

## Formation Fonctionnement des PKI



Si les PKI ont longtemps été mises à l'honneur, la réalité de leurs déploiements demeure toutefois plus mitigée.

Cette session fournit une approche pragmatique des possibilités offertes au travers de la technologie des PKI et indique la méthode pour optimiser leur mise en place

### Objectifs

---

- Acquérir la maîtrise des concepts de clé publique et des certificats
- Appréhender les enjeux et limites des infrastructures de gestion de clés

### Public concerné

---

- Responsable sécurité
- Chef de projets
- Acteur d'un projet sécurité

### Pré requis

---

- Une connaissance élémentaire de mécanismes cryptographiques de base (chiffrement, signature) est recommandée
- Avoir suivi la formation "Sécurité des réseaux et des transmissions"

### Une formation d'une journée

---

Caractéristiques
<b>Tarif : 1200 € HT par personne</b>
<b>Numéro de formateur : 11753687675</b>
<b>Nombre d'heures : 7</b>
<b>Référence : SPKI</b>
<b>Contact : Loic LE FUR</b>
<b>Telephone : 01.45.28.09.82</b>
<b>Email : <a href="mailto:contact@anaska.com">contact@anaska.com</a></b>

Paris
<b>09/06/2008</b>

## Description des modules

num	Module
1	<b>Base de cryptographie</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Introduction et contexte (dématérialisation des échanges)</li><li>- Vocabulaire et notions de base</li><li>- Algorithmes à clef secrète</li><li>- Algorithmes à clef publique</li><li>- Fonctions de hachage</li><li>- Boîte à outils (Open SSL, DumpASN1, SSLDump)</li><li>- En pratique : chiffrement et signature, messagerie « sécurisée » avec S/MIME</li></ul>
2	<b>De la clé publique au certificat</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Introduction (Clef SSH, clef PGP, problématique de la certification)</li><li>- Les certificats X.509 : standard X.509, profil PKIX, champs standards et extensions X.509v3</li><li>- En pratique : panorama des certificats inclus dans Windows 2000, sécurisation des échanges avec SSL/TLS, télé déclaration des impôts</li></ul>
3	<b>Architectures PKI</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Introduction</li><li>- Architecture et composantes : analogie : carte d'identité nationale; entités et rôles respectifs</li><li>- Cycle de vie des certificats : demande de certificat; signature de demande de certificat ; publication de certificat ; révocation de certificat</li><li>- Politique énoncé de pratiques de certification</li></ul>
4	<b>ICP commerciales</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Offres (Microsoft, Baltimore, Entrust...)</li><li>- Critères de sélection</li><li>- Descriptions et choix techniques</li></ul>