

Les formations de L'INFORMATIQUE COMMUNICANTE en infrastructures et systèmes IT



Les formations de L'INFORMATIQUE COMMUNICANTE (LIC) permettent d'acquérir l'essentiel des méthodes et des technologies utilisées dans les infrastructures et systèmes de communication et de transactions électroniques. Elles s'adressent à des Ingénieurs, des Techniciens, des Décideurs ou des Commerciaux.

Elles peuvent être organisées de manière indépendante ou groupée.

Les formations s'appuient sur un contenu de référence qui adhère en permanence à l'évolution de la technologie et de la normalisation.

Des formateurs qualifiés

Tous nos formateurs sont des ingénieurs et consultants aux qualités pédagogiques éprouvées. Ils possèdent la compétence fonctionnelle, technique et la connaissance des systèmes de communications et des réseaux.

Outils et supports

La formation théorique est dispensée à l'aide d'un PC portable, au moyen d'un vidéo-projecteur.

Un support de présentation enrichi de nombreux commentaires et de tout autre document pertinent, est fourni aux participants.

Travaux pratiques

Ces formations sont complétées par des exercices, travaux dirigés et pratiques qui permettent aux participants de consolider concrètement leurs acquis théoriques.

Les travaux pratiques sont effectués à l'aide d'outils de génération et d'analyse de trafic

Durée des sessions

Chaque session dure de 1 à 5 jours (voire plus) selon l'approfondissement souhaité.

L'INFORMATIQUE COMMUNICANTE assure aussi des variantes des formations de référence (personnalisation de la durée et du contenu des sessions) ou des formations sur d'autres thématiques d'infrastructure.

Lieu des formations

Les sessions ont lieu dans le Centre de Séminaires LIC d'Issy-les-Moulineaux (déjeuner assuré et pauses café) ... mais elles peuvent aussi se tenir ailleurs à la demande.

Nous consulter au + 33 1 46 62 91 00 – formations@lic.fr

Agrément de L'INFORMATIQUE COMMUNICANTE

LIC est agréée par le Contrôle de la Formation Professionnelle sous le n° 11920653792.

Tarifs des formations

La base de tarif est de **500 € H.T.** par jour et par participant

Sommaire

F1.	Infrastructures informatiques et dématérialisation _____	4
F1.1.	Infrastructures informatiques : du serveur au poste de travail _____	4
F1.2.	Dématérialisation _____	6
F1.3.	Archivage sécurisé _____	7
F1.4.	PKI, cryptage, Signature électronique _____	8
F1.5.	Méthodes utilisées dans les Systèmes d'Information _____	9
F2.	Systèmes de communication et réseaux d'entreprise _____	10
F2.1.	Infrastructures de réseaux locaux et réseaux IP _____	10
F2.2.	Téléphonie sur IP – communications unifiées : l'essentiel _____	12
F2.3.	Téléphonie sur IP - communications unifiées : approfondissement _____	13
F2.4.	Systèmes de Communication d'entreprise _____	15
F2.5.	Administration de réseaux _____	16
F3.	Sécurité des Systèmes d'information et des réseaux _____	17
F3.1.	Sensibilisation à la sécurité de l'information _____	17
F3.2.	Architectures de défense globale de sécurité _____	18
F3.3.	Mise en place d'un Plan Directeur de Sécurité (PSI, SMSI, Audit) _____	19
F3.4.	Authentification et PKI en environnement ouvert _____	20
F3.5.	Migration de Windows à Linux _____	22
F3.6.	Sécurité des Systèmes d'information : la norme ISO 27001 _____	23
F3.7.	Gestion des identités et authentification _____	24
F3.8.	PRA/PCA _____	25
F4.	Télécommunications _____	27
F4.1.	Introduction aux réseaux et télécommunications _____	27
F4.2.	Télévision sur DSL et triple play _____	29
F5.	Radio-communications _____	30
F5.1.	Introduction aux réseaux radio _____	30
F5.2.	L'essentiel des réseaux Wi-Fi _____	31
F5.3.	Les réseaux WiFi – session approfondie _____	32
F5.4.	Applications mobiles : cartes SIM / USIM _____	33
F6.	TES : Transactions Electroniques et monétique _____	34
F6.1.	Monétique : fonctions – architecture - EMV _____	34
F6.2.	EMV : spécifications et certification _____	35
F6.3.	Les technologies sans contact et NFC _____	36
F6.4.	NFC : Near Field Communications _____	37

F1. Infrastructures informatiques et dématérialisation

F1.1. Infrastructures informatiques : du serveur au poste de travail

Durée standard : 2 jours

La gestion des infrastructures informatiques, du data center au poste de travail, vit en parallèle plusieurs révolutions : la virtualisation, le « cloud computing », les logiciels SaaS, le Web 2.0, la cohabitation de facto entre Microsoft et les logiciels libres, l'informatique verte ...

Gérer l'environnement de travail des utilisateurs

- ◆ Déployer instantanément et de manière sécurisée de nouveaux postes ou applications virtuels
- ◆ Protocole d'affichage optimisé PCoIP
- ◆ Migration des postes de travail ou applications vers Windows 7
- ◆ État des lieux des standards Web Services : SOAP, WSDL, UDDI et les Web Services
- ◆ Intérêts et limites des Web Services pour intégrer les applications existantes.

Gérer le datacenter

- ◆ Convergence des solutions réseaux et des solutions d'infrastructure
- ◆ Partage de ressources virtualisées
- ◆ Automatisation des opérations
- ◆ Optimisation de la consommation énergétique
- ◆ Protection des données : protection en temps réel - déduplication des données
- ◆ Archivage, Optimisation des ressources de stockage et réduction de l'encombrement des données.
- ◆ Couche d'accès dans les DC: Architectures et solutions
- ◆ Couches de distribution et de Coeur dans les DC : Architectures et solutions
- ◆ Gestion du stockage - Architecture des réseaux de stockage
- ◆ Haute disponibilité / Reprise après incident Garantie de fonctionnement optimal pour les applications stratégiques et réduction des coûts de protection.
- ◆ Architectures innovantes : VPC end-to-End, accès serveur en 10GbE , Unified I/O ...
- ◆ Solutions d'interconnexion de Data Centers

Virtualisation 'Du poste de travail au datacenter'

La virtualisation est la clé d'un système d'information performant. Elle apporte des avantages stratégiques de flexibilité et de capacité à monter en charge qu'il s'agisse d'optimiser des postes de travail ou des salles informatiques convergentes de nouvelle génération. Elle permet de réduire les coûts d'exploitation et d'accélérer le déploiement de nouvelles applications.

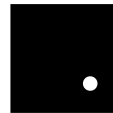
- ◆ Etat de l'art du marché
- ◆ Les salles informatiques convergentes
- ◆ Lien entre le Cloud et la virtualisation
- ◆ Cohabitation et Intéropérabilité entre Windows et linux dans le datacenter
- ◆ Virtualisation des salles de serveurs
- ◆ Déploiement de serveurs virtualisés
- ◆ Améliorer les performances des environnements physiques et virtualisés et faciliter l'administration.
- ◆ Virtualiser l'infrastructure IT de bout en bout : outils, processus et procédures de contrôle et de sécurité



- ◆ Virtualisation : retour sur investissement ?
- ◆ Virtualisation des postes de travail
- ◆ Techniques de virtualisation : micro partitionnement, virtualisation de la mémoire
- ◆ Virtualisation et Gestion des performances : les bonnes pratiques

Public concerné

Tout Responsable des infrastructures en entreprise, en SSII, Commercial ou autre ayant besoin d'appréhender les concepts, les méthodes, les techniques, et les procédures de l'évolution .



F1.2. Dématérialisation

Durée standard : 2 jours

La dématérialisation consiste à mettre en œuvre des moyens électroniques pour effectuer des opérations de traitement, d'échange et de stockage d'informations sans support papier.

L'e-administration couvre les technologies et les usages liés à la possibilité d'informer, d'orienter, mais aussi de réaliser des démarches administratives (tant au niveau central que local) au moyen de services en ligne (Internet, centres d'appel).

Concepts de la dématérialisation et historique

- ◆ Dématérialisation des contenus / Dématérialisation des procédures
- ◆ SLA
- ◆ Confiance
- ◆ Protection du patrimoine
- ◆ Gestion Electronique des Documents

Applications de la dématérialisation

- ◆ E-Business : sites Web, portails d'e-business, sécurité, pratiques commerciales...
- ◆ E-formation
- ◆ E-Administration

Administration électronique

- ◆ Dématérialisation des factures
- ◆ Fourniture et collecte d'informations
- ◆ Lettre recommandée
- ◆ Vote électronique
- ◆ Dématérialisation des achats
- ◆ Archivage électronique

Dématérialisation : technologies utilisées et bonnes pratiques

- ◆ Technologies de traitement
- ◆ Gestion performante d'un SI en exploitation
- ◆ Notion de Workflow
- ◆ Stockage des informations dématérialisées
- ◆ Cartes à puces (CNIE, CVQ...), Biométrie ...
- ◆ Codes à barres, RFID, GPS, Codage des contenus (MPEG..),
- ◆ Comment choisir son opérateur de confiance et sa plate-forme de dématérialisation ?

Dématérialisation : standards et normes

- ◆ EDI
- ◆ UML
- ◆ XML

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial, Juriste ou autre souhaitant appréhender les concepts, les méthodes, les techniques, et les procédures de la dématérialisation et de l'administration électronique.

F1.3. Archivage sécurisé

Durée standard : 2 jour

L'archivage sécurisé est l'une des applications les plus critiques de la dématérialisation. Mais la réflexion qu'une telle activité impose, doit se faire en parallèle avec les réalités et les risques de l'archivage matériel. Avant la mise en place effective d'un archivage électronique sécurisé, il faut évaluer l'existant en matière d'archivage en tenant compte du contexte à la fois technique et juridique. A partir des enjeux de l'archivage et des possibilités de sa forme électronique, peuvent naître les nouveaux projets.

Introduction à l'archivage électronique sécurisé

- ◆ Nature des documents archivables : documents comptables, juridiques, fiscaux, commerciaux...
- ◆ Support papier vs support dématérialisé.
- ◆ Solutions techniques d'archivage électronique.
- ◆ Ecosystème de l'archivage sécurisé

Contraintes de l'archivage électronique

- ◆ Procédures et formalités légales
- ◆ Conditions requises pour qu'un document devienne un original numérique.
- ◆ Supports d'archivage : notion de média non réinscriptible.
- ◆ Formats d'archivage : spécifications techniques requises.
- ◆ Données « sensibles » et contrôle de la CNIL.

Conservation et restitution des documents dématérialisés

- ◆ Normes techniques de référence en archivage sécurisé : ISO, AFNOR...
- ◆ Nécessité ou non de conserver des originaux papier
- ◆ Conditions d'accès aux données archivées électroniquement
- ◆ Durée et lieu d'archivage
 - Durée propre aux documents en question / Durée particulière au mode d'archivage électronique
 - Destruction des données archivées à l'issue de la période de conservation : obligation ou faculté ? preuve de la destruction.
 - L'archivage peut-il franchir les frontières ?

Externalisation de l'archivage ?

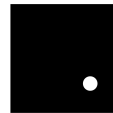
- ◆ Archivage interne : audit à mettre en place.
- ◆ Archivage externe : précautions à prendre.
- ◆ Externaliser la fonction archivage : cahier des charges et suivi

Archivage électronique et Contrôle Fiscal des Comptabilités Informatisées

- ◆ Données élémentaires et traitements informatiques à archiver.
- ◆ Contraintes particulières en matière de restitution des données et documents archivés.

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial, Juriste ou autre ayant besoin d'appréhender les concepts, les méthodes, les techniques, et les procédures de l'archivage sécurisé.



F1.4. PKI, cryptage, Signature électronique

Durée standard : 2 jours

L'achat en ligne se démocratise, le e-commerce continue de progresser à un rythme soutenu. Simultanément, la croissance des échanges électroniques via Internet soulève des problèmes accrus de protection des données et des documents. Le périmètre de ces échanges dématérialisés s'étend chaque jour (facture, bulletin de paie, commandes, devis, pièces de marché public, propositions commerciales,...). Du coup, les menaces se multiplient : usurpation d'identité, échanges non tracés, non signés ; d'où l'importance de systèmes d'authentification adaptés et sécurisés.

Généralités

- ◆ Cadre Général de la Certification Electronique
- ◆ Configurations d'un site http.

Les Infrastructures à Clé Publique (PKI)

- ◆ Du Modèle PKI au Certificat X509
- ◆ Standards & Politique de certification
- ◆ PKI d'entreprise et ouverture de session par carte à puce

La Signature Electronique

- ◆ La création de la signature électronique
- ◆ Vérification de la signature électronique
- ◆ Mise en place de la signature électronique dans un environnement, Net & J2ee

Cryptage et VPN

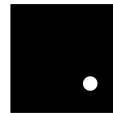
- ◆ Présentation de la Cryptographie et les Besoins des VPN
- ◆ Protocoles, Architectures et Sécurité des VPN & la Présentation : VPN et PKI
- ◆ Implémentation d'un VPN
- ◆ Simulation de tentative d'intrusion dans un VPN.

Exercices

- ◆ Mise en application des principes de la formation : création de documents, exploitation de documents

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial, Juriste ou autre ayant besoin d'appréhender les concepts, les méthodes, les techniques, et les procédures de l'authentification forte et de la signature électronique.



F1.5. Méthodes utilisées dans les Systèmes d'Information

Durée standard : 2 jours

Pour gouverner leurs systèmes d'information, les entreprises et les administrations adoptent et font coexister des référentiels de bonnes pratiques. Les trois méthodes qui se sont imposées sont : COBIT, CMMi, ITIL. Cette formation présente les champs d'application de ces référentiels, leurs différences et leurs complémentarités.

Introduction aux méthodes phares : CoBIT, ITIL, CMMI

- ◆ Définition du concept de gouvernance des systèmes d'information.
- ◆ Gouverner par les processus
- ◆ Les " best practices " et la mise au point des processus.
- ◆ La contribution d'ITIL à la gouvernance des systèmes d'information

Le CoBIT

- ◆ CoBIT : une méthode structurante de gouvernance du SI
- ◆ La gouvernance des systèmes d'information selon COBIT.
- ◆ La philosophie de CoBIT.
- ◆ Le champ d'action de CoBIT.
- ◆ Le synoptique des processus CoBIT
- ◆ Pilotage = spécification – contrôle - recadrage

ITIL

- ◆ ITIL : en aval de CoBIT
- ◆ ITIL v3 et la gestion du système d'information.
- ◆ La philosophie d'ITIL, son architecture, ses concepts.
- ◆ Le champ d'action d'ITIL.
- ◆ Le synoptique des processus ITIL
- ◆ Articulation avec COBIT.

CMMI

- ◆ L'incidence de CMMi à la gouvernance des systèmes d'information
- ◆ CMMi et la gestion des projets.
- ◆ La philosophie de CMMi son architecture, ses concepts.
- ◆ Le champ d'action de CMMi.
- ◆ Le synoptique des processus CMMI
- ◆ Articulation de CMMI avec COBIT et ITIL.

Comment arbitrer entre les méthodes ? La méthode des méthodes

Public concerné

Cette formation s'adresse à toute personne impliquée dans la définition ou la gestion des systèmes d'information : DSI, auditeurs, responsables des services informatiques, MOA, MOE.
Aucune connaissance technique particulière n'est nécessaire pour suivre cette formation.

F2. Systèmes de communication et réseaux d'entreprise

F2.1. Infrastructures de réseaux locaux et réseaux IP

Durée standard : 2 jours

Les infrastructures utilisées par les systèmes de communication sont la base des échanges de voix, de données et d'images numérisées dans l'entreprise mais aussi en dehors. Cette formation fait le point sur cette thématique majeure.

Infrastructures de câblage

- ◆ Applications du câblage multimédia (SVDI ou Sécurité – Voix – Données – Image)
- ◆ Principe de la communication physique
- ◆ Attributs du câblage (Critères, connectique, accessibilité, câbles, équipements)
- ◆ Les supports physiques
 - Paire torsadée : classes et catégories, média, débits, évolutions
 - Câble coaxial
 - Fibre optique (monomode, multimode, multiplexage optique WDM, DWDM)
- ◆ Notions de câblage structuré et de précâblage
- ◆ Réseaux radio (Infra-rouge, satellite, VHF, ...)
- ◆ Support du Courant Porteur en Ligne (CPL)
- ◆ Evaluation d'un système de câblage existant
- ◆ Organisation, ingénierie et validation d'un système de câblage voix-données-image

Infrastructures : réseaux locaux (LAN)

- ◆ Introduction - caractéristiques techniques
- ◆ Technologie (Topologie, Support, Techniques d'Accès)
- ◆ Principe de la communication physique
- ◆ Les supports physiques (paire torsadée, câble coaxial, fibre optique)
- ◆ Les principales méthodes d'accès (CSMA, ALOHA, ...)
- ◆ Réseaux radio (Wi-Fi et IEEE 802.11, satellite, VHF, ...) – sécurité
- ◆ Les Courants Porteurs en Ligne (CPL)
- ◆ La famille des réseaux Ethernet (10-100 BT, Gigabit, 10G, Commutation,...)
- ◆ Sûreté de fonctionnement d'un réseau local
- ◆ Sécurité d'un réseau local
- ◆ Gestion de la Qualité de Service (QoS)
- ◆ Interconnexion des réseaux locaux
- ◆ VLAN (Réseaux locaux virtuels)
- ◆ Commutation de niveau 3 et de niveau 7
- ◆ Les principaux équipements de réseaux et le marché
- ◆ Evolution des réseaux locaux et perspectives

Réseaux IP : Partie théorique

- ◆ Introduction au modèle TCP/IP
- ◆ Réseaux locaux (Câblage, Ethernet, WiFi)
- ◆ La couche Réseau (Adressage IP, routage, format des datagrammes, ...)
- ◆ La couche Transport (format du segment TCP, format du datagramme UDP, TCP vs UDP, RTP/RTCP)
- ◆ Qualité de service (QoS)



- ◆ Les services Utilisateur (DNS, HTTP, FTP/TFTP, SMTP, SNMP, ...)
- ◆ Boucle locale (xDSL WiMax, Hotspots)
- ◆ La sécurité sur les réseaux IP: Menaces et défenses

- ◆ Perspectives et évolutions (IPv6, ...)
- ◆ Normalisation et régulation
- ◆ Réseaux d'entreprise pour la ToIP : architectures et redondances

Exercices et Travaux pratiques

- ◆ Analyse de trames sur un réseau local
 - Trames Ethernet,
 - Flux IP : IP, TCP, UDP, DHCP, ...
- ◆ Sécurisation d'un réseau

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les services, les méthodes, les techniques, et les contraintes du câblage des réseaux voix – données – image, les services et les technologies des réseaux locaux et des réseaux IP d'entreprise ou de collectivités .

F2.2. Téléphonie sur IP – communications unifiées : l'essentiel

Durée standard : 1 jour

Les réseaux IP, Internet en tête, et leurs infrastructures, WAN, LAN et systèmes de câblage, se sont imposées définitivement. La téléphonie sur IP est devenue une application informatique commune autre ... ou presque. Le grand chantier qui s'annonce aujourd'hui est celui des communications unifiées. Il fédère la téléphonie sur IP et les autres applications de communication. Cette formation fait le point sur l'essentiel de ces deux thèmes importants.

- ◆ Introduction et vue d'ensemble : enjeux, comparaison ToIP - téléphonie traditionnelle, principes de fonctionnement, convergence, bénéfices attendus
- ◆ Principe de la commutation et du réseau téléphonique
- ◆ Périmètre applicatif – ToIP et communications unifiées :
 - Accueil téléphonique (postes opérateurs, ACD, SVI, ...),
 - Mobilité
 - Communications Unifiées : annuaire, messagerie unifiée, présence, visiophonie, visioconférence
 - La taxation
 - Interfaces utilisateurs
- ◆ Plan de numérotation
- ◆ La téléphonie sur IP : architecture et produits
- ◆ Architectures : PBX hybride TDM et IP, PBX pur IP, IP CENTREX
- ◆ Installations, câblage, répartition
- ◆ Le RNIS : interfaces pour l'entreprise – évolution vers le SIP-T
- ◆ Contraintes majeures : reprise de l'existant, qualité de service, sécurité
- ◆ Rôles et acteurs économiques (équipementiers, intégrateurs, opérateurs), caractérisation des principales solutions du marché
- ◆ Exemples de projets et retour d'expérience concrets, étude de cas
- ◆ Migration : pré requis, questions clés, approches
- ◆ Projet : audit, scénarios, cahier des charges, choix de solution, pilote, déploiement, accompagnement du changement
- ◆ Etudes de cas économiques
- ◆ VoIP / ToIP : Evolutions en cours et à prévoir

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les services et les technologies de la téléphonie sur IP et des infrastructures qu'elle emprunte.

F2.3. Téléphonie sur IP - communications unifiées : approfondissement

Durée standard : 2 jours

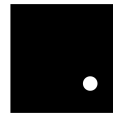
Possédant déjà l'essentiel de la téléphonie sur IP des communications unifiées, le stagiaire trouvera ici l'approfondissement nécessaire à une compréhension détaillée de ce domaine en plein essor. Cette formation lui permettra de posséder des bases très solides sur ce thème au confluent entre la téléphonie et l'informatique communicante.

Partie 1 : Approfondissement fonctionnel : ToIP et Communications Unifiées

- ◆ Accueil téléphonique (Postes opérateurs, ACD, SVI, ...)
 - Application à l'entreprise
 - Application aux centres de contact
- ◆ ToIP - Interfaces utilisateur :
 - Postes fixes : postes IP, postes analogiques, postes numériques : ressemblances et différences
 - Softphones
 - Postes sans fil
- ◆ Mobilité :
 - Mobilité intra site et intra entreprise
 - Approche DECT
 - Approche Wi-Fi
 - Convergence ToIP – GSM : offres techniques et financières, typologie des terminaux
- ◆ Communications Unifiées : annuaire, messagerie unifiée, présence, visiophonie, visioconférence, administration
- ◆ Communications Unifiées : approche des leaders du marché et conséquences sur les interfaces utilisateurs
 - Approche Cisco
 - Approche Microsoft OCS
 - Approche Cycos
 - Approche Phonality (DELL, Aastra Matra, ...)
 - ...

Exercices et Travaux pratiques

- ◆ Fonctionnement concret de la ToIP
 - Réalisation d'appels internes et externes
 - Réalisation d'appels SIP à SIP
- ◆ Communications Unifiées
 - Messagerie Instantanée
 - "Click to Call"
 - Messagerie Unifiée



Partie 2 : Approfondissement technique : ToIP et communications unifiées

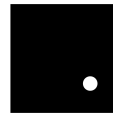
- ◆ Architecture : typologie et détails :
 - Le cœur du système : serveur de signalisation, iPBX,
 - Le lien avec l'existant : les passerelles
 - Système hébergé et partagé : IP Centrex,
- ◆ Mobilité :
 - Architecture et caractéristiques techniques DECT
 - Architecture et caractéristiques techniques Wi-Fi
- ◆ Normalisation et protocoles VoIP :
 - H.323,
 - SIP,
 - MGCP,
 - ENUM,
 - ...
- ◆ Qualité de Service : mesurer, évaluer, maîtriser
- ◆ Sécurité, sûreté de fonctionnement
- ◆ Administration :
 - Gestion des utilisateurs et configuration
 - Supervision
 - Traitement des incidents

Exercices et Travaux pratiques

- ◆ Analyse de trafic sur un réseau de Voix sur IP
 - Analyse de trames - Protocoles SIP, RTP
 - Observation de la qualité de service selon les architectures
- ◆ Administration
 - IPBX matériel : mono site, multi site –
 - IPBX logiciel
 - Enregistrement de terminaux (softphone, hardphone)
 - Création de lignes de postes sur iPBX
 - Configuration manuelle et automatique des postes

Public concerné

Tout Ingénieur ou Technicien ayant besoin d'approfondir, aussi bien en théorie qu'en pratique, les technologies de téléphonie sur IP et ses infrastructures.



F2.4. Systèmes de Communication d'entreprise

Durée standard : 1 jour

Cette formation fournit les bases du câblage, de la téléphonie, des réseaux et des accès à Internet.

Notion de réseau local

- ◆ Introduction - caractéristiques techniques
- ◆ Technologie : Topologie, Support, Techniques d'Accès
- ◆ Câblage voix-données-image / Courants faibles / CPL
- ◆ Les réseaux Ethernet
- ◆ Les réseaux IP

La téléphonie

- ◆ Téléphonie classique : PABX
- ◆ Téléphonie sur IP
- ◆ Les systèmes internes de téléphonie sur IP
- ◆ Externalisation : IP Centrex ou IPBX dédié ?

Techologies de Mobilité en entreprise

- ◆ Wi-Fi
- ◆ Bluetooth
- ◆ DECT
- ◆ NFC

Accès à Internet et utilisation d'Internet

- ◆ Les architectures Internet
- ◆ Modes d'accès en haut-débit : xDSL, fibre optique, Wi-Fi, Wi-Max, satellite ...
- ◆ Les fournisseurs d'accès (FAI)
- ◆ Messagerie
- ◆ Sécurité
- ◆ Internet : outil de marketing, exploiter le web 2.0, réseaux sociaux

Réseau étendu

- ◆ WAN,
- ◆ Accès nomade et au réseau d'entreprise, travail à domicile
- ◆ IP VPN MPLS / IPsec

Projets de systèmes de communication d'entreprise

- ◆ Les principaux types d'équipements et de logiciels
- ◆ Intégrer, mettre en service et maintenir PCs et serveurs
- ◆ Définition et conduite d'un projet de mise en œuvre

Public concerné

Tout Gestionnaire d'entreprise ou de collectivité ayant besoin de maîtriser pour ses utilisateurs les technologies de communication de base.

F2.5. Administration de réseaux

Durée standard : 2 jours

Cette formation permet de traiter tous les volets de l'administration des réseaux, la configuration des systèmes, la supervision des réseaux, le diagnostic des pannes et des incidents, la gestion des utilisateurs.

L'administration des réseaux

- ◆ Principe et Fonctionnalités
- ◆ Architectures et notions pratiques (Manager, Agent, MIB ...)
- ◆ L'évolution des protocoles d'administration SNMP
- ◆ Plates-formes constructeurs
- ◆ Configuration du câblage
- ◆ Les métiers liés à l'administration de réseaux
- ◆ Evolution des normes

La maintenance des réseaux

- ◆ Contraintes liées à l'environnement
- ◆ La configuration d'un réseau
- ◆ La supervision d'un réseau
- ◆ Diagnostic de pannes d'un réseau : isoler les défaillances
- ◆ La sécurité dans un réseau
- ◆ Analyse de trafic (avec un analyseur de trafic et de protocole)

La sécurité des réseaux et les VPN

- ◆ Introduction à la sécurité des réseaux
- ◆ Classification des risques
- ◆ Principaux mécanismes de sécurité
- ◆ les VPN
- ◆ Conclusion

Public concerné

Tout praticien de l'administration de réseaux et systèmes ayant besoin d'appréhender les concepts, les méthodes, outils et technologies de l'administration de réseaux.

F3. Sécurité des Systèmes d'information et des réseaux

F3.1. Sensibilisation à la sécurité de l'information

Durée standard : 0,5 jour

Présentation en une demi journée pour les différents collaborateurs de l'entreprise aux risques et dangers liés à la sécurité de l'information. Sensibilisation aux bonnes pratiques de sécurité.

- ◆ Sécurité de la messagerie
- ◆ Sauvegarde des postes de travail
- ◆ Manipulation des objets de stockage mobile (clés USB, disques durs amovibles)
- ◆ Utilisation et sécurité des mots de passe de session
- ◆ Comportement « responsable » vis-à-vis des informations de l'entreprise
 - Communication sur les réseaux publics
 - Ingénierie sociale
 - Echanges d'informations en lieu public (TGV, aéroport,...)
- ◆ Protection du matériel de l'entreprise
 - PC portables
 - PDA, BlackBerry, I Phone,...

Public concerné

Tout manager d'entité métier ou de systèmes d'information ayant besoin de maîtriser les principes de la sécurité de l'information dans les activités informatiques de tous les jours.

F3.2. Architectures de défense globale de sécurité

Durée standard : 1 jour

Le « concept de défense globale » positionne aux endroits adéquats les renforts de sécurité indispensables pour parer et anticiper les attaques. L'objectif de cette formation est de savoir évaluer les menaces et les défenses disponibles et définir de nouveaux types de défenses appropriées. Elle vous permettra aussi d'apprendre comment protéger l'intérieur du réseau et déjouer les attaques applicatives.

Hacking et hackers

- Typologie des hackers et des attaques (sniffing, phishing,...)
- Evaluation des défenses actuelles(Firewall, IDS,...)
- Mise en oeuvre et positionnement, gestion des alertes, plans de secours

Sécurité interne

- Attaques internes, Chevaux de Troie, Key loggers, ...
- Notions de quarantaine, mise en oeuvre et VLAN

Sécurité hors de l'entreprise

- Télé-travail et nomadismes, accès aux outils de l'entreprise (VPN SSL, Webmail, remote office)
- Authentification forte (Token, OTP, biométrie)

Sécurité des clients applicatifs

- Anti-virus (base de signatures, analyse comportementale et heuristique), anti-spam et anti-spyware

Sécurité des applications

- Attaques lentes
- Analyse et protection des codes sources
- Réseaux radio et Wifi

Attaques futures

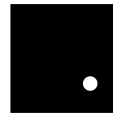
- Téléphone PDA, VoIP, chat et « peer to peer »
- Rootkits et « zero day »

Notion de défense en profondeur

- Point de renforcement, Honeypots
- Veille technologique et cellule de crise

Public concerné

Tout responsable de systèmes d'information ou d'infrastructures IT souhaitant anticiper la typologie des attaques les plus répandues et se préparer à les prévenir ou à les guérir.



F3.3. Mise en place d'un Plan Directeur de Sécurité (PSI, SMSI, Audit)

Durée standard : 3 jours

Mise en application des premiers chapitres de la norme ISO 27001 sur l'organisation de la sécurité au sein d'un organisme. Cette formation s'appuie également sur les document de la ANSSI (PSI) et sur les consignes du COBIT et ITIL (ISO 20000).

Introduction

- Qu'est-ce qu'un Plan Directeur de Sécurité ?

La PSI

- Principes détaillés d'une PSI
- Méthode de conception : analyse des risques, norme ISO 27001, PSSI de l'ANSSI
- Communication de la PSI auprès de la DG

Les normes et standards

- Normes et Standards de sécurité : 15408, 13335, 10181 et autres
- L'ISO 27001 et la certification sécurité

Le SMSI

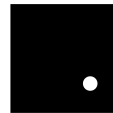
- Les chapitres 4 à 8 de l'ISO 27001
- L'amélioration continue : la roue de Deming

Le contrôle et le suivi

- L'audit technique, organisationnel
- Les campagnes d'audits, plan d'audit, consolidation des résultats
- Les tableaux de bord de sécurité

Public concerné

Tout responsable de systèmes d'information devant se préparer à mettre en place une organisation « sécurité » efficace et durable.



F3.4. Authentification et PKI en environnement ouvert

Durée standard : 2 jours

Mise en place d'une plate forme d'authentification sécurisée avec PKI, Certificat et Single-Sign On pour l'ensemble des applications Web (Intranet et Extranet) de l'entreprise en environnement ouvert et hétérogène (Linux, Windows ...).

La formation intègre la présentation et l'explication de mise en place d'annuaires LDAP sécurisés.

Introduction

- Présentation du module
- Rappel des principes d'authentification (web, ms-chap, etc.)

L'authentification forte

- Les 3 conditions
- Les outils techniques (token, biométrie, etc.)

Les techniques de chiffrement

- La confidentialité et l'intégrité
- Historiques des méthodes de chiffrement et de codage
- la cryptographie symétrique : théorie, algorithmie, principaux mécanismes de chiffrement (DES, AES, etc.)
- la cryptographie asymétrique : théorie, algorithmie, RSA, perspectives d'avenir

Les échanges de clé

- Notion de clé publique
- Principaux mécanismes de diffusion et management des clés (symétrique et asymétrique)
- Fabrication de la confiance
- Signature électronique

Les certificats

- Création et enregistrement, diffusion, durée de vie, révocation

Organisation de la PKI

- Notion de datage, gestion du temps
- Sécurité des clés et certificats racines
- Les principaux tiers de confiance

Application pratique avec des produits OpenSource

- Utilisation et montage d'un ensemble de clés et certificats avec OpenSSL



- Gestion avec Vulture/Rooster, Fedora PKI Dogtag Certificat System

Public concerné

Tout manager d'entité métier ou de systèmes d'information dont l'informatique évolue vers un environnement mixte Windows / Linux (entre autres) et souhaitant une sécurisation globale au moyen d'une infrastructure à clé publique.

F3.5. Migration de Windows à Linux

Durée standard : 2 jours

Cette formation a pour objectif d'aider les dirigeants de PME/PMI et les intégrateurs de solutions informatiques, à migrer des systèmes propriétaires (Windows) au tout gratuit (Linux). Présentations pratiques d'outils et d'applications Open Source.

Introduction

- Historique
- les licences GNU / BSD/ GPL, les sites WEB de référence

Linux

- Le système, la console, les distributions
- La conduite à tenir pour migrer
- la migration bureautique : expertise, formation des utilisateurs

L'entreprise par domaine

- La bureautique : Côté serveur (FTP, NFS, SAMBA, CUPS), Côté utilisateur (Gnome, KDE, OpenOffice, Firefox, ...)
- Les chaînes graphiques : Gimp (DAO), Blender (DA03D), Scribus (PAO), Xfig, QCAD, HeeksCAD (CAO,CNC), KiCAD
- Les chaînes audio/video : Ardour, KINO, Cinelerra, VLC
- Le travail collaboratif : messagerie (sendmail, postfix, ...), Thunderbird, Sunbird, etc., les Groupwares (eGroupWare, ...)
- Le SGBD : PostgreSQL, MySQL
- Comptabilité, gestion, finance : les limitations légales, SQL-Ledger, Oratio, Les ERP (OpenERP, Dolibarr, OpenSI)
- La Gestion de Relation Client : SugarCRM, Vtiger
- Le CMS : EzPublish, Zope/Plone et Zwook, Joomla, Spip, etc.

La sécurité du système et de l'administration

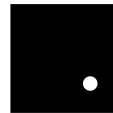
- La surveillance et l'administration : Nagios, JFFNMS, SNORT, SQUID, Webmin
- La sauvegarde : BackupPC, Bacula, etc.

Si ça n'existe pas sous Linux

- L'émulation de windows : Wine
- La virtualisation : Vmware, Qemu, Bochs, Zen

Public concerné

Tout manager de systèmes d'information dont l'informatique évolue vers un environnement mixte Windows / Linux (entre autres) et souhaitant faire cohabiter et administrer les deux environnements.



F3.6. Sécurité des Systèmes d'information : la norme ISO 27001

Durée standard : 1 jour

Cette formation présente la norme de sécurité des SI : ISO 27001 et le fonctionnement des Systèmes de Management de la Sécurité de l'Information. Elle fournit une première approche certification.

D'où vient la norme ISO 27001 ?

- Les normes antécédentes
- La BS 7799
- L'ISO 17799

Que contient le standard ?

- Les 14 chapitres
- Le SMSI
- Les 133 points de contrôle

Comment la mettre en œuvre ?

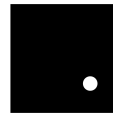
- L'organisation de la sécurité
- Le projet SMSI
- Le principe d'amélioration continue

Les livrables de l'ISO

- La déclaration d'applicabilité
- La certification, son renouvellement

Public concerné

Tout manager de systèmes d'information ou de la sécurité de l'information souhaitant appréhender une approche normalisée de la sécurité de l'information et des systèmes d'information, à travers la norme de référence en la matière : ISO 27001 (et ses dérivées), et son pendant : la certification.



F3.7. Gestion des identités et authentification

Durée standard : 1 jour

Cette formation présente les concepts suivants : Contrôle d'accès, Identity management (gestion des identités, fédération, authentification, signature électronique, chiffrement, biométrie, Protocole Liberty Alliance, ...). Elle permet d'appréhender les différentes techniques d'authentification et d'offrir une introduction à l'IAM.

La gestion de l'identité (ou Identity Management)

- Gestion des identités, fédération
- Protocoles divers : Liberty Alliance, etc.

Notion de chiffrement

- Chiffrement symétrique
- Chiffrement asymétrique

Les mécanismes d'authentification

- Login, mot de passe
- Les certificats
- Signature électronique

Authentification Web

- Méthode Post
- Méthode Basic
- Méthode par formulaire

Authentification forte

- Principe de Token
- Calculatrice, iphone

Public concerné

Tout manager d'entité métier ou de systèmes d'information dans un environnement où les utilisateurs doivent accéder à des ressources ou effectuer des transactions électroniques pouvant induire un besoin d'authentification forte.

F3.8. PRA/PCA

Durée standard : 1 jour

Cette formation présente les risques pouvant avoir un impact sur la productivité de l'entreprise, ainsi que les méthodes et les technologies permettant d'anticiper un sinistre et de reprendre l'activité de manière acceptable s'il s'en produit un.

Qu'est-ce que la continuité d'activité ?

- Les enjeux de la continuité d'activité
- Les concepts clés
- Qu'est-ce qui peut atteindre à la continuité d'activité ?
- Définir le périmètre de la continuité d'activité
- Contrôler la continuité d'activité
- Plan de continuité d'activité (PCA) vs Plan de reprise d'activité (PRA)
- Notions de temps de reprise (RTO), de point de reprise (RPO)
- Criticité des activités et des processus : les classes de service :
- Appliquer un plan de reprise lors d'un sinistre
- Les exigences réglementaires : normes ISO, Bâle II, SARBANES OXLEY, contrats d'assurances...
- Les technologies de base indispensables

Continuité de l'activité lors d'un sinistre

- Analyse d'impact du sinistre sur l'activité
- Estimation des besoins et des ressources
- Bâtir un plan de continuité de service (objectifs de reprise, portée du plan, procédures, priorités...)
- Les tests et mises à jour du plan
- Les sites de reprise ; qualité, nombre et localisation
- Site de reprise interne vs externe
- Bien dimensionner les ressources du site de reprise
- Les architectures de continuité de service
- Dispositifs de reprise après sinistre
- Choix des technologies utilisées lors de la reprise (sauvegarde / restauration, mirroring)
- Solutions d'archivage (bases de données, messagerie, données patrimoniales...)
- Fonctionnalités des serveurs : clustering, load balancing, NAS, etc. ?
- Redondances des réseaux LAN, WAN,
- Utiliser la virtualisation

Formalisation communication et entraînement

- Le plan de gestion de crise
- La cellule de crise
- Le plan de secours informatique et la reprise d'activité informatique
- Le plan de continuité des opérations



- Sensibiliser et former les utilisateurs
- Tests et simulation de sinistre
- Procédures et les moyens de suivi
- Pratiques pour garantir la cohérence des données
- Un exemple de plan de reprise après sinistre

Méthodes et outils de la continuité d'activité

- Expression des besoins
- Analyse d'impact sur les activités
- Identifier et évaluer différents scénarii
- Contrôler la qualité de service : outils de mesure et tableaux de bord
- Les méthodes ITIL et CoBit pour la continuité d'activité
- Combien coûte la continuité d'activité ?

Public concerné

Tout responsable de systèmes d'information qui doit garantir la continuité de l'activité de l'entreprise à travers une informatique robuste et réactive.

F4. Télécommunications

F4.1. Introduction aux réseaux et télécommunications

Durée standard : 3 jours

Cette formation académique fournit les bases fondamentales des réseaux et des télécommunications. Elle est de plus illustrée par des références constantes aux technologies et aux réseaux qui ont fait les télécommunications.

Concepts de base en réseaux et télécommunications

- ◆ Notion de service
- ◆ Notion de modèle
- ◆ Le modèle de référence OSI
- ◆ Les modèles réels : IP et modèles dérivés
- ◆ Notion de protocole
- ◆ Les architectures de réseaux et de télécommunications
- ◆ L'industrie et les familles d'équipements
- ◆ La normalisation des réseaux et télécommunications

Les réseaux d'Opérateurs : voix et données

- ◆ Principes d'architecture : ossature / accès, transmission / commutation
- ◆ Opérateurs d'infrastructure vs Opérateurs de service
- ◆ Réseaux commutés : RNIS, accès primaire, accès de base, commutation de paquets
- ◆ Téléphonie d'Opérateurs : réseaux et signalisation, réseaux intelligents
- ◆ La boucle locale : xDSL, Wi-Fi, Wi-Max, CPL, fibre optique ...
- ◆ Le transport des informations par Internet
- ◆ Les réseaux IP d'Opérateurs
 - Les Réseaux Privés Virtuels (VPN)
 - Les réseaux MPLS : QoS et classes de service
 - Les réseaux Ipsec : authentification et cryptage
- ◆ Les Opérateurs de mobiles (GSM, UMTS) et les MVNO
- ◆ Tarification
- ◆ Système d'information des réseaux d'Opérateurs
- ◆ Evolution des réseaux d'Opérateurs

Les réseaux d'accès

Les réseaux de transmission

- ◆ Les supports
- ◆ Les techniques
- ◆ Les liaisons E1 / T1
- ◆ Les réseaux de transmission (SDH, PDH, DWDM)
- ◆ La boucle locale : xDSL, fibre optique, Wi-Fi, Wi-Max, CPL, ...



Les technologies historiques

- ◆ X.25
- ◆ Frame Relay
- ◆ ATM (Asynchronous Transfer Mode)

Les nouvelles architectures

- ◆ IP sur SDH
- ◆ 10G-Ethernet sur MAN

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les notions fondamentales des réseaux et télécommunications.

F4.2. Télévision sur DSL et triple play

Durée standard : 1 jour

Cette thématique est au croisement d'une double révolution technologique : celle du haut-débit et celle du multimédia sur IP. Cette double rupture permet un éventail de nouveaux services, s'appuie sur une nouvelle architecture, modifie les modèles économiques et les profils de métiers. Tout cela est traité lors de cette formation.

Une double révolution technologique : haut-débit et multimédia sur IP

- ◆ Accès : le haut-débit
- ◆ Voix / données / Image sur IP
- ◆ Broadcast vs broadband

Une grande variété de services

- ◆ Accès à Internet (single play)
- ◆ Téléphonie sur IP (double play)
- ◆ Les services de transmission d'image (triple play) : visiophonie (point à point, visioconférence), Video on demand, E-television

Architectures des réseaux NGN

- ◆ Architectures des réseaux d'Opérateurs
- ◆ Architectures des réseaux de téléphonie sur IP
- ◆ Technologies de transmission d'image : Codec, MPEG 2 vs MPEG 4, Multicast IP, ...
- ◆ Accès : le haut-débit
- ◆ La boucle locale : xDSL, câble, fibre optique, ..
- ◆ Et chez l'abonné ?
 - La passerelle d'accès multimédia
 - Comment simplifier le câblage ?
 - Les terminaux
 - Problèmes de latence et solutions

Modèles économiques

- ◆ L'impulsion des marchés résidentiels
- ◆ Modèles économiques pour les Opérateurs
- ◆ Modèles économiques pour l'entreprise

Evolution des métiers

- ◆ Les métiers des réseaux IP
- ◆ Les métiers de service dans l'image
- ◆ Les nouveaux métiers de la téléphonie

Public concerné

Tout professionnel se trouvant à la confluence de l'audiovisuel et des télécommunications et souhaitant anticiper sur l'usage croissant des télécommunications dans l'audiovisuel.

F5. Radio-communications

F5.1. Introduction aux réseaux radio

Durée standard : 1 jour

Les réseaux radio commencent à foisonner. Il est nécessaire, dans de nombreux métiers à caractère technologique, de les appréhender à partir de leurs fondements. C'est ce que propose cette formation.

- ◆ Les techniques de base (fréquences, utilisation d'un canal radio, architecture d'un réseau mobile cellulaire)
- ◆ Caractéristiques du réseau GSM 900
- ◆ Caractéristiques propres au GSM / DCS 1800
- ◆ Réseaux Tétra et Tétrapol
- ◆ Le GPRS
- ◆ L'UMTS et les réseaux de mobiles de 3^{ème} génération
- ◆ Les réseaux de 4^{ème} génération et la transition
- ◆ Du SMS au MMS
- ◆ Wi-Fi et les réseaux IEEE 802.11
- ◆ De la BLR au Wi-Max

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les services et les technologies des réseaux radio.

F5.2. L'essentiel des réseaux Wi-Fi

Durée standard : 1 jour

Les réseaux WiFi se sont développés de manière accélérée. La normalisation du 802.11n (mimo) permet de multiplier la bande passante disponible sur ces réseaux, ouvrant ainsi de nouvelles perspectives dans le sans-fil. Cette formation de référence permet de connaître l'essentiel sur ces réseaux, de manière académique et pratique.

Architecture physique et logique

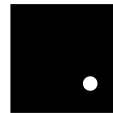
- ◆ L'origine du WiFi
- ◆ Les constituants de base
- ◆ Les aspects radio
 - Les principes de la radiopropagation
 - Les communications numériques sans fil
 - (Techniques de modulation, accès multiples, technique MIMO)
 - Les autres technologies sans fil (DECT, GSM, DCS, UMTS, WIMAX, Bluetooth, Zigbee, DVBH, T T, ...)
 - La couche physique du 802.11 (WiFi, a/b/g/n)
- ◆ Architecture logique et sécurité
 - Les topologies (architecture)
 - La technique d'accès a support (couche MAC, CSMA/CA, roaming)
 - La sécurité (chiffrement WEP, WPA, authentification 802.1x, solutions centralisées)
- ◆ Etat de la normalisation

Travaux pratiques

- ◆ Configuration d'un point d'accès Wi-Fi de milieu de gamme (Linksys)
- ◆ Configuration d'un point d'accès Wi-Fi professionnel (Cisco)

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les usages, les aspects techniques et les contraintes des réseaux Wi-Fi.



F5.3. Les réseaux WiFi – session approfondie

Durée standard : 2 jours

A partir d'une connaissance sur l'essentiel du WiFi, le stagiaire pourra, à l'issue de cette formation, concevoir, déployer utiliser et administrer les principaux réseaux WiFi du marché.

Architecture physique et logique

- ◆ L'origine du WiFi
- ◆ Les constituants de base
- ◆ Les aspects radio
 - Les principes de la radiopropagation
 - Les communications numériques sans fil
 - (Techniques de modulation, accès multiples, technique MIMO)
 - Autres technologies sans fil (DECT, GSM, DCS, UMTS, WIMAX, Bluetooth, Zigbee, DVBH, T T, ...)
 - La couche physique du 802.11 (WiFi, a/b/g/n)
- ◆ Architecture logique et sécurité
 - Les topologies (architecture)
 - La technique d'accès a support (couche MAC, CSMA/CA, roaming)
 - La sécurité (chiffrement WEP, WPA, authentification 802.1x, solutions centralisées)
- ◆ Etat de la normalisation

Applications

- ◆ Les différents marchés
- ◆ Les exigences des applications "données"
- ◆ Les exigences des applications "voix" (VoWiFi)
- ◆ Les applications hybrides GSM-WiFi
- ◆ Le WiFi en milieu industriel et ferroviaire

Déploiement du WiFi

- ◆ Informations à recueillir en vue d'un déploiement
- ◆ Dimensionnement d'un réseau (étude de cas)
- ◆ Choix des équipements
- ◆ Les outils du déploiement : mesure, simulation
- ◆ Résolutions des principaux problèmes (antennes, pollution électromagnétique, ...)

Travaux pratiques

- ◆ Configuration d'un point d'accès Wi-Fi de milieu de gamme (Linksys)
- ◆ Configuration d'un point d'accès Wi-Fi professionnel (Cisco)
- ◆ Réalisation d'un audit de site à l'aide d'un logiciel de cartographie (AirMagnet)
- ◆ Réalisation d'une analyse spectrale (AirMagnet)

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les usages, les aspects techniques et les contraintes des réseaux Wi-Fi de manière approfondis.

F5.4. Applications mobiles : cartes SIM / USIM

Durée standard : 1 jour



En partenariat avec les Experts Européens en Systèmes de Transactions Electroniques

- ◆ Introduction à la carte à puce (SIM/USIM)
- ◆ Normes et standards
- ◆ Environnement cartes et réseaux
- ◆ Operating System cartes (Javacard, Multos, propriétaire)
- ◆ Introduction à la sécurité (WIM, DRIM ...)
- ◆ Architectures de systèmes de transactions sécurisées mobiles (mobiles GSM, PDA...)
- ◆ Les tendances cartes (SIM/USIM) à moyen terme
- ◆ Les moyens et outils de tests (SIM, USIM...)
- ◆ Les grandes applications mobiles

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les services et la sécurité des usages transactionnels (paiement ...) des mobiles.

F6. TES : Transactions Electroniques et monétique

F6.1. Monétique : fonctions – architecture - EMV

Durée standard : 5 jours



En partenariat avec les Experts Européens en Systèmes de Transactions Electroniques

Monétique : fonctions et architecture

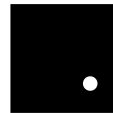
- ◆ Notions de base sur la monétique
- ◆ L'environnement de la monétique en France et en Europe
- ◆ Les produits et services de la monétique
- ◆ Les principes fonctionnels d'une transaction à partir d'un terminal de paiement fixe et d'un terminal mobile
- ◆ La fonction Emetteur
- ◆ La fonction Acquéreur
- ◆ Les fonctions Back Office
- ◆ La sécurité et les moyens d'authentification (Jetons, Calculettes, Pin code, Biométrie...)
- ◆ Les moyens de tests cartes, terminaux et front office

Applications EMV

- ◆ Le projet EMV : objectifs et spécifications
- ◆ Fonctionnement dans le système bancaire français : B0' et migration à EMV
- ◆ Les impacts de la migration EMV

Public concerné

Tout Ingénieur, Gestionnaire, Commercial ou autre ayant besoin d'appréhender les applications et systèmes de transactions électroniques et de monétique.



F6.2. EMV : spécifications et certification

Durée standard : 1 jour

Principe et enjeux d'EMV

- ◆ Précurseurs d'EMV en France
- ◆ Pourquoi EMV ?
- ◆ Principe d'EMV

Normalisation EMVco

- ◆ Les normes ISO 7816 (Base de EMV contact)
- ◆ Les normes ISO 14443 (Base de EMV contactless)

Les spécifications EMVco

- ◆ Niveau I : mécanique, électrique, protocole
- ◆ Niveau II : commandes – réponses, articulation des transactions – format des données

Certification des terminaux et des cartes

- ◆ Objectif et principes de la conformité
- ◆ Les normes ISO 9646 et leur application à la conformité EMV
- ◆ Signification de la conformité
- ◆ Essais et Tests : méthodes de tests / suites de tests
- ◆ Les laboratoires d'essais
- ◆ Bâtir un schéma d'homologation de type EMV

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial aux prises avec les contraintes et les caractéristiques détaillées de la norme EMV qui s'est imposée comme la norme de base dans le paiement par carte à puce.

F6.3. Les technologies sans contact et NFC

Durée standard : 1 jour

Principe et enjeux des cartes à puce sans contact

- ◆ Principe
- ◆ Réduire le temps de transaction
- ◆ Réduire l'usure mécanique

Normalisation

- ◆ ISO 14443
- ◆ Autres standards de référence
- ◆ Introduction à NFC

Applications

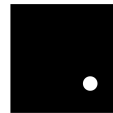
- ◆ Monétique – paiement de proximité
- ◆ Télébillettique
- ◆ Contrôle d'accès
- ◆ Carte de vie quotidienne (CVQ)
- ◆ Passeport et carte d'identité électronique
- ◆ ...

Certification des cartes et de terminaux sans contact

- ◆ Objectif et principes de la conformité
- ◆ Les normes ISO 9646 et leur application à la conformité "contactless"
- ◆ Signification de la conformité
- ◆ Essais et Tests : méthodes de tests / suites de tests
- ◆ Les laboratoires d'essais
- ◆ Bâtir un schéma d'homologation

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin de maîtriser les applications et les technologies des cartes à puce sans contact.



F6.4. NFC : Near Field Communications

Durée standard : 3 jours

Near Field Communication (NFC) est une technologie de communication de proximité qui résulte des technologies sans contact. Ses usages vont de l'échange d'informations dématérialisé au paiement sécurisé et contrôlé via un équipement de poche (téléphone mobile, appareil de photo) lequel peut être aussi utilisé comme une carte à puce ou un lecteur, un téléviseur, une automobile ... Cette formation permet d'appréhender tous les détails techniques et toutes les problématiques fonctionnelles, applicatives, d'usage et de service, afférentes à la technologie de même que la mise en œuvre dans un appareil NFC.

NFC : fonctions, applications et approfondissement technique radio

- ◆ Introduction à NFC
- ◆ A quoi sert NFC ?
- ◆ NFC sur le terrain
- ◆ NFC en pratique
- ◆ Caractéristiques techniques de NFC
- ◆ L'interface air : ses problèmes et ses solutions
- ◆ NFC et applications autour du marché de la téléphonie mobile
- ◆ NFC et les relations ISO avec la « RFID » et les « mobiles RFID »
- ◆ Conclusions et commentaires

Développement d'un service NFC

- ◆ Principales spécifications Techniques et Marketing du marché (AEPM, GSMA/Pay Buy Mobile, Mastercard/Paypass, Cityzi, GlobalPlatform et NFC Forum)
- ◆ Créer un Tiers de Confiance et administrer les services multi applications

NFC Forum : protocoles, spécifications et tests – approfondissement technique

- ◆ Typologie technique des Applications et NFC Forum
- ◆ Descriptions techniques détaillées des protocoles et formats de communication des normes NFCIP 1, NFCIP 2 et des normes du NFC Forum
- ◆ Encapsulation des couches hautes applicatives dans les couches de communication
- ◆ Les tests de conformité software
- ◆ Conclusions et commentaires

Public concerné

Tout Ingénieur, Technicien, Gestionnaire, Commercial ou autre ayant besoin de maîtriser les technologies et les usages des communications en champ proche (NFC).