

EOLE AD DC - Tâche #37579

Scénario # 37568 (Nouveau): Maquette Sphinx 2.11 démontrant l'implémentation du nouveau modèle strongSwan

certificats parsing

10/08/2026 14:40 - Ludwig Seys

Statut:	Résolu	Début:	01/10/2022
Priorité:	Normal	Echéance:	
Assigné à:	Ludwig Seys	% réalisé:	100%
Version cible:	Carnet Cadoles - MEN	Temps estimé:	0.00 heure
Description			

Révisions associées

Révision 25a0f3ee - 10/08/2026 14:50 - Ludwig Seys

fix: supporte le format OpenSSL CN sans espaces

ref #37579

Révision a21f339e - 10/08/2026 15:02 - Ludwig Seys

fix manque indentation

ref #37579

Révision 83e7ce11 - 11/08/2026 10:41 - Benjamin Bohard

Formatage du champ issuer avec espace ou pas

Ref #37579

Historique

#1 - 10/08/2026 14:40 - Ludwig Seys

- Statut changé de Nouveau à En cours

#2 - 10/08/2026 14:45 - Ludwig Seys

- % réalisé changé de 0 à 80

Problème rencontré

Lors de l'instance du module Sphinx 2.11, le script posttemplate/00-arv échoue pendant l'initialisation de la base ARV.

L'erreur se produit lors de l'ajout de l'autorité de certification locale ARV :

```
Exception: error in add_cred_auth: list index out of range
```

La trace montre que l'échec vient de : `creole.cert.get_subject(cert=credential)` appelé depuis ARV lors du parsing du certificat CA local.

Le problème n'apparaît pas sur les autres modules => Il ne vient pas de la génération du certificat : le certificat ARV est bien présent et lisible par OpenSSL.

Le blocage vient du parsing du subject par `creole.cert.get_subject()`. Ce cas est visible sur Sphinx parce que ARV appelle explicitement cette fonction

pendant son initialisation. Les autres modules peuvent utiliser des certificats sans passer par ce chemin de code précis, donc ils ne déclenchent pas l'erreur.

Cause :

La fonction `creole.cert.get_subject()` attend un ancien format de sortie OpenSSL : `CN = valeur`

Or OpenSSL retourne désormais : `CN=valeur`

Exemple constaté :

```
subject=C=FR, O=Education Nationale, L=Dijon, OU=0002 110043015, CN=CA-sphinx-RVP
```

La regex ne trouve donc aucune correspondance, puis l'accès à `[0]` provoque : `IndexError: list index out of range`

Méthode de reproduction

Sur un Sphinx 2.11 avec ARV initialisé :

```
python3 - <<'PY'
from creole import cert
from arv.config import ssl_dir, ca_conf_file, x509_default_key_bits
from os.path import join

cert.load_conf({
    'ssl_dir': ssl_dir,
    'start_index': "01",
    'ca_conf_file': ca_conf_file,
    'ca_file': join(ssl_dir, 'certs/CaCert.pem'),
    'ssl_default_key_bits': x509_default_key_bits,
    'ssl_default_cert_time': '5475'
})

credential = open(cert.ca_file, 'r').read()
print(cert.get_subject(cert=credential))
PY
```

Avant correction, la commande échoue avec : `IndexError: list index out of range`

On peut confirmer que le certificat est valide avec :

```
openssl x509 -in /var/lib/arv/CA/certs/CaCert.pem -noout -subject -issuer -dates
```

Solution proposée

Corriger `creole.cert.get_subject()` pour accepter les deux formats de sortie OpenSSL :

```
CN = valeur
CN=valeur
```

Correction minimale proposée :

```
regexp_get_subject = re.compile(r'^subject=(.*) (??:\s*CN\s*=\s*|,\s*CN=) (.*?)$')
matches = regexp_get_subject.findall(ret)
if not matches:
    raise Exception(('Invalid certificate subject format: {0}').format(ret))
return matches[0]
```

Après correction, le test retourne correctement :

```
('C=FR, O=Education Nationale, L=Dijon, OU=0002 110043015', 'CA-sphinx-RVP')  
Conclusion
```

Le problème est un bug de compatibilité Creole/OpenSSL dans `creole.cert.get_subject()`.
Il est révélé par Sphinx/ARV car ARV parse explicitement le subject de sa CA locale pendant l'instance.
Ce point est indépendant du portage strongSwan/swanctl.

#3 - 10/08/2026 15:07 - Ludwig Seys

- % réalisé changé de 80 à 100

#4 - 10/08/2026 15:07 - Ludwig Seys

- Statut changé de En cours à À valider

#5 - 21/09/2026 15:28 - Ludwig Seys

- Statut changé de À valider à Résolu