# Table des matières

**Public** : personnels opérant des serveurs

# Certificats X.509

**Règle** : le RSSI impose qu'aucun mot de passe ne transite « en clair », suivant en cela les bonnes pratiques en cours. Tout service requérant une authentification par *login* / mot de passe doit donc passer uniquement à travers un protocole chiffré.

Les services sécurisés par TLS (HTTPS par exemple) requièrent un certificat X.509. Pour que les clients se connectent de manière transparente, ils ont besoin de connaître l'autorité de certification. La DSI peut fournir de tels certificats ainsi reconnus pour un certain nombre de domaines DNS qu'elle opère.

Voir Créer une demande de certificat X.509 & Ajouter les certificats X.509 manquants.

**Information** : Les certificats sont à renouveler une fois par an.