autorité-certififcation

```
MARK RODERICK - Certificats
```

🔑 PKI (Infrastructure à clés publiques)

PKI (Public Key Infrastructure) = système basé sur des certificats numériques et une paire de clés (publique/privée) pour sécuriser les communications.

PKI est idéal pour les environnements professionnels où la sécurité et la confiance sont essentielles.

Principe : repose sur la cryptographie asymétrique.

- Une **clé publique** : utilisée pour chiffrer ou vérifier une signature.
- Une **clé privée** : utilisée pour déchiffrer ou signer.
- **Certificats numériques :** délivrés par une autorité de certification (CA), ils garantissent l'identité d'un site, d'une personne ou d'un appareil.

Avantages :

- Sécurité élevée (difficile à casser).
- Authentification fiable grâce aux certificats.
- Utilisé dans HTTPS, emails sécurisés, VPN, etc.

Inconvénients :

- Complexité de mise en place.
- Nécessite une gestion des certificats (renouvellement, révocation).

🔒 PSK (Pre-Shared Key)

PSK (Pre-Shared Key) = mot de passe partagé à l'avance entre deux parties pour établir une connexion sécurisée.
PSK est pratique pour des usages simples (Wi-Fi domestique), mais moins robuste.

- **Principe :** une clé secrète (mot de passe) est partagée à l'avance entre deux parties.
- **Utilisation :** souvent dans les réseaux Wi-Fi WPA/WPA2 ou certains VPN.

Avantages :

- Simplicité : facile à mettre en place.
- Pas besoin de certificats ni d'autorité externe.

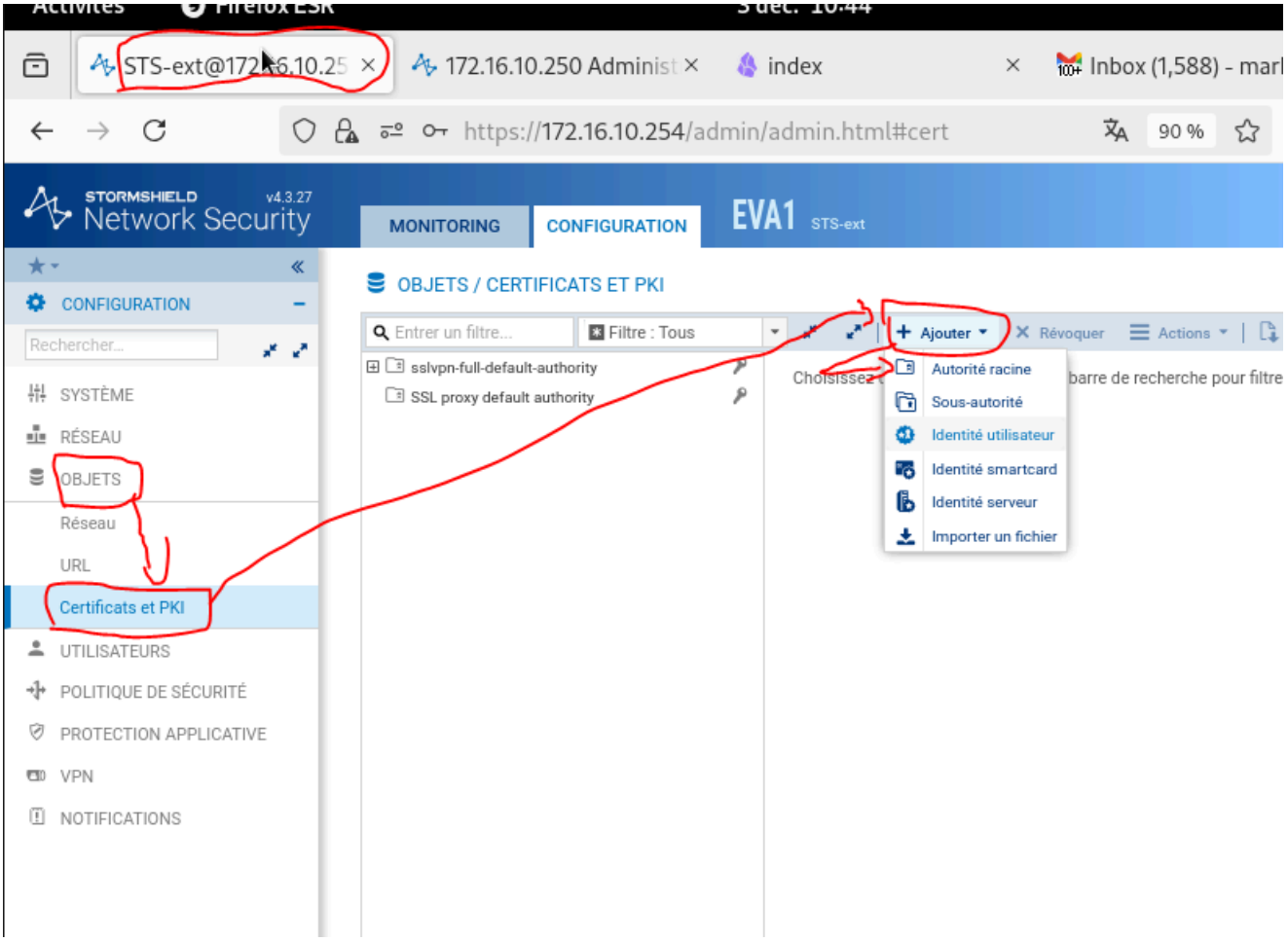
Inconvénients :

- Moins sécurisé : si la clé est divulguée, tout le système est compromis.
- Difficile à gérer dans de grands réseaux (changer la clé pour tous les utilisateurs).

Comparaison simple

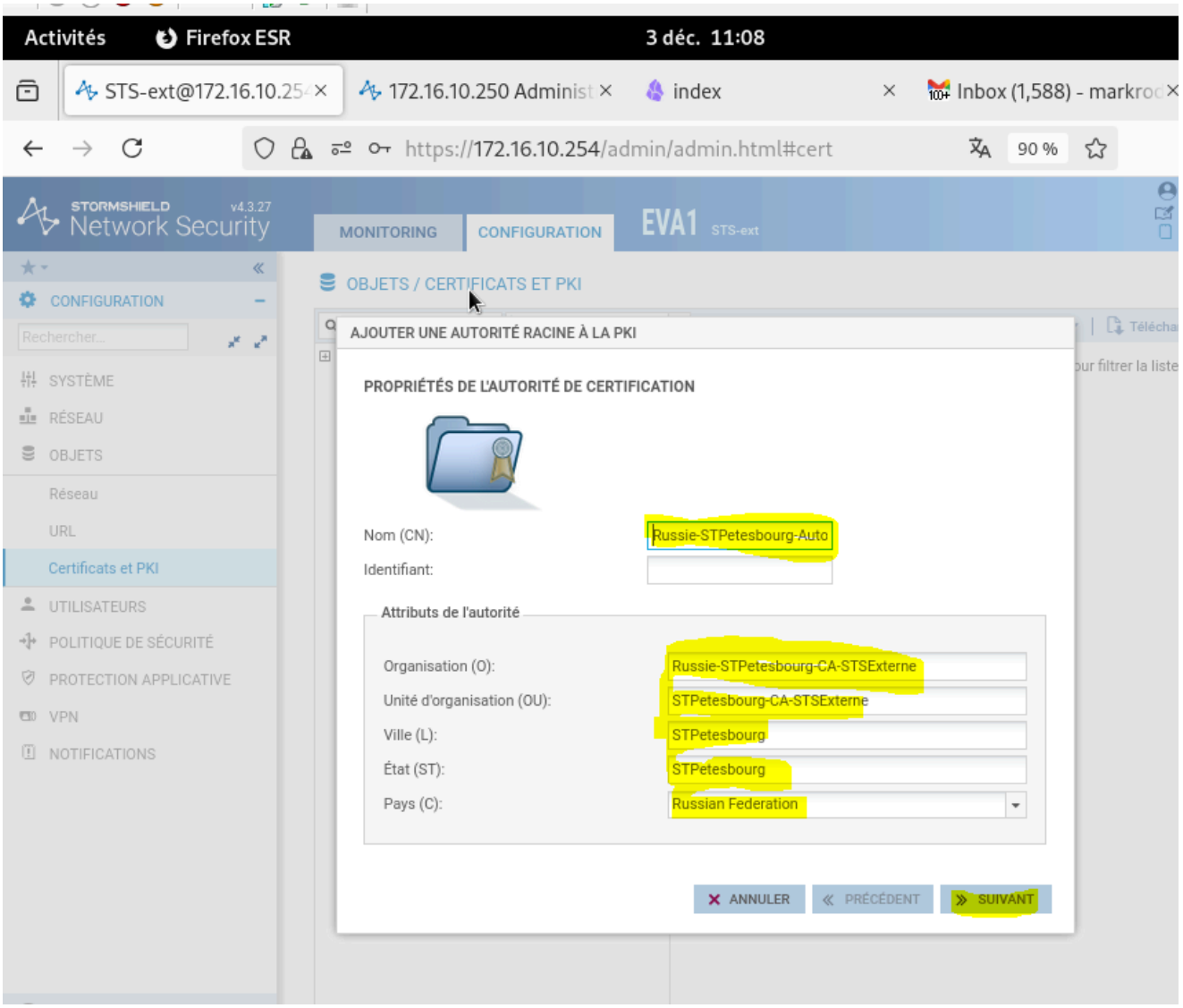
Aspect	PKI	PSK
Type de clé	Asymétrique (publique/privée)	Symétrique (clé partagée)
Authentification	Certificat numérique	Mot de passe partagé
Sécurité	Très élevée	Moyenne (dépend du mot de passe)
Complexité	Mise en place plus complexe	Très simple
Usage courant	HTTPS, emails, VPN pro	Wi-Fi, VPN perso

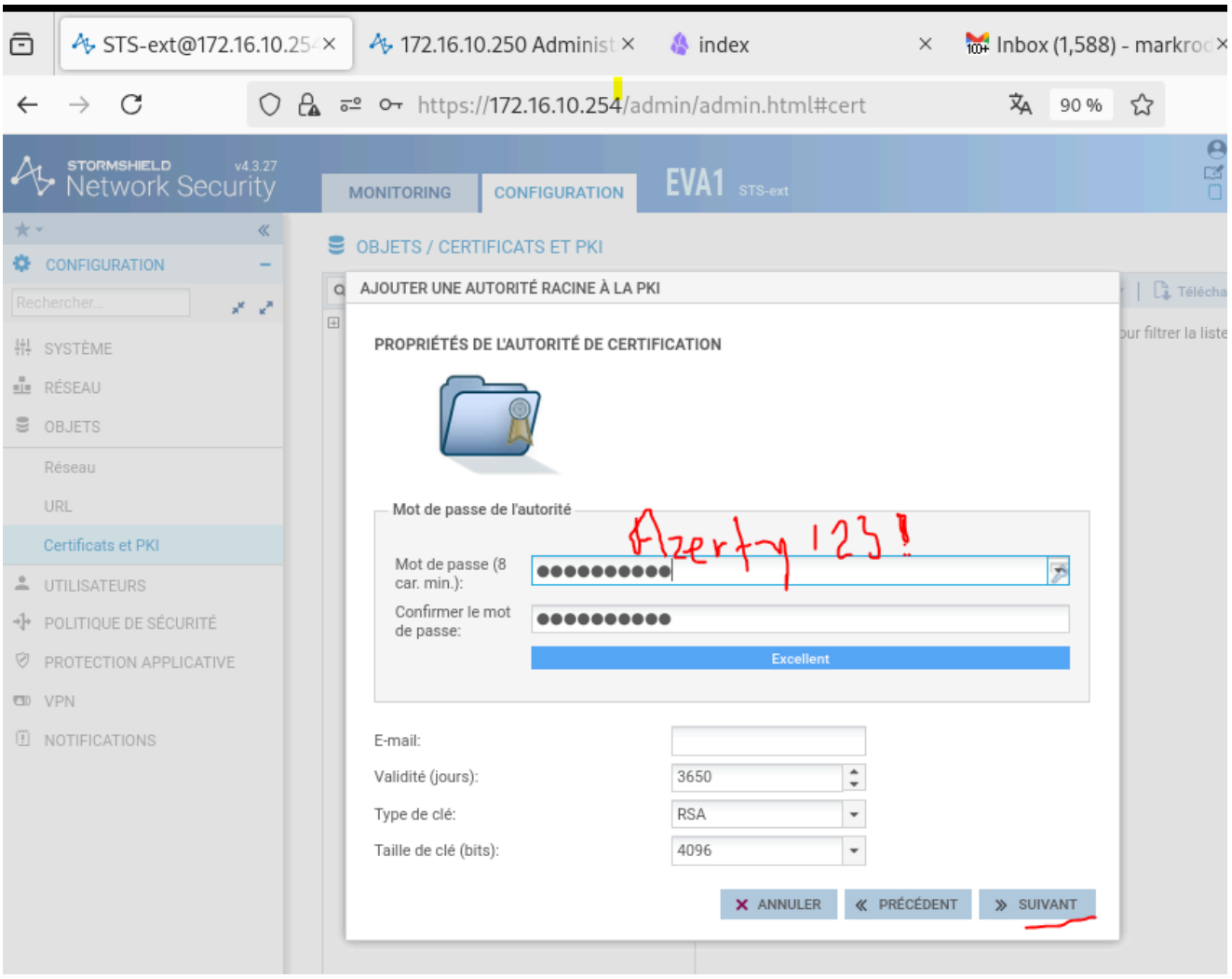
Creation Autorité racine

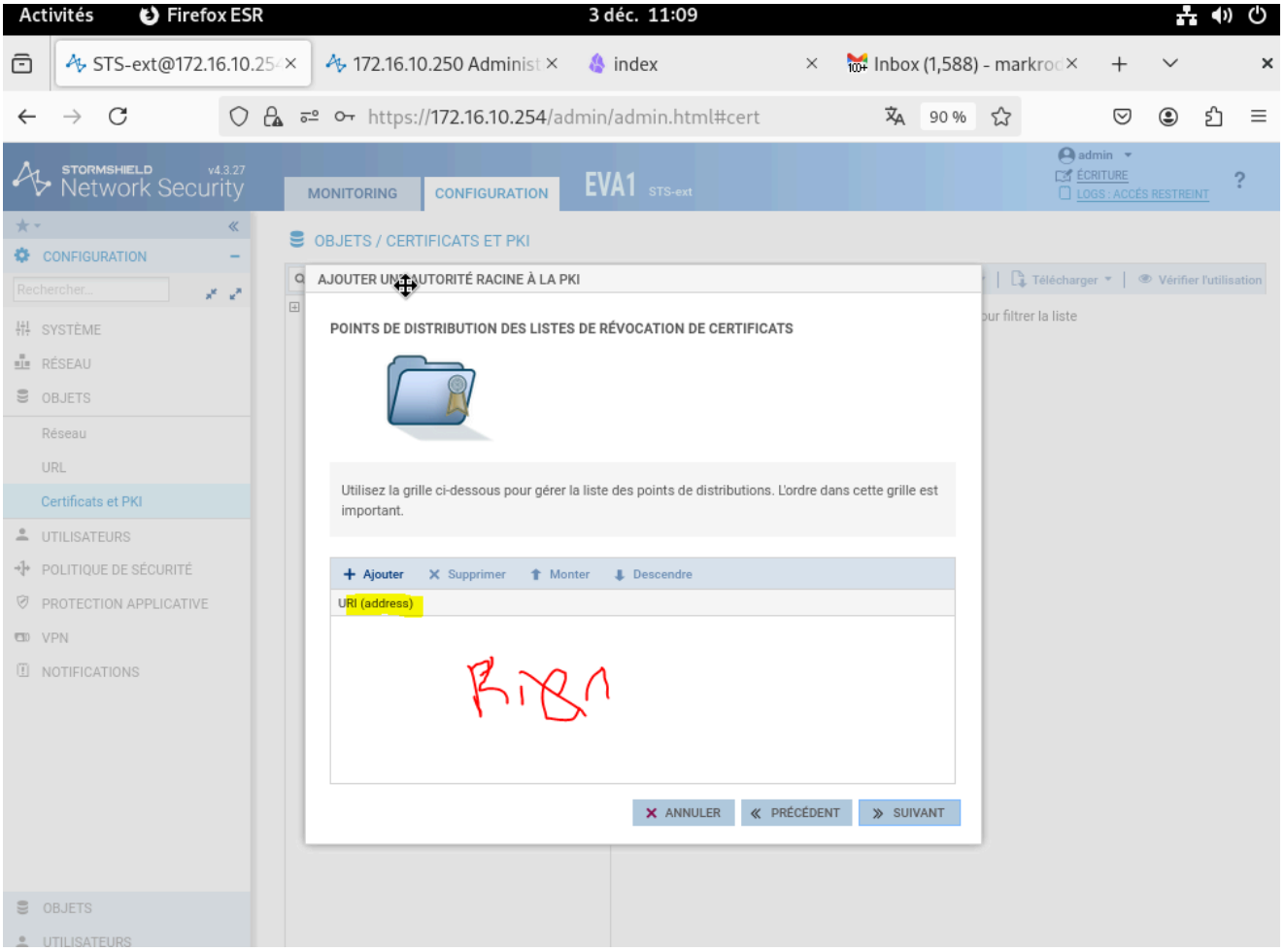


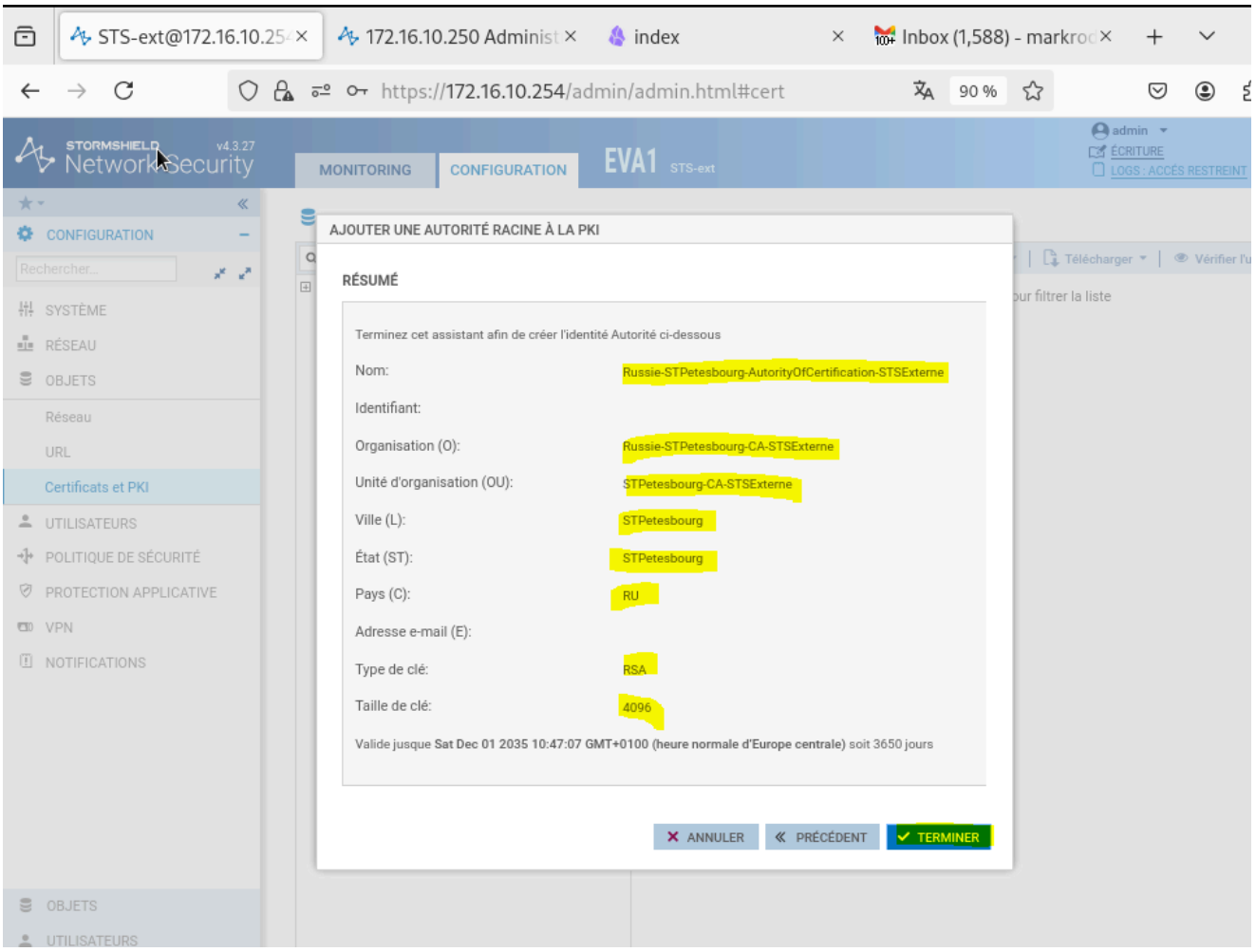
En nom CN, l'autorité de Certification aura comme nom,
Autorité de Certification : Russia-Moscou-AutorityOfCertification-StSExt
identifiant : (non rempli)
Ensuite on passe au nom de l'organisation,
Nom de l'organisation : Russie-STPetesbourg-CA-STSExterne
Unité d'organisation : STPetesbourg-CA-STSExterne
Lieu : STPetesbourg
Etat : STPetesbourg
Pays : Russian Federation

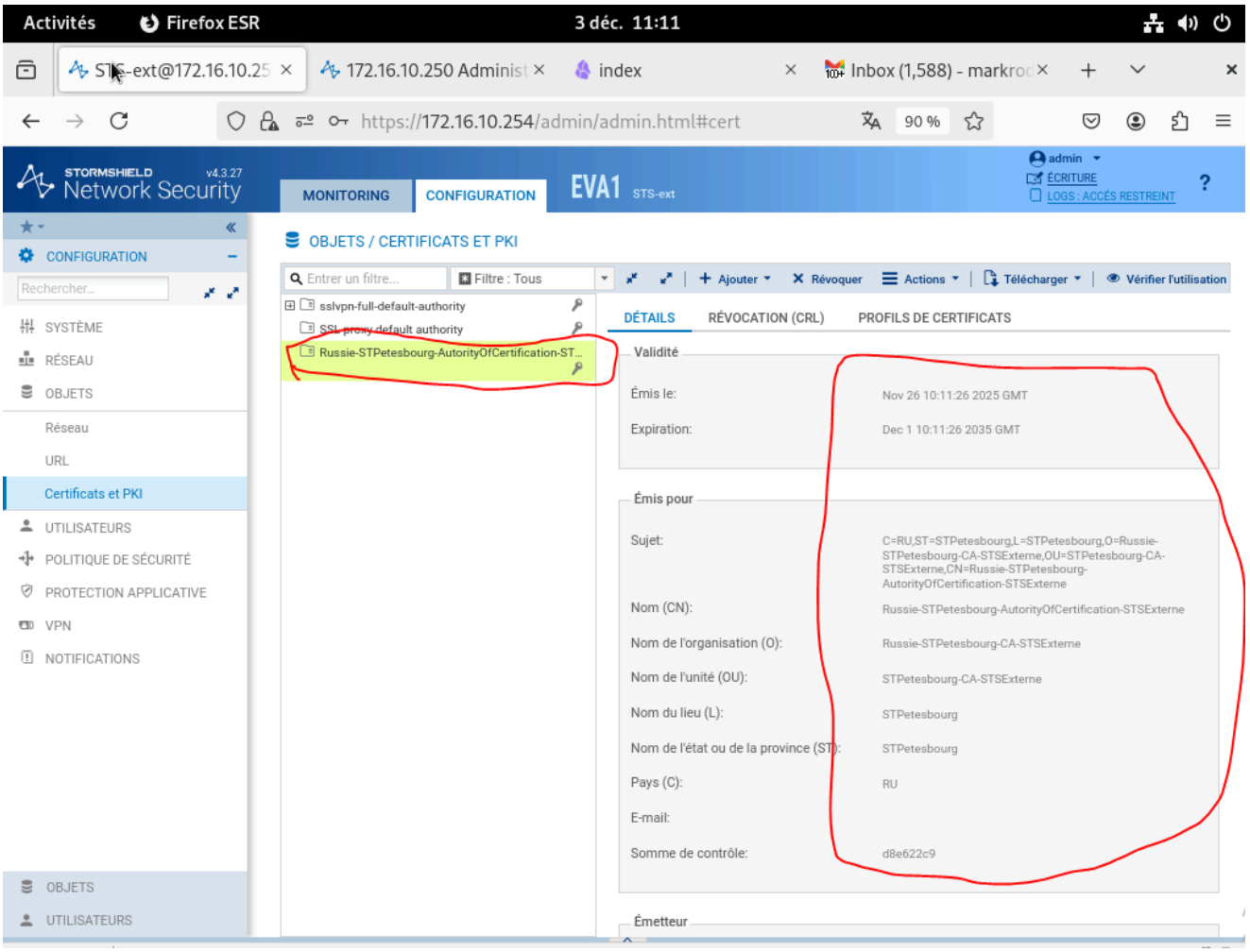
Ce que cela rend sur le Stormshield Externe




STS-ext@172.16.10.25
172.16.10.250 Administ
index
Inbox (1,588) - markroc
https://172.16.10.254/admin/admin.html#cert
90 %
STORMSHIELD
Network Security
v4.3.27
MONITORING
CONFIGURATION
EVA1
STS-ext
OBJETS / CERTIFICATS ET PKI
CONFIGURATION
SYSTÈME
RÉSEAU
OBJETS
Réseau
URL
Certificats et PKI
UTILISATEURS
POLITIQUE DE SÉCURITÉ
PROTECTION APPLICATIVE
VPN
NOTIFICATIONS
AJOUTER UNE AUTORITÉ RACINE À LA PKI
PROPRIÉTÉS DE L'AUTORITÉ DE CERTIFICATION
Mot de passe de l'autorité
Mot de passe (8 car. min.):
Confirmer le mot de passe:
Excellent
E-mail:
Validité (jours):
3650
Type de clé:
RSA
Taille de clé (bits):
4096
ANNULER
PRÉCÉDENT
SUIVANT


Activités
Firefox ESR
3 déc. 11:09
STS-ext@172.16.10.25
172.16.10.250 Administ
index
Inbox (1,588) - markroc
https://172.16.10.254/admin/admin.html#cert
90 %
STORMSHIELD
Network Security
v4.3.27
MONITORING
CONFIGURATION
EVA1
STS-ext
admin
ÉCRITURE
LOGS : ACCÈS RESTREINT
OBJETS / CERTIFICATS ET PKI
AJOUTER UNE AUTORITÉ RACINE À LA PKI
POINTS DE DISTRIBUTION DES LISTES DE RÉVOCATION DE CERTIFICATS
Utilisez la grille ci-dessous pour gérer la liste des points de distributions. L'ordre dans cette grille est important.
Ajouter
Supprimer
Monter
Descendre
URI (address)
ANNULER
PRÉCÉDENT
SUIVANT


STS-ext@172.16.10.25
172.16.10.250 Administ
index
Inbox (1,588) - markroc
https://172.16.10.254/admin/admin.html#cert
90 %
STORMSHIELD
Network Security
v4.3.27
MONITORING
CONFIGURATION
EVA1
STS-ext
admin
ÉCRITURE
LOGS : ACCÈS RESTREINT
CONFIGURATION
Rechercher...
SYSTÈME
RÉSEAU
OBJETS
Réseau
URL
Certificats et PKI
UTILISATEURS
POLITIQUE DE SÉCURITÉ
PROTECTION APPLICATIVE
VPN
NOTIFICATIONS
OBJETS
UTILISATEURS
Télécharger
Vérifier l'u
our filtrer la liste
AJOUTER UNE AUTORITÉ RACINE À LA PKI
RÉSUMÉ
Terminez cet assistant afin de créer l'identité Autorité ci-dessous
Nom: Russie-STPetesbourg-AutorityOfCertification-STSExterne
Identifiant:
Organisation (O): Russie-STPetesbourg-CA-STSExterne
Unité d'organisation (OU): STPetesbourg-CA-STSExterne
Ville (L): STPetesbourg
État (ST): STPetesbourg
Pays (C): RU
Adresse e-mail (E):
Type de clé: RSA
Taille de clé: 4096
Valide jusque Sat Dec 01 2035 10:47:07 GMT+0100 (heure normale d'Europe centrale) soit 3650 jours
ANNULER
PRÉCÉDENT
TERMINER


Activités
Firefox ESR
3 déc. 11:11
STS-ext@172.16.10.25
172.16.10.250 Administ
index
Inbox (1,588) - markroc
https://172.16.10.254/admin/admin.html#cert
90 %
STORMSHIELD
Network Security
v4.3.27
MONITORING
CONFIGURATION
EVA1
STS-ext
admin
ÉCRITURE
LOGS : ACCÈS RESTREINT
CONFIGURATION
Rechercher...
SYSTÈME
RÉSEAU
OBJETS
Réseau
URL
Certificats et PKI
UTILISATEURS
POLITIQUE DE SÉCURITÉ
PROTECTION APPLICATIVE
VPN
NOTIFICATIONS
OBJETS
UTILISATEURS
OBJETS / CERTIFICATS ET PKI
Entrer un filtre...
Filtre : Tous
Ajouter
Révoquer
Actions
Télécharger
Vérifier l'utilisation
sslvpn-full-default-authority
SSL proxy default authority
Russie-STPetesbourg-AutorityOfCertification-ST...
DÉTAILS
RÉVOCATION (CRL)
PROFILS DE CERTIFICATS
Validité
Émis le:
Nov 26 10:11:26 2025 GMT
Expiration:
Dec 1 10:11:26 2035 GMT
Émis pour
Sujet:
C=RU,ST=STPetesbourg,L=STPetesbourg,O=Russie-STPetesbourg-CA-STSExterne,OU=STPetesbourg-CA-STSExterne,CN=Russie-STPetesbourg-AutorityOfCertification-STSExterne
Nom (CN):
Russie-STPetesbourg-AutorityOfCertification-STSExterne
Nom de l'organisation (O):
Russie-STPetesbourg-CA-STSExterne
Nom de l'unité (OU):
STPetesbourg-CA-STSExterne
Nom du lieu (L):
STPetesbourg
Nom de l'état ou de la province (ST):
STPetesbourg
Pays (C):
RU
E-mail:
Somme de contrôle:
d8e622c9
Émetteur