Lasso - Development #33823

Expired certificate prevents tests from running

10 juin 2019 20:56 - Jakub Hrozek

Statut:	Fermé	**Début:**	10 juin 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.6.1		
Patch proposed:	Oui	**Planning:**	Non

Description

Hi,
a certificate used for the tests expired some time ago

```
openssl x509 -in tests/data/metadata/metadata-federation-renater.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1237974697 (0x49c9fea9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = FR, O = RENATER, CN = Certificat de signature des meta donnees de la federatio
n Education-Recherche
        Validity
            Not Before: Mar 25 09:51:37 2009 GMT
            Not After : Mar 23 09:51:37 2019 GMT
        Subject: C = FR, O = RENATER, CN = Certificat de signature des meta donnees de la federati
on Education-Recherche
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (1024 bit)
                Modulus:
                    00:90:57:70:b2:20:ba:89:06:8b:2b:58:48:ea:e0:
                    99:4e:9f:37:ed:43:5c:ae:1e:6a:ab:af:14:63:1a:
                    b3:0b:a1:71:13:c3:e2:d5:ed:4a:cf:02:1b:13:cf:
                    f3:f5:45:32:97:2b:cb:4e:25:7c:f0:37:9a:9c:03:
                    8a:ce:3b:86:cb:e6:2e:a1:89:56:67:d2:ba:f9:03:
                    b0:fc:7e:23:7d:b9:87:85:aa:1b:31:15:f2:47:ed:
                    b6:42:52:8b:c0:f4:40:b2:a4:f7:0b:1e:03:e0:47:
                    ce:80:69:53:a7:b9:b9:69:86:a9:f5:89:81:b6:65:
                    71:4b:98:28:22:04:da:72:ff
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
         4f:4a:d4:4b:91:93:b6:a5:bd:6b:4a:40:bf:43:e3:89:e4:92:
         e9:b5:b7:28:6d:cc:b6:7d:23:0b:57:66:6a:fe:97:f5:f6:e1:
         86:61:4b:d5:74:82:f5:69:c2:53:65:03:df:df:3a:11:65:98:
         2a:13:76:20:d1:e0:84:71:3f:7d:01:af:79:5c:1d:71:54:92:
         b7:ad:35:3a:90:2c:50:5d:7c:b7:1d:2f:1e:a9:1f:4a:17:23:
         ee:6b:5e:ab:9f:46:bf:88:4e:13:c5:35:52:b7:7f:a5:24:5a:
         20:ed:c6:e3:65:fa:fc:bf:c0:95:77:83:92:27:1f:19:91:e1:
         ab:b4
```

This is unfortunate, because the test test13_test_lasso_server_load_metadata fails. A simple workaround is to just pass NULL instead of the cert to the call to lasso_server_load_metadata, but then we lose some test coverage.

And I didn't find any CA that issued the certificate shipped in the tree, so I was wondering if the certificate could be reissued? Or wouldn't it be even better to create some simple CA using e.g. openssl command line utilities so that the certs are always valid?

Révisions associées

Révision 7c075657 - 11 juin 2019 10:10 - Benjamin Dauvergne

tests: use self-generated certificate to sign federation metadata file (#33823)

Generation procedure :

```
openssl genrsa -out rootCA.key 4096
        openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 99999 -out rootCA.crt
        openssl genrsa -out lasso.key 2048
        openssl req -new -sha256 -key lasso.key -subj "/C=FR/CN=Lasso" -out lasso.csr
        openssl x509 -req -in lasso.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out lasso.crt -days
99999 -sha256
        openssl pkcs12 -export -inkey lasso.key -password pass: -in lasso.crt -name lasso -out lasso.pkcs12
        xmlsec1 --sign --output renater.xml --trusted-pem rootCA.crt --pwd "" --pkcs12 lasso.pkcs12 metadata/r
enater-metadata.xml
        xmlsec1 --verify --trusted-pem rootCA.crt metadata/renater-metadata.xml
```

Historique

#1 - 11 juin 2019 10:10 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 11 juin 2019 10:24 - Benjamin Dauvergne

- Fichier 0001-tests-use-self-generated-certificate-to-sign-federat.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

I replaced the certificate by a self-signed rootCA and certificates, the test passes now.

#3 - 11 juin 2019 10:24 - Benjamin Dauvergne

- Statut changé de Solution proposée à Résolu (à déployer)

```
commit 7c075657a4d64f4d8dbcd03521a0694287d5059f
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Jun 11 10:10:42 2019 +0200

    tests: use self-generated certificate to sign federation metadata file (#33823)

    Generation procedure :

            openssl genrsa -out rootCA.key 4096
            openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 99999 -out rootCA.crt
            openssl genrsa -out lasso.key 2048
            openssl req -new -sha256 -key lasso.key -subj "/C=FR/CN=Lasso" -out lasso.csr
            openssl x509 -req -in lasso.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out lasso.crt -d
ays 99999 -sha256
            openssl pkcs12 -export -inkey lasso.key -password pass: -in lasso.crt -name lasso -out lasso.pkcs1
2
            xmlsec1 --sign --output renater.xml --trusted-pem rootCA.crt --pwd "" --pkcs12 lasso.pkcs12 metada
ta/renater-metadata.xml
            xmlsec1 --verify --trusted-pem rootCA.crt metadata/renater-metadata.xml
```

#4 - 11 juin 2019 10:37 - Jakub Hrozek

Thank you, this works

#5 - 03 septembre 2019 13:48 - Benjamin Dauvergne

- Version cible mis à 2.6.1

#6 - 06 septembre 2019 14:40 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Solution déployée

Fichiers

0001-tests-use-self-generated-certificate-to-sign-federat.patch	25,8 ko	11 juin 2019	Benjamin Dauvergne