# FORMATION : SÉCURITÉ

## DS-122 : Sécuriser un réseau WiFi à la norme 802.11i *(2 jours)*

### Logiciels utilisés

Linux, FreeRadius, OpenLDAP et OpenSSL

### Présentation

La sécurité est un aspect à ne pas négliger lors du déploiement d'un réseau sans fil. Afin de préserver la confidentialité des données de l'entreprise, il est nécessaire de mettre en place un système d'authentification qui n'autorise que les personnes habilitées à se connecter en WiFi, et un système de chiffrement qui assure l'intégrité des données échangées par le client.

Les protocoles pouvant être mis en place sont nombreux, mais peu remplissent ces deux objectifs.

### Objectifs

Ce stage permet aux administrateurs réseaux et sécurité de comprendre l'ensemble des spécificités de la sécurité des réseaux sans fil en terme de chiffrement des données et d'authentification des utilisateurs.
Ils pourront ensuite appréhender la mise en place d'un réseau sans fil sécurisé à la norme 802.11i en ayant recours à des certificats numériques côté serveur et côté client.

### Public Concerné

Administrateur réseaux/sécurité

### Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Notions sur le chiffrement informatique et sur les certificats numériques (ex: SSL)

Installation et configuration de réseaux sans fil en mode WEP (point d'accès et client)

### Programme

**JOUR 1 – Théorie des réseaux sans fil**

Définition, terminologie et rappels lexicaux
- WiFi
- 802.11b/g, 802.1x
- 802.11i

Authentification et chiffrement sur WiFi
- Études comparatives : WEP, WPA, WPA2, WPA-PSK, TKIP, EAP-TLS, EAP-TTLS, LEAP
- Principes de fonctionnement
- Bénéfices et contraintes

Maquette
- Mise en place d'un réseau sans fil sécurisé à la norme WPA/WPA2 basé sur des certificats

**JOUR 2 – Utiliser EAP-TLS et EAP-TTLS**

Maquette - PKI
- Installer et configurer une infrastructure à clés publiques (PKI), gestion et déploiement de certificat

Maquette – EAP-TTLS avec Freeradius
- Configurer un serveur RADIUS 802.1x
- Installer et configurer un point d'accès en mode authentification EAP
- Installer et configurer un client WiFi WPA
  - TKIP ou AES pour le chiffrement
  - EAP-TTLS pour l'authentification

Le programme ci-dessus présente le programme initial de la formation DS-122 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.