

CRÉATION D'UNE IDENTITÉ SERVEUR

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 IDENTITÉ SERVEUR

- Création d'une identité serveur : étape 1

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

Fully Qualified Domain Name (FQDN): server1.training.net

ID: server1.training.net

X CANCEL << PREVIOUS >> NEXT

STORMSHIELD

29

Création d'une identité serveur – 1^{ère} étape

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

Nom de domaine pleinement qualifié (FQDN)	Saisissez le nom de domaine pleinement qualifié du serveur pour lequel il faut générer l'identité. Ce paramètre est inscrit comme CN dans le certificat correspondant. Il doit généralement coïncider avec le nom DNS du serveur auquel il est destiné et dont il représente l'identité.
Identifiant	Permet de définir un raccourci de l'attribut FQDN (champ optionnel).

CRÉATION D'UNE IDENTITÉ SERVEUR

- Création d'une identité serveur : étape 2

30

Création d'un certificat serveur – 2^{ème} étape

Il s'agit de choisir l'autorité de certification à utiliser pour le certificat serveur :

Autorité de certification (CA)	Permet de choisir l'autorité de certification qui génère l'identité serveur et qui va signer le certificat correspondant. Il est possible de choisir l'autorité de certification parmi toutes celles dont l'identité est stockée sur le firewall.
Mot de passe de l'autorité	Saisir le mot de passe de l'autorité de certification permet l'accès à sa clé privée utilisée pour signer le certificat serveur.
Attributs du certificat	Il s'agit d'informations pré-remplies en fonction de l'autorité de certification sélectionnée.

CRÉATION D'UNE IDENTITÉ SERVEUR

- Création d'une identité serveur : étape 3

STORMSHIELD

31

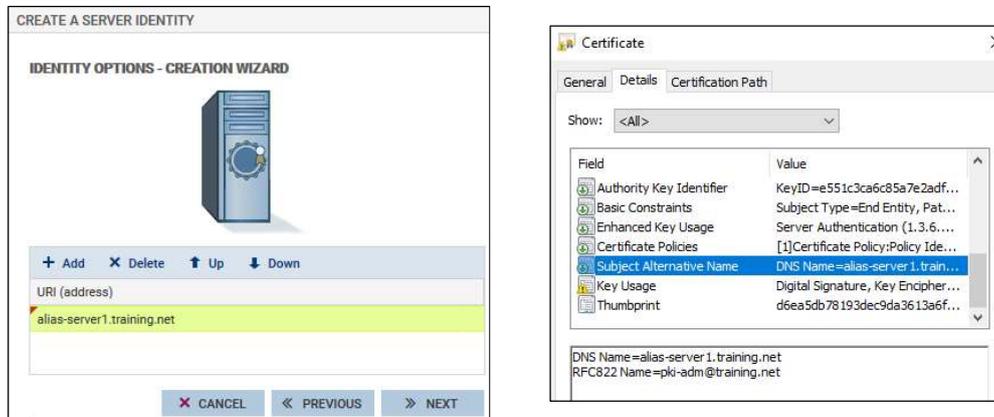
Création d'un certificat serveur – 3^{ème} étape

Vous devez définir ici la durée de validité du certificat que vous ajoutez :

Validité	Durée de validité du certificat serveur. Par défaut, cette valeur est fixée à 365 jours.
Type de clé	Permet de choisir entre une clé classique ou basée sur des courbes elliptiques.
Taille de clé (bits)	Définir la taille de clé à utiliser pour les chiffrements asymétriques faisant intervenir l'identité serveur en cours de création.

CRÉATION D'UNE IDENTITÉ SERVEUR

- Création d'une identité serveur : étape 4

**Création d'un certificat serveur – 4^{ème} étape**

Vous pouvez ajouter au certificat du serveur qui va être signé par la CA des noms DNS différents (attribut Subject Alternative Name dans un certificat).

Le caractère * (wildcard) n'est pas accepté ici.

CRÉATION D'UNE IDENTITÉ SERVEUR

- Création d'une identité serveur : récapitulatif

CREATE A SERVER IDENTITY

SUMMARY

Finish this wizard in order to create the server identity below

Name:	server1.training.net
Identifier:	server1.training.net
Parent authority:	Root-Ca-Training
Organization:	Training
Organizational unit:	CSNE
City (L):	Paris
State (ST):	Idf
Country:	FR
Key size:	2048

Valid until Tue Dec 01 2020 10:02:26 GMT+0100 (Central European Standard Time) (365 days)

33

Création d'un certificat serveur – récapitulatif

Avant de valider la création de l'identité du serveur, vérifiez attentivement l'ensemble des informations saisies.

Les noms DNS différents (attribut Subject Alternative Name dans le certificat correspondant à cette identité) n'apparaissent pas dans le récapitulatif.