

CRÉATION D'UNE AUTORITÉ DE CERTIFICATION

INFRASTRUCTURE À CLÉS PUBLIQUES

STORMSHIELD

Programme du module

- ✓ Qu'est-ce que la cryptographie ?
- ✓ Éléments de cryptographie
- ✓ Infrastructures à clés publiques
- ✓ PKI Stormshield Network
- ➔ Création d'une autorité de certification
 - Création d'une identité serveur
 - Création d'une identité utilisateur
 - Gestion des identités et certificats
 - Révocation de certificats et CRL
 - Lab - PKI

CRÉATION D'UNE AUTORITÉ DE CERTIFICATION

- Création d'une autorité de certification : étape 1

Autorité racine

CREATE ROOT AUTHORITY

CERTIFICATE AUTHORITY PROPERTIES

CN: Root-CA-Training
Identifier: Root-CA-Training

Authority attributes

Organization: Training
Organizational unit: CSNE
City (L): Paris
State (ST): IdF
Country: France

Buttons: CANCEL, PREVIOUS, NEXT

Sous-autorité

CREATE SUB AUTHORITY

CERTIFICATE AUTHORITY PROPERTIES

CN: Sub-CA-Training-Lyon
Identifier: Sub-CA-Training-Lyon

Select the parent Authority

Parent CA: Select a CA as a parent of this one
CA passphrase: [password field]

Authority attributes

Organization: Training-Lyon
Organizational unit: CSNE
City (L): LYON
State (ST): Rhône
Country: France

Buttons: CANCEL, PREVIOUS, NEXT

24

Création d'une autorité de certification (C.A.) – 1^{ère} étape

Vous devez définir les propriétés de l'autorité que vous souhaitez ajouter :

⚠ AVERTISSEMENT

Ces informations ne sont plus modifiables après leur création.

CN	Saisissez un nom permettant d'identifier l'autorité de certification (64 caractères au maximum)
Identifiant	Permet de définir un raccourci de l'attribut CN (champ optionnel)
Autorité parente	Pour une sous-autorité, permet d'indiquer l'autorité de certification parente (forcément créée au préalable puisqu'elle va signer le certificat de la sous-autorité)
Mot de passe autorité parente	Obligatoire pour valider la signature du certificat de la sous-autorité en cours de création
Organisation (O)	Nom de l'organisation
Unité d'organisation (OU)	Branche au sein de l'organisation
Lieu (L)	Ville où est située l'organisation
Etat ou province (ST)	Département ou état où est située l'organisation
Pays (C)	Pays où est située l'organisation

CRÉATION D'UNE AUTORITÉ DE CERTIFICATION

- Création d'une autorité de certification : étape 2

25

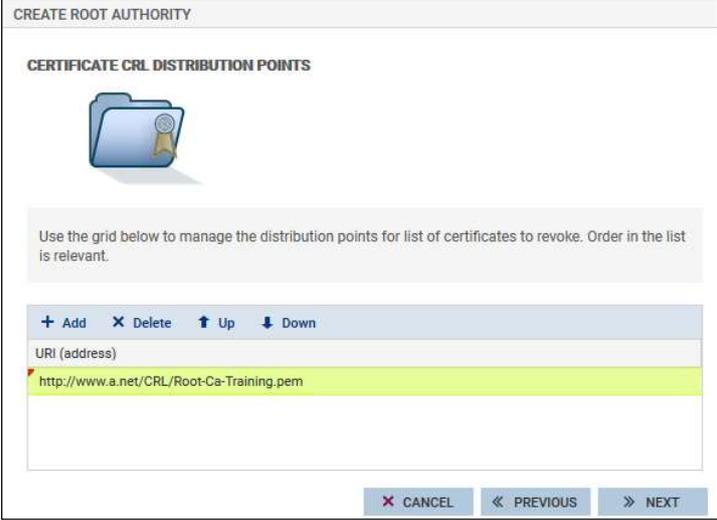
Création d'une autorité de certification - 2^{ème} étape

Vous devez définir les propriétés de l'autorité que vous souhaitez ajouter :

Mot de passe (8 car. Min.)	<p>Saisissez un mot de passe de 8 caractères minimum afin de protéger l'accès à la clé privée de votre CA.</p> <p>⚠ AVERTISSEMENT</p> <p>Ce mot de passe n'est pas récupérable sur le firewall. Si vous l'oubliez, vous ne pourrez plus signer de certificats ou de CRLs avec cette CA.</p>
Confirmez le mot de passe	Tapez une seconde fois votre mot de passe dans ce champ afin de le confirmer.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe . Il est fortement conseillé d'utiliser des majuscules, minuscules, chiffres et caractères spéciaux.
E-mail	Renseignez l'adresse e-mail du gestionnaire de la CA (optionnel).
Type de clé	Permet de choisir entre une clé RSA classique ou basée sur des courbes elliptiques.
Taille de clé (bits)	Choix de la taille de la clé. Plus la taille de la clé est grande, plus les opérations réalisées avec cette clé sont sécurisées.
Validité (jours)	Ce champ correspond au nombre de jours durant lesquels votre certificat d'autorité et par conséquent votre PKI seront valides. Une fois ce certificat expiré, tous les certificats émis sont considérés comme invalides. Cette valeur n'est pas modifiable par la suite.

CRÉATION D'UNE AUTORITÉ DE CERTIFICATION

- Création d'une autorité de certification : étape 3



26

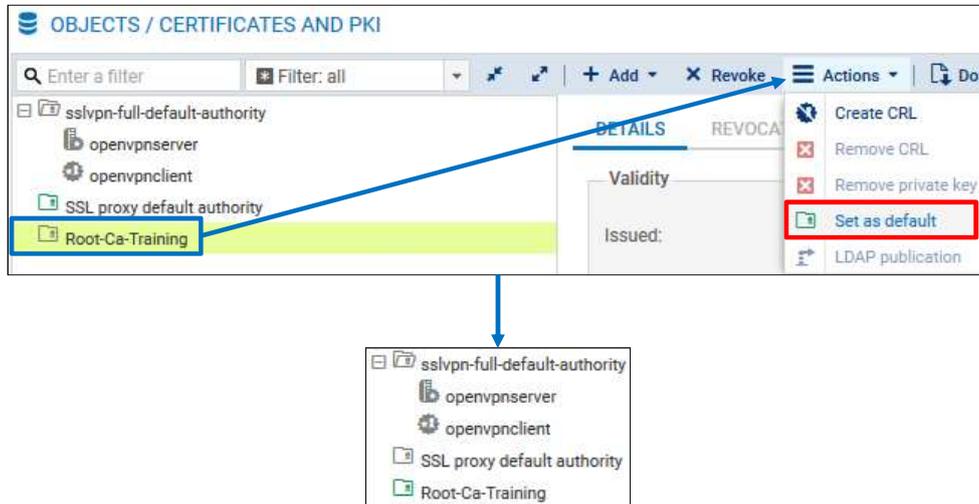
Création d'une autorité de certification - 3^{ème} étape

Vous devez définir les propriétés de l'autorité que vous souhaitez ajouter :

<p>Distribution de la CRL</p>	<p>Vous pouvez indiquer les points de distribution (URL) de la liste des certificats révoqués (invalides).</p> <p>⚠ AVERTISSEMENT ces CRLDP sont visibles dans tous les certificats signés par cette CA. L'équipement ne maintient pas à jour automatiquement le fichier CRL disponible à ces emplacements.</p>
--------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CRÉATION D'UNE AUTORITÉ DE CERTIFICATION

- Autorité de certification par défaut



27

Définir une autorité de certification en tant qu'autorité par défaut

1. Mettez l'autorité souhaitée en surbrillance,
2. Dans le menu Action, cliquez sur **Définir comme défaut**, l'autorité par défaut apparaît en vert à l'affichage.

Nous verrons plus tard dans ce module qu'il est possible de générer une identité utilisateur directement depuis l'annuaire LDAP interne du firewall. Dans ce cas, le choix de l'autorité signataire se porte automatiquement sur la CA désignée par défaut.