



[Date]

# Infrastructure à clés publiques (PKI) - Identité & Certificat ssh

Stormshield



Mamadou CAMARA  
[NOM DE LA SOCIETE]

## Table des matières

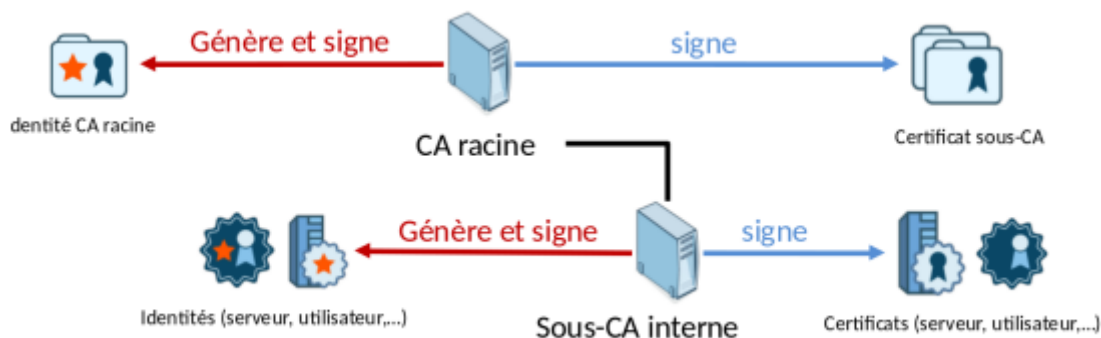
<b>1.Création de l'autorité de certification ca, certificat et autorité utilisateur sur Stormshield .....</b>	<b>2</b>
<b>1.1L'autorité de certification ca .....</b>	<b>2</b>
<b>1.2Identité utilisateur .....</b>	<b>5</b>
<b>2.Gestion des identités et certificats.....</b>	<b>10</b>
<b>2.1 Connexion ssh en utilisant l'identité utilisateur sur un serveur distant.....</b>	<b>11</b>
<b>2.2 Extraction des clés privée et publique du fichier identité de charles .....</b>	<b>11</b>
<b>2.3 Test : .....</b>	<b>16</b>
<b>3.Configuration du client ssh sous Windows .....</b>	<b>17</b>
<b>4.Certificat :.....</b>	<b>18</b>

## 1. Contexte :

Les activités consistent :

- à mettre en oeuvre une **infrastructure à clé publique (PKI)** avec un pare-feu Stormshield ;  
créer et utiliser :
- des **certificats utilisateurs** signés pour s'authentifier sur un serveur Debian distant et pour l'interface d'administration du SNS Stormshield.
- Un certificat racine ca

## 2. Présentation



### CA interne

Cette fonctionnalité de gestion d'une infrastructure à clés publiques permet de répondre à un grand nombre de cas d'usage :

- **Le pare-feu agit en tant qu'autorité de certification racine (root CA) :** le boîtier SNS permet de définir les chaînes de confiance nécessaires à une authentification par certificat. Des autorités par défaut sont disponibles pour signer les certificats utilisés par le proxy SSL ou livrer les certificats nécessaires au fonctionnement du VPN SSL. Son certificat d'autorité est auto-signé. Les fonctions proposées par le boîtier SNS permettent de répondre pleinement au rôle d'autorité de certification (création de certificat de différentes natures, signature de CSR, révocation de certificat et gestion de CRL).

- **Le pare-feu agit en tant que sous-autorité de certification** : il est possible de définir un boîtier SNS comme étant une sous-autorité de certification d'une CA parente (gérée obligatoirement sur le même boîtier). Le certificat de la sous-autorité est signé par l'autorité parente (pas nécessairement une autorité racine), laquelle est une autorité interne ou externe. Cela permet d'organiser plus finement la répartition et la distribution des identités, par usages ou par entités d'une même entreprise.

## 3. Création de l'autorité de certification ca, certificat et autorité utilisateur sur Stormshield

### 3.1 L'autorité de certification ca

Se rendre au menu CONFIGURATION / OBJETS / Certificats et PKI Cliquer sur Ajouter puis sélectionner **Autorité racine**.



Ensuite :

Renseigner un CN (obligatoire) : il s'agit d'un nom permettant d'identifier votre autorité racine, dans la limite de 64 caractères. Ce nom peut faire référence à une organisation, un utilisateur, un serveur, une machine, etc.

Renseigner un Identifiant (facultatif) : vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande.

renseigner les attributs de l'autorité. Ces informations seront présentes dans le certificat de l'autorité ainsi que dans les certificats qu'elle émettra :

- Organisation (O) : nom de votre société.
- Unité d'organisation (OU) : "branche" de votre société.
- Lieu (L) : ville dans laquelle est située votre société
- État ou province (ST) : département géographique de votre société.
- Pays (C) : pays dans laquelle est située votre société Cliquer sur Suivant

## AJOUTER UNE AUTORITÉ RACINE À LA PKI

### PROPRIÉTÉS DE L'AUTORITÉ DE CERTIFICATION



Nom (CN):

Nom (CN)

Identifiant:

#### Attributs de l'autorité

Organisation (O):

Nom de l'organisation (O)

Unité d'organisation (OU):

Nom de l'unité (OU)

Ville (L):

Nom du lieu (L)

État (ST):

Nom de l'état (ST)

Pays (C):

Sélectionner le pays (C)

✕ ANNULER

« PRÉCÉDENT

» SUIVANT

Cliquer sur suivant :

## 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:

Faible

E-mail:

test@kayes.cub.fr

Validité (jours):

3650

Type de clé:

RSA

Taille de clé (bits):

4096

✕ ANNULER

« PRÉCÉDENT

» SUIVANT

Le ca est crée

AJOUTER UNE AUTORITÉ RACINE À LA PKI

RÉSUMÉ

Terminez cet assistant afin de créer l'identité Autorité ci-dessous

Nom:

pki

Identifiant:

pki

Organisation (O):

Test

Unité d'organisation (OU):

Kayes

Ville (L):

Limoges

État (ST):

HT

Pays (C):

FR

Adresse e-mail (E):

test@kayes.cub.fr

Type de clé:

RSA

Taille de clé:

4096

Valide jusqu'à Fri Dec 15 2034 08:25:44 GMT+0100 (heure normale d'Europe centrale) soit 3650 jours

✖ ANNULER

⏪ PRÉCÉDENT

✓ TERMINER

L'autorité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall.

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... Filtre : Tous

Ajouter Révoquer Actions Télécharger Vérifier l'utilisation

sslvpn-full-default-authority

**pkiKayes**

SSL proxy default authority

pkiKayes

DÉTAILS

RÉVOCATION (CRL)

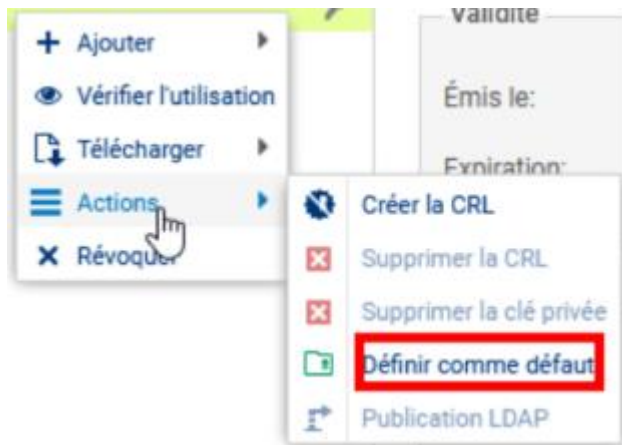
PROFILS DE CERTIFICATS

Validité

Émis le: Dec 2 13:07:58 2024 GMT

Expiration: Dec 7 13:07:58 2034 GMT

- Définir éventuellement par défaut l'autorité de certification :



### 3.2 Identité utilisateur

Première méthode à partir d'un utilisateur créé dans l'annuaire LDAP externe du firewall. Il est possible de générer une identité utilisateur directement depuis l'annuaire LDAP du firewall. Dans ce cas, le choix de l'autorité signataire se porte automatiquement sur la CA désignée par défaut. Se rendre au menu **CONFIGURATION / UTILISATEURS / Utilisateurs** Sélectionner l'utilisateur puis cliquer sur CERTIFICAT puis Créer l'identité

Cliquer sur « Créer l'identité » Le certificat de l'utilisateur s'affiche

scamss (Spin Camss)

COMPTE CERTIFICAT MEMBRE DES GROUPES

Créer l'identité X Supprimer

Validité

Émis le: Dec 16 07:46:55 2024 GMT

Expiration: Dec 17 07:46:55 2025 GMT

Émis pour

Sujet:

/C=FR/ST=Haute-Vienne/L=Limoges/O=KAYES/OU=Kayes/CN=Camss/emailAddress=scamsss@kayes.cub.fr

Nom (CN):

Camss

Nom de l'organisation (O):

KAYES

Nom de l'unité (OU):

Kayes

Nom du lieu (L):

Limoges

Nom de l'état ou de la province (ST):

Haute-Vienne

Pays (C):

FR

E-mail:

scamsss@kayes.cub.fr

Autres informations:

Il est également visible via le menu **OBJETS / CERTIFICATS et PKI**

CONFIGURATION

Rechercher...

SYSTÈME

RÉSEAU

OBJETS

Réseau

URL

Certificats et PKI

UTILISATEURS

Utilisateurs

Comptes temporaires

Droits d'accès

Authentification

Enrôlement

Configuration des annuaires

POLITIQUE DE SÉCURITÉ

PROTECTION APPLICATIVE

VPN

NOTIFICATIONS

OBJETS

UTILISATEURS

OBJETS / CERTIFICATS ET PKI

Entrer un filtre...

Filtre : Tous

+ Ajouter

X Révoquer

Actions

Télécharger

Vérifier l'utilisation

sslvpn-full-default-authority

pkikayes

Camara

charles

miamadou

Mamadou MC. Camara

Cams

parfeu

Martin

Dupond

Camss

SSL proxy default authority

pkikayes

DETAILS

RÉVOCATION (CRL)

PROFILS DE CERTIFICATS

Validité

Émis le: Dec 16 07:46:55 2024 GMT

Expiration: Dec 17 07:46:55 2025 GMT

Émis pour

Sujet:

C=FR,ST=Haute-Vienne,L=Limoges,O=KAYES,OU=Kayes,CN=Camss,emailAddress=scamsss@kayes.cub.fr

Nom (CN):

Camss

Nom de l'organisation (O):

KAYES

Nom de l'unité (OU):

Kayes

Nom du lieu (L):

Limoges

Nom de l'état ou de la province (ST):

Haute-Vienne

Pays (C):

FR

E-mail:

scamsss@kayes.cub.fr

Somme de contrôle:

138eb799

Émetteur

Émetteur:

C=FR,ST=Haute-Vienne,L=Limoges,O=KAYES,OU=Kayes,CN=pkikayes

Nom (CN):

pkikayes

## Deuxième méthode

Se rendre au menu **CONFIGURATION / OBJETS / Certificats et PKI** Cliquer sur **+Ajouter** puis Identité Utilisateur.

Renseigner : un CN (obligatoire) : nom permettant d'identifier l'utilisateur dans la limite de 64 caractères. 2. un Identifiant (facultatif) : vous pouvez ici indiquer un



raccourci de votre CN, utile pour vos lignes de commande (exemple : si le CN est un couple Prénom+Nom, l'identifiant peut correspondre aux initiales du CN).

l'adresse e-mail (obligatoire) de l'utilisateur pour lequel vous créez une identité.  
Cliquer sur Suivant.

#### CRÉER UNE IDENTITÉ UTILISATEUR

##### OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Nom (CN):

Nom (CN)

Identifiant:

E-mail:

✕ ANNULER

« PRÉCÉDENT

» SUIVANT

Sélectionner l'Autorité parente destinée à signer le certificat de l'identité.

Renseigner le Mot de passe de l'autorité parente.

Les attributs de l'autorité sont automatiquement ajoutés. Ils seront présents dans le certificat utilisateur.

## CRÉER UNE IDENTITÉ UTILISATEUR

### OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



#### Sélectionnez l'autorité parente

Autorité parente:

pkiKayes

Mot de passe de la CA:

.....

#### Attributs de l'autorité

Organisation (O):

KAYES

Unité d'organisation (OU):

Kayes

Ville (L):

Limoges

État (ST):

Haute-Vienne

Pays (C):

France

✕ ANNULER

⏪ PRÉCÉDENT

⏩ SUIVANT

Cliquer sur suivant

Si l'autorité utilisée pour générer le certificat est l'autorité par défaut du firewall ET si un utilisateur déclaré dans l'annuaire LDAP référence la même adresse e-mail que celle précisée à l'étape 3, vous pouvez associer automatiquement cette identité à l'utilisateur correspondant : Cocher la case **Publier cette identité dans l'annuaire LDAP**, Saisissez deux fois un mot de passe destiné à protéger le conteneur PKCS#12 de l'identité. Cliquer sur Suivant

## CRÉER UNE IDENTITÉ UTILISATEUR

### OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Validité (jours):	<input type="text" value="365"/>	▲▼
Type de clé:	<input type="text" value="RSA"/>	▼
Taille de clé (bits):	<input type="text" value="2048"/>	▼

#### Publication dans l'annuaire LDAP

Publier le certificat correspondant dans l'annuaire LDAP: ☐

Mot de passe du conteneur PKCS#12 publié (8 car. min.):

Confirmez le mot de passe:

Robustesse du mot de passe

✖ ANNULER

⏪ PRÉCÉDENT

⏩ SUIVANT

Un résumé des informations saisies vous est présenté. ⇒ Cliquer sur Terminer

## CRÉER UNE IDENTITÉ UTILISATEUR

### RÉSUMÉ

Terminez cet assistant afin de créer l'identité utilisateur ci-dessous

Nom:	cam
Identifiant:	cam
Autorité parente:	pkiKayes
Organisation (O):	KAYES
Unité d'organisation (OU):	Kayes
Ville (L):	Limoges
État (ST):	Haute-Vienne
Pays (C):	FR
Adresse e-mail (E):	cam@kayes.cub.fr
Type de clé:	RSA
Taille de clé:	2048

Cette identité sera publiée dans l'annuaire LDAP

Valide jusque Wed Dec 17 2025 08:58:33 GMT+0100 (heure normale d'Europe centrale) soit 365 jours

✕ ANNULER

⏪ PRÉCÉDENT

✓ TERMINER

L'identité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall, sous son autorité parente.

## 4. Gestion des identités et certificats

### 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).

## 2.1 Connexion ssh en utilisant l'identité utilisateur sur un serveur distant

- Télécharger l'identité utilisateur créée sur Stormshiel au format p12 :
- Puisque l'identité contient une clé privée qui est sensible et son export doit être protégé par un mot de passe, lequel permet de chiffrer la clé privée qu'il contient.
- Indiquer le mot de passe :

ENTREZ UN MOT DE PASSE POUR PROTÉGER LE CERTIFICAT CHARLES

Entrez le mot de passe:

Confirmer:

Robustesse du mot de passe

 Télécharger le certificat (P12)  Annuler

- 
- Ensuite téléchargé l'identité :

## 2.2 Extraction des clés privée et publique du fichier identité de charles

Avec la commande **ssh-keygen -f /fichieridentité**

```

PS C:\Users\camar\Downloads> ssh-keygen -f .\identité_charles.pem
Generating public/private ed25519 key pair.
.\identité_charles.pem already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in .\identité_charles.pem
Your public key has been saved in .\identité_charles.pem.pub
The key fingerprint is:
SHA256:c8bDsoXLZ59Eji1238suZ9X06CINijk8qDG9elI10VE camar@Mamadou
The key's randomart image is:
+--[ED25519 256]--+
|      ..oE      |
|      . .       |
|      . .       |
|      o * =      |
|      . S O * = .|
|      .. B. = o+ |
|      o..o o.. o o++|
|      .oo.* . . o.oo+|
|      o=. o . o*+ |
+----[SHA256]-----+

```

On renomme les clés générées : id\_rsa est la clé privée et id\_rsa.pub est la clé publique

```

+----[SHA256]-----+
PS C:\Users\camar\Downloads> ren .\identité_charles.pem id_rsa
PS C:\Users\camar\Downloads> ren .\identité_charles.pem.pub id_rsa.pub
PS C:\Users\camar\Downloads>

```

On copie la clé publique dans **.ssh/authorized\_key** du client windows

```

+ FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCom
PS C:\Users\camar\Downloads> cat id_rsa.pub >> ~/.ssh/authorized_key
PS C:\Users\camar\Downloads> |

```

On copie les deux clé publique/Privée dans **.ssh/** du Windows

```

PS C:\Users\camar\Downloads> cp .\id_rsa C:\Users\camar\.ssh\
PS C:\Users\camar\Downloads> cp .\id_rsa.pub C:\Users\camar\.ssh\

```

On copie la clé publique sur le serveur distant

NB : Pour pouvoir se connecter au serveur distant depuis internet, on fait une redirection de port :

- Source : Internet

EDITION DE LA RÈGLE N° 5

Général	<b>SOURCE</b>
Action	
Source	
Destination	
Port / Protocole	
Inspection	

**GÉNÉRAL**   GÉOLOCALISATION / RÉPUTATION   CONFIGURATION AVANCÉE

**Général**

Utilisateur:

Rechercher...

Machines sources:

+ Ajouter

×

Supprimer

internet

Interface d'entrée:

out

✕ ANNULER

✓ OK

- Deestination : l'interface OUT du pare feu

Général	<b>DESTINATION</b>  <b>GÉNÉRAL</b> GÉOLOCALISATION / RÉPUTATION    CONFIGURATION AVANCÉE  Général  Machines destinations: <div><div>+ Ajouter    ✕ Supprimer    ⌵</div><div>Firewall_out</div></div>
Action	
Source	
Destination	
Port / Protocole	
Inspection	

✕ ANNULER

✓ OK

-Dans Configuration avancée, on indique l'adresse ip de notre serveur distant (NAT Destination):



# EDITION DE LA RÈGLE N° 5

Général
Action
Source
Destination
Port / Protocole
Inspection

## DESTINATION

GÉNÉRAL GÉOLOCALISATION / RÉPUTATION CONFIGURATION AVANCÉE

### Configuration avancée

Interface de sortie: Choisissez une interface

### NAT sur la destination

Destination: serv\_priv\_dhcp

☐ Publication ARP sur la destination externe (publique)

✖ ANNULER

✔ OK

- Dans l'onglet Port/Protocole :
- Pour **le Port Destination**, on choisi un port disponible, **ici 8022** pour pouvoir se connecter au serveur via ssh port **22 (port de translation )**

EDITION DE LA RÈGLE N° 5

Général

Action

Source

Destination

Port / Protocole

Inspection

### PORT ET PROTOCOLE

Port

Port destination:

+ Ajouter X Supprimer

ssh\_8022

Protocole

Type de protocole: Détection automatique du protocole (par défaut)

Protocole applicatif: Basé sur les ports par défaut ou le contenu

Protocole IP: Tous

Translation de port

Port destination traduit: ssh

ANNULER

OK

5	on	passer	Internet interface: out	Firewall_out serv_priv_dhcp	ssh_8022 ssh	IPS
---	----	--------	----------------------------	--------------------------------	-----------------	-----

On copie la clé publique sur le serveur distant via la commande :

**Scp -P 8022 fichierIdentite.pub compte@192.168.229.36:/home/compte**

-P : indique le port de destination

```
C:\Users\camar\Downloads>scp -P 8022 id_rsa.pub charles@192.168.229.36:/home/charles/.ssh
charles@192.168.229.36's password:
id_rsa.pub                                100% 96 13.4KB/s 00:00
C:\Users\camar\Downloads>
```

On copie en suite la clé dans authorized\_keys avec la commande

**Cat id\_rsa.pub >> authorized\_keys**

## 2.3 Test :

```
C:\Users\camar\Downloads>ssh charles@192.168.229.36 -p 8022
Enter passphrase for key 'C:\Users\camar\.ssh\id_rsa':
Linux DHCP1 6.5.11-7-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.11-7 (2023-12-05T09:44Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec 12 16:01:00 2024 from 192.168.229.37
charles@DHCP1:~$ |
```

## 5. Configuration du client ssh sous Windows

### Configuration du client SSH

Sur le client LWindows, le fichier `C:\Users\camar\.ssh\config` permet de configurer les **paramètres globaux** du client pour toutes les connexions vers des serveurs **ssh**.

Pour chaque compte utilisateur, une configuration personnalisée se fait créant/modifiant le fichier **config** situé dans le répertoire utilisateur **.ssh** (`C:\Users\[nom_utilisateur]\.ssh\config` sous Windows)

### Exemple :

On crée un fichier **config** dans le dossier **.ssh**, on ajoute les informations suivantes :

#### Host dhcp

**Hostname** 192.168.229.X

**Port** 8022

**User** mamadou

### Explication :

- **Host** : définit un nom pour le serveur ssh
- **Hostname** : adresse IP ou nom DNS du serveur
- **Port** : port ssh si différent du port SSH par défaut 22
- **User** : précise le nom de connexion

### Utilisation :

Pour se connecter au serveur DHCP via ssh, il suffit d'indiquer le nom défini dans le fichier de configuration C:\Users\[nom\_utilisateur]\.ssh\config

```
C:\Users\camar>ssh dhcp
Enter passphrase for key 'C:\Users\camar\.ssh/id_rsa':
Linux DHCP1 6.5.11-7-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.11-7 (2023-12-05T09:44Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec 16 14:09:59 2024 from 192.168.229.37
mamadou@DHCP1:~$ |
```

## 6. Certificat :

On met le ca dans : /usr/local/share/ca-certification

Puis on tape la **commande update-ca-certificates**

```
mamadou@ns0:~$ mv pkiKayes.pem /usr/local/share/ca-certificates/
mv: cannot move 'pkiKayes.pem' to '/usr/local/share/ca-certificates/pkiKayes.pem': Permission denied
mamadou@ns0:~$ sudo mv pkiKayes.pem /usr/local/share/ca-certificates/
[sudo] password for mamadou:
mamadou@ns0:~$ ls
mamadou@ns0:~$ cd /usr/local/share/ca-certificates/
mamadou@ns0:/usr/local/share/ca-certificates$ ls
pkiKayes.pem
mamadou@ns0:/usr/local/share/ca-certificates$ update-ca-certificates
bash: update-ca-certificates: command not found
mamadou@ns0:/usr/local/share/ca-certificates$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
mamadou@ns0:/usr/local/share/ca-certificates$ |
```