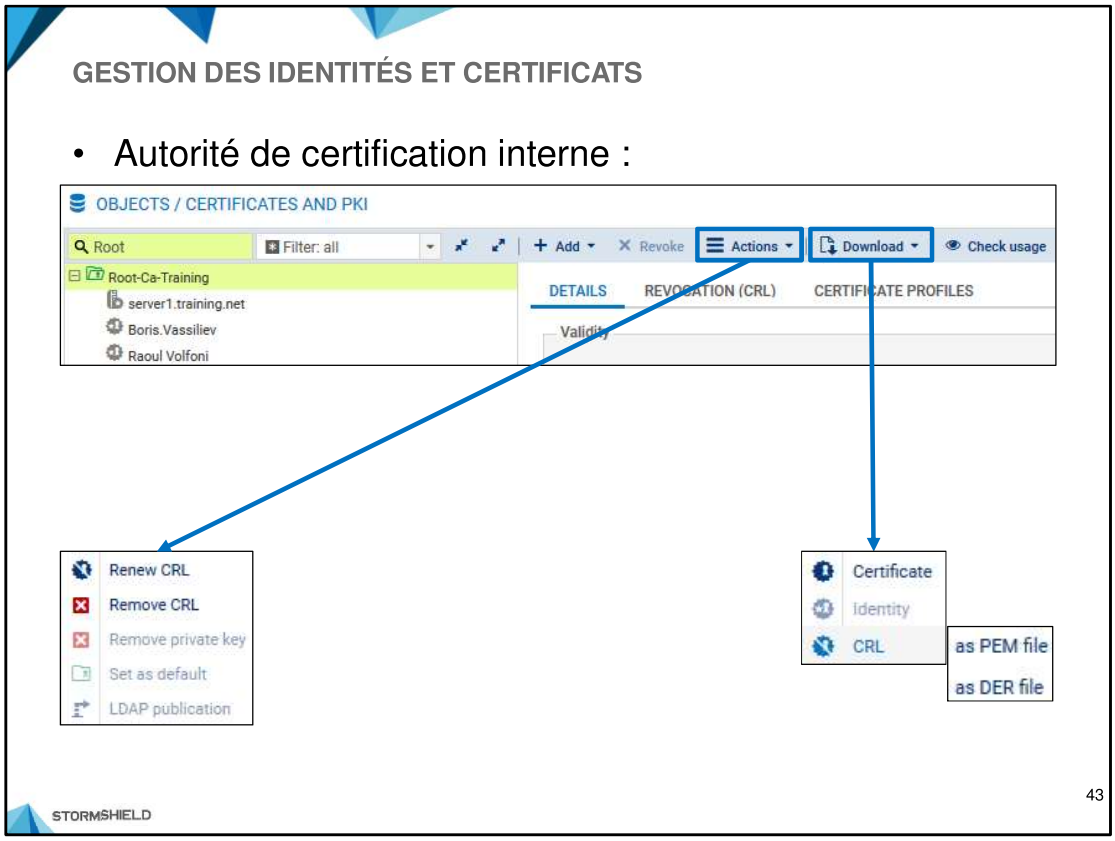
Programme du module

- ✔ 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



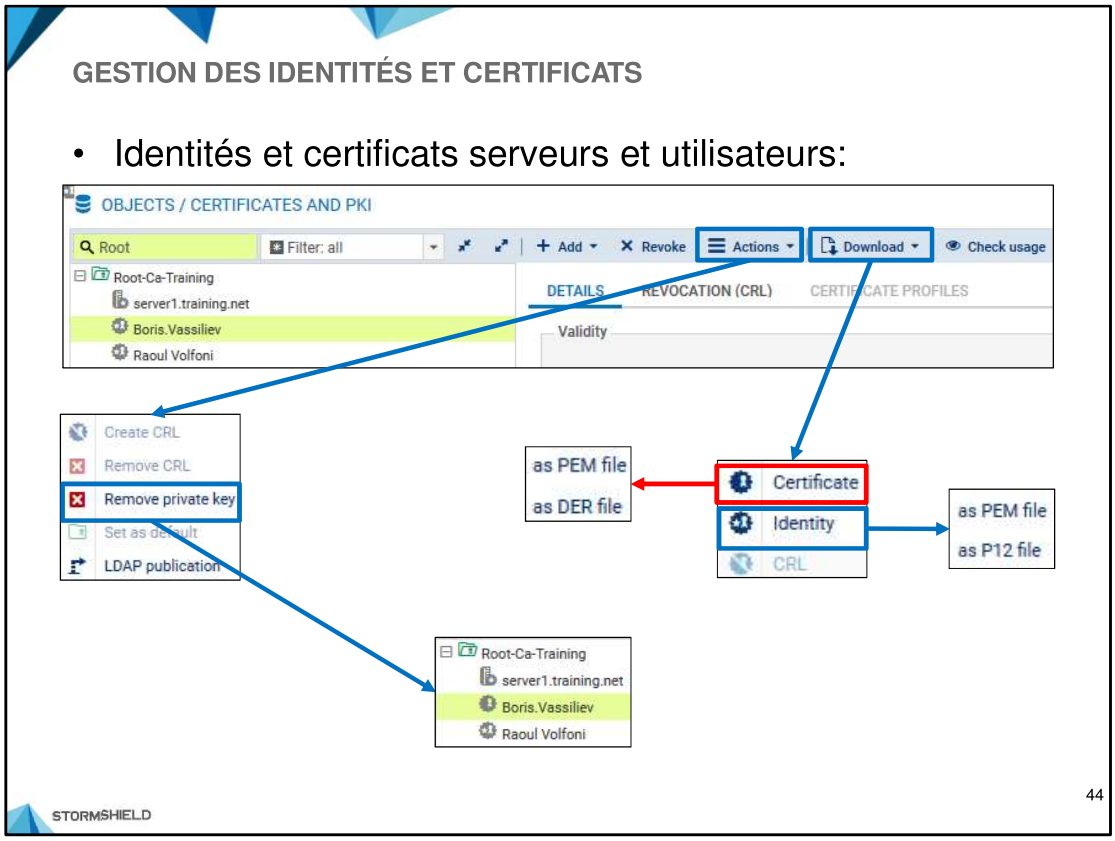
Menu Actions

Pour une autorité de certification interne (créée sur le firewall), les actions suivantes sont possibles :

- **Créer / Renouveler la CRL :** Lorsqu'une autorité de certification est créée, vous pouvez créer la CRL, puis la renouveler ultérieurement. Le renouvellement de la CRL est automatique sur le firewall (une fois par mois), mais pas la maintenance des éventuels points de distribution (CRLDP) aux emplacements où ils ont été définis.
- **Supprimer la CRL :** il est possible de supprimer la CRL.
- **Définir comme défaut :** lors de la création d'une identité utilisateur depuis sa fiche LDAP, l'annuaire défini par défaut est automatiquement utilisé. L'option est grisée dans l'exemple ci-dessus car l'autorité de certification en surbrillance est déjà l'autorité par défaut.

Menu Télécharger

- **Certificat :** le format d'export contient des données en base64 (.pem) ou des données binaires (.der)
- **CRL :** le fichier de CRL exporté permet de maintenir les CRLDP externes (même format d'export que pour les certificats).



Menu Actions

Pour un serveur ou un utilisateur, les actions suivantes sont possibles :

- **Supprimer la clé privée :** l'identité du serveur ou de l'utilisateur est stockée sur le firewall. Après suppression de la clé privée, il reste seulement le certificat, les icônes utilisées sont différentes, comme illustré ci-dessus.
- **Publication LDAP (utilisateur uniquement) :** lorsque le certificat d'un utilisateur est présent sur le firewall, il peut être publié sur l'annuaire, si les champs ID (login) et adresse e-mail correspondent, comme détaillé dans le chapitre « Création d'une identité utilisateur ».

Menu Télécharger

- **Certificat :** le format d'export contient des données en base64 (.pem) ou des données binaires (.der). Le fichier exporté contient le certificat du porteur mais également les certificats des autorités présentes dans la chaîne de confiance de ce certificat.
- **Identité :** l'identité, puisqu'elle contient une clé privée, est sensible et son export doit être protégé par un mot de passe, lequel permet de chiffrer la clé privée qu'il contient. L'identité est pour rappel constituée de la clé privée du porteur, de son certificat (qui contient sa clé publique), et des certificats de la chaîne de confiance. le fichier d'export est un container .pem ou un container PKCS#12 (ou .p12).