Programme du module

- ✔ Qu'est-ce que la cryptographie ?
- ✔ Eléments 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

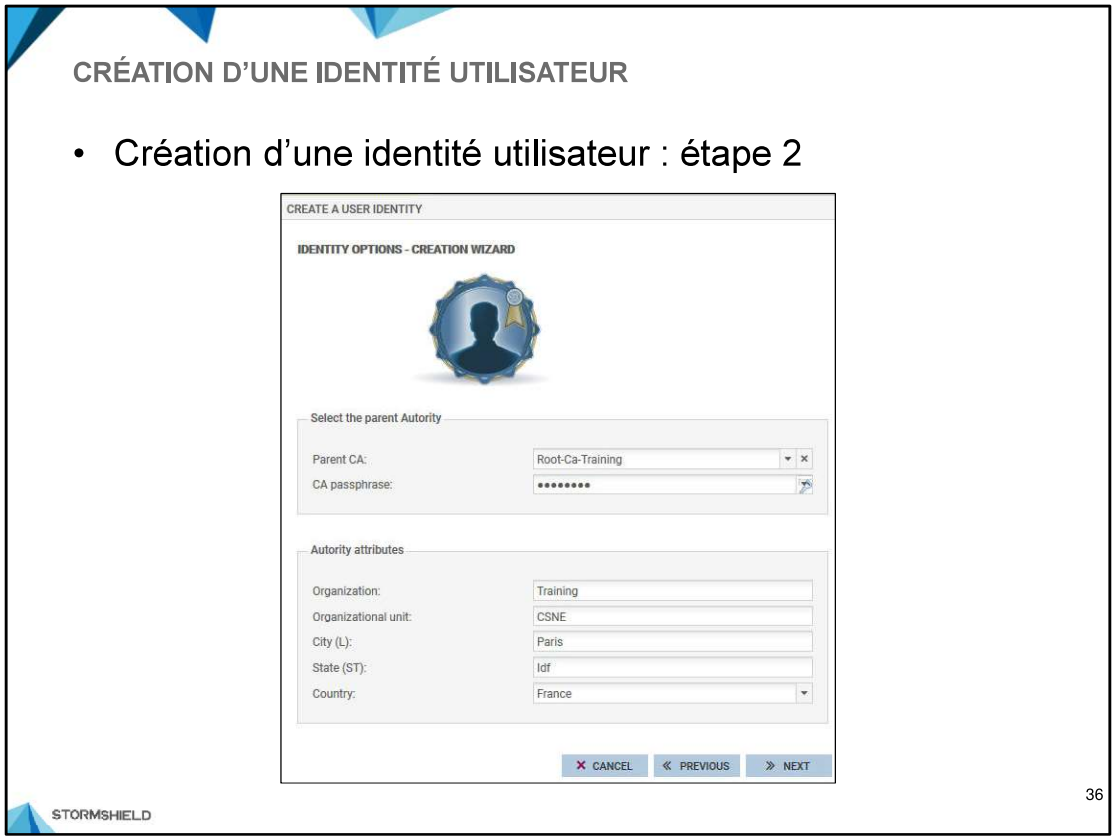
Création d'une identité utilisateur – 1ère étape

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.

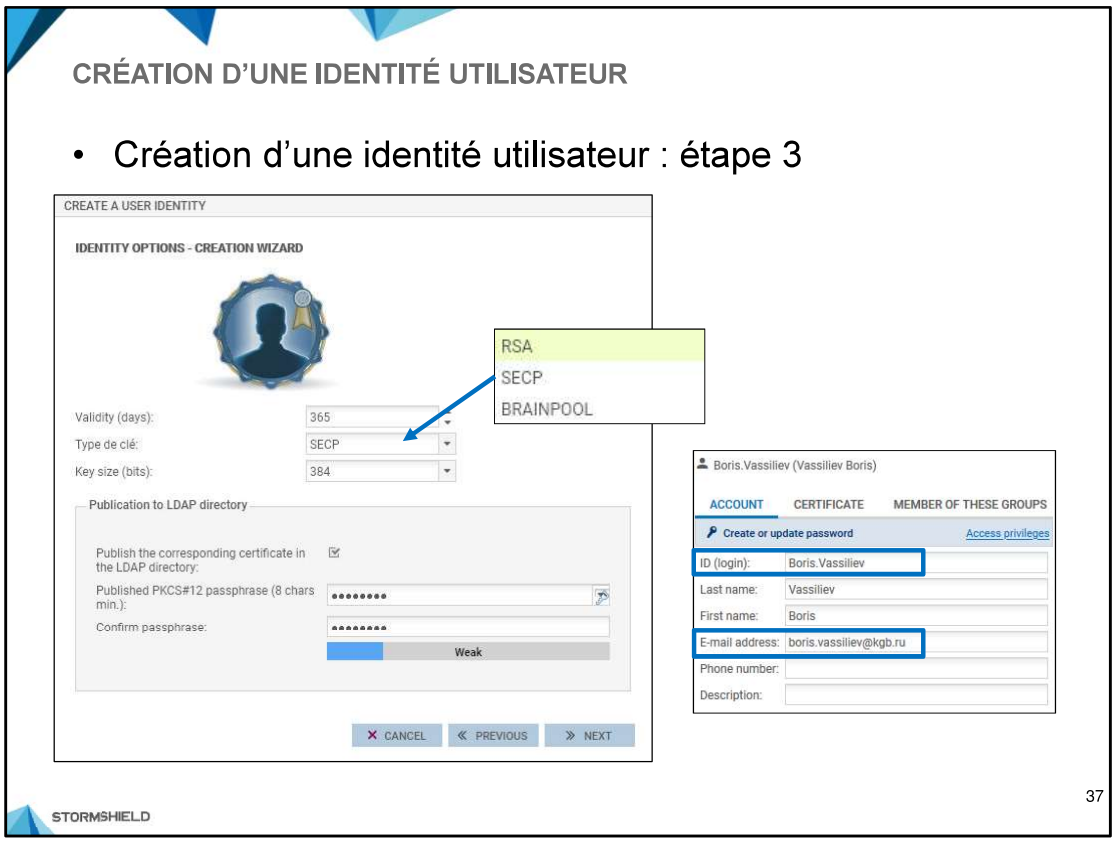
CN	Saisissez le nom de l'utilisateur dans la limite de 64 caractères maximum.
Identifiant	Permet de définir un raccourci de l'attribut CN (champ optionnel).
Mail	Renseigner l'adresse e-mail de l'utilisateur. Cette information peut être utilisée pour identifier l'utilisateur lorsqu'il présente son certificat.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



Création d'une identité utilisateur – 2ième étape

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

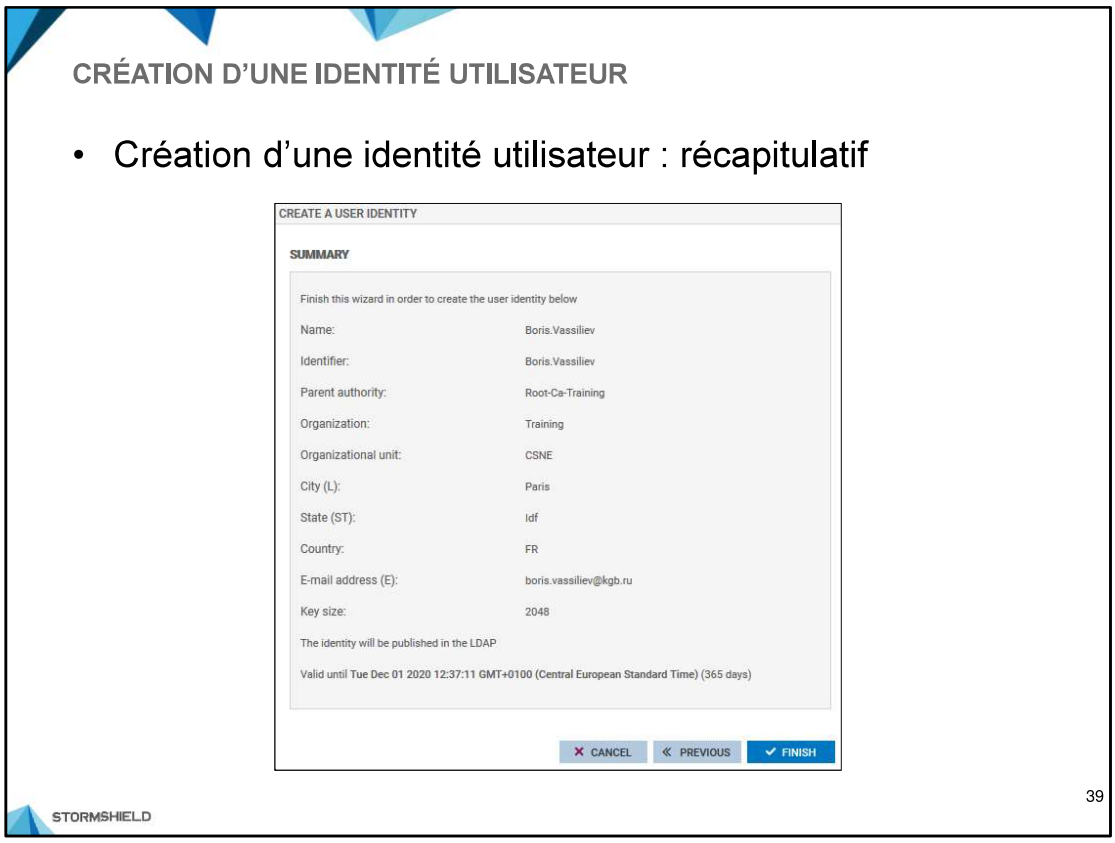
Autorité de certification (CA)	Permet de choisir l'autorité de certification signataire du certificat utilisateur. Il est possible de choisir l'autorité de certification parmi toutes celles dont la clé privée est stockée dans les objets PKI. L'assistant de configuration présélectionne l'autorité de certification par défaut.
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 utilisateur.
Attributs du certificat	Il s'agit d'informations pré-remplies en fonction de l'autorité de certification sélectionnée ou désignée par défaut.



Création d'une identité utilisateur – 3ième 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).

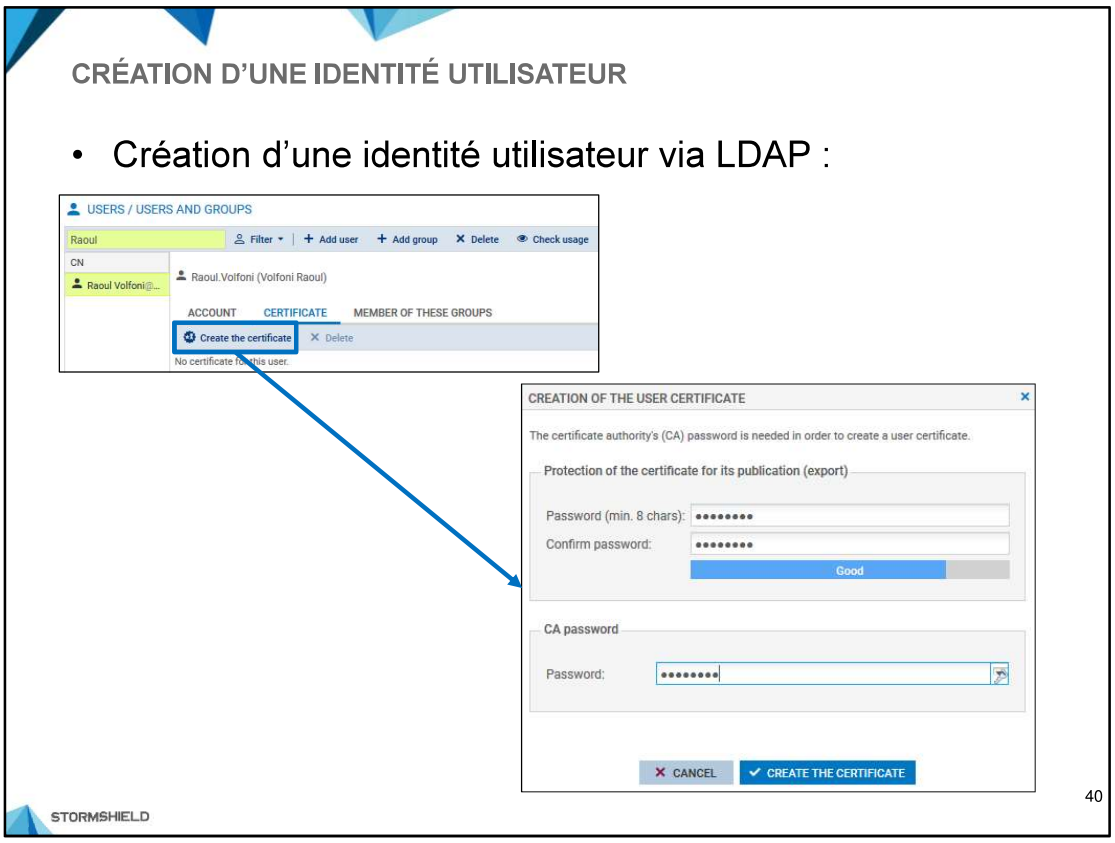
Mot de passe du container PKCS#12 publié	Le container PKCS#12 contient l 'identité de l'utilisateur, ainsi que le certificat de l'autorité de certification signataire Renseignez un mot de passe afin de protéger ces informations sensibles.
Confirmez le mot de passe	Retapez une seconde fois votre mot de 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 – 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 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 :

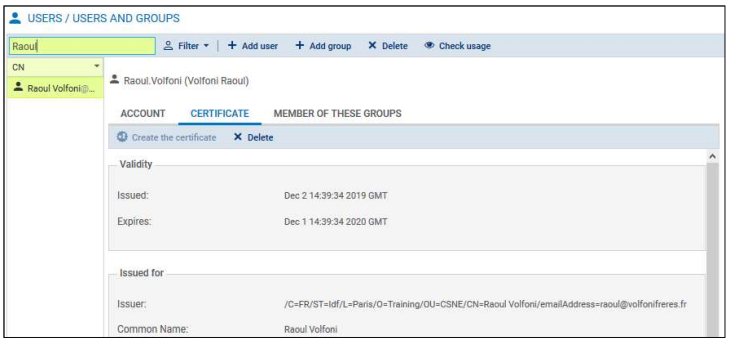
- La publication du certificat utilisateur dans la base LDAP est immédiate,
- L'identité de l'utilisateur est ajoutée dans les objets **CERTIFICATS ET PKI**.

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

41

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.