Identification électronique ▪ Technologie du mobile (Mobile ID, Mobile Signature, Mobile PKI, M-payment, ...) ▪ Facturation électronique ▪ Paiement électronique ▪ Contrat électronique Evaluation des auditeurs Evaluation du séminaire, remise des attestations et clôture de l'atelier.	Exposés, travaux pratiques et échanges interactifs.	2h	**2h**
Total			**14h**	**14h**

Critères et indicateurs d'évaluation QCM

NB : *Fiche à établir par l'opérateur de formation*

Case réservée à l'administration :

Avis technique : ……

……

……

Fait à ……. le ……..Signature

المركز الوطني للتكوين المستمر والترقية المهنية CNFCPP	**FICHE PROGRAMME D'UNE ACTION DE FORMATION**	Réf: **FORM.FINC.02** Version : 00 Date d'application : 20/04/09