

CRÉATION D'UNE IDENTITÉ UTILISATEUR 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 UTILISATEUR

- Création d'une identité utilisateur : étape 1

STORMSHIELD

35

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

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

NOTE

Une fois le certificat généré et publié par l'administrateur, l'identité numérique de l'utilisateur doit lui être transmise par une voie sécurisée.

CN	Saisissez le nom de l'utilisateur dans la limite de 64 caractères maximum.
Identifiant	Permet de définir un raccourci de l'attribut CN (champ optionnel).
Mail	Renseigner l'adresse e-mail de l'utilisateur. Cette information peut être utilisée pour identifier l'utilisateur lorsqu'il présente son certificat. Ce champ est obligatoire.

CRÉATION D'UNE IDENTITÉ UTILISATEUR

- Création d'une identité utilisateur : étape 2

CREATE A USER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

Select the parent Authority

Parent CA: Root-Ca-Training

CA passphrase:

Authority attributes

Organization: Training

Organizational unit: CSNE

City (L): Paris

State (ST): Idf


Country: France

CANCEL PREVIOUS NEXT

36

Création d'une identité utilisateur – 2^{ème} étape

Choisir l'autorité de certification à utiliser pour signer le certificat utilisateur :

<p>Autorité de certification (CA)</p>	<p>Permet de choisir l'autorité de certification signataire du certificat utilisateur.</p> <p>Il est possible de choisir l'autorité de certification parmi toutes celles dont la clé privée est stockée dans les objets PKI.</p> <p> L'assistant de configuration présélectionne l'autorité de certification par défaut.</p>
<p>Mot de passe de l'autorité</p>	<p>Saisir le mot de passe de l'autorité de certification permet l'accès à sa clé privée utilisée pour signer le certificat utilisateur.</p>
<p>Attributs du certificat</p>	<p>Il s'agit d'informations pré-remplies en fonction de l'autorité de certification sélectionnée ou désignée par défaut.</p>

CRÉATION D'UNE IDENTITÉ UTILISATEUR

- Création d'une identité utilisateur : étape 3

37

Création d'une identité utilisateur – 3^{ème} étape

Validité	Durée de validité du certificat utilisateur. 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 utilisateur en cours de création.
Publier ce certificat dans l'annuaire LDAP	En cochant cette case, une copie du certificat est stockée dans l'annuaire LDAP et ainsi mise à disposition pour téléchargement à partir du portail captif; ce qui facilite sa distribution. Pour pouvoir utiliser cette option, il est impératif, que l'identifiant (ID) et l'adresse email saisis soient identiques à ceux d'un utilisateur existant dans la base LDAP (interne ou externe) avec laquelle le firewall est connecté (comme dans l'exemple ci-dessus).

Mot de passe du container PKCS#12 publié	Le container PKCS#12 contient l'identité de l'utilisateur, ainsi que le certificat de l'autorité de certification signataire. Renseignez un mot de passe afin de protéger ces informations sensibles.
Confirmez le mot de passe	Retapez 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 : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

CRÉATION D'UNE IDENTITÉ UTILISATEUR

- Création d'une identité utilisateur : récapitulatif

CREATE A USER IDENTITY

SUMMARY

Finish this wizard in order to create the user identity below

Name:	Boris.Vassiliev
Identifier:	Boris.Vassiliev
Parent authority:	Root-Ca-Training
Organization:	Training
Organizational unit:	CSNE
City (L):	Paris
State (ST):	Idf
Country:	FR
E-mail address (E):	boris.vassiliev@kgb.ru
Key size:	2048

The identity will be published in the LDAP

Valid until Tue Dec 01 2020 12:37:11 GMT+0100 (Central European Standard Time) (365 days)

39

Création d'une identité utilisateur – récapitulatif

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

Après validation de la création, la bi-clé est générée, le certificat est signé et tous deux sont stockés localement sur le firewall dans les objets **CERTIFICATS ET PKI** ; une copie du certificat est publiée dans la base LDAP lorsque l'option correspondante a été demandée.

CRÉATION D'UNE IDENTITÉ UTILISATEUR

- Création d'une identité utilisateur via LDAP :

The screenshot displays the 'USERS / USERS AND GROUPS' management interface. A user profile for 'Raoul Volfoni' is selected, and the 'CERTIFICATE' tab is active. A 'Create the certificate' button is highlighted with a blue box. A blue arrow points from this button to a 'CREATION OF THE USER CERTIFICATE' dialog box. This dialog box contains fields for 'Password (min. 8 chars)', 'Confirm password', and 'CA password', along with 'Good' and 'CREATE THE CERTIFICATE' buttons.

Création d'une identité utilisateur à partir de sa fiche LDAP

Il est possible de déclencher la génération d'une identité utilisateur directement à partir de l'annuaire LDAP.

Le choix de la CA se porte automatiquement sur la CA désignée par défaut :

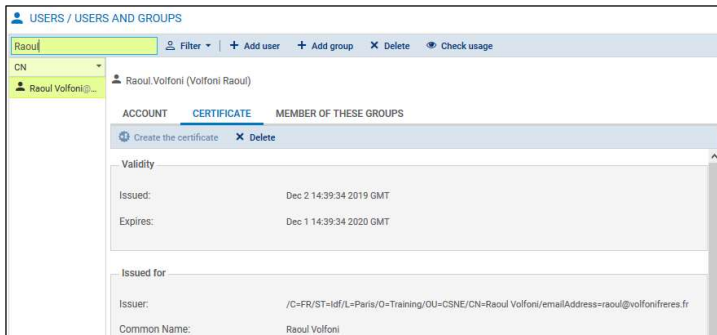
- La publication du certificat utilisateur dans la base LDAP est immédiate,
- L'identité de l'utilisateur est ajoutée dans les objets **CERTIFICATS ET PKI**.

Note

- Lorsque l'annuaire est un LDAP de type Active Directory, l'accès en lecture/écriture utilisant un compte ayant suffisamment de droits est requis pour publier les certificats sur l'annuaire.

CRÉATION D'UNE IDENTITÉ UTILISATEUR

- Création d'une identité utilisateur via LDAP : résultat



Vue du
certificat dans
l'annuaire

Vue de l'identité dans la CA



Le certificat correspondant est obligatoirement signé par la CA par défaut, le CN du certificat est identique au CN de l'utilisateur tel qu'il est défini dans la base LDAP.