Instituts thématiques Inserm

Institut national de la santé et de la recherche médicale

Département du Système d'Information
Pôle Infrastructures - Sécurité opérationnelle

NOTE

à l'attention de CPI, RAI, DRSI, DBA

pour information Direction DSI, MSSI, Pôle infrastructures

date 13/03/13 13:45
contexte DSI - Sécurité opérationnelle
objet Procédure de demande de certificat "RENATER/TERENA"
référence SECOP001033V06V.docx

1 Contexte

Renater est membre de Terena, organisme associant les réseaux européens pour le monde de l'éducation et de la recherche, http://www.terena.org/ .

Renater offre, via Terena à ses membres dont l'Inserm, la possibilité d'obtenir gratuitement des certificats numériques pour serveurs reconnus par les navigateurs Internet. Cette offre est ouverte à toutes les structures de l'Inserm.

Cette note explique comment créer une demande de certificat numérique pour serveur afin de le faire signer numériquement par Renater / Terena suivant la procédure démarrée en octobre 2009.

Ce document annule le document précédent : SECOP001033V03V.

2 Prérequis

La demande de certificat se fait à partir de la console Web mise à disposition par Renater : https://certificats.renater.fr/tcs/apply/18003604800015/

.

Vous serez d'abord redirigé vers une page d'authentification :

L’accès à cette console de saisie de demande de certificats est authentifié. L’authentification est réalisée principalement au travers de la fédération d’identité à laquelle l’Inserm adhère ; pour cela il faut posséder un compte utilisateur Inserm (mêmes identifiants que la messagerie @inserm.fr) ; ce qui est le premier choix proposé « **Veuillez sélectionner votre établissement** »

La demande de certificat se fait avec une requête PKCS#10, il est plus que conseillé d’utiliser le logiciel ***openssl***.

3 Périmètre

Des certificats serveurs peuvent être demandés pour les domaines listés ci-dessous :

- ***ansvs.eu, ansvs.fr, ansvs.info, ansvs.net, ansvs.org, ansvs.tv***
- ***avisan.info, avisan.net, avisan.tv, avisan.eu, avisan.fr***
- ***aviesan.fr, aviesan.eu, aviesan.net, aviesan.org, aviesan.com, aviesan.info, aviesan.tv***
- ***hbsl.eu, hbsl.org, hbsl.fr***
- ***inserm.eu, inserm.fr, inserm.info, inserm.jobs, inserm.org, inserm.pro, inserm.tv, inserm.tel***
- ***insermactualites.fr, insermactualites.com, insermactualites.eu, insermactualites.info, insermactualites.net, insermactualites.org***
- ***inserm-actualites.fr, inserm-actualites.com, inserm-actualites.eu, inserm-actualites.info, inserm-actualites.net, inserm-actualites.org***
- ***orpha.net***
- ***orphanet.fr***
- ***orphanet-urgences.fr***
- ***serimedis.com, serimedis.eu, serimedis.info, serimedis.net, serimedis.org, serimedis.fr***

D’autres domaines peuvent être ajoutés sous condition que leurs « whois » indiquent que l’Inserm en est l’organisme propriétaire.

4 Procédure

La procédure a été simplifiée par rapport à la précédente de GlobalSign, les demandeurs ont accès à une console de saisie dans laquelle il dépose La requête PKCS#10 et juste une adresse courriel de demandeur. L’un des trois valideurs désignés par le DSI (Patrick Lerouge, Guillaume Stevens et Julio Martins) valide la requête. Le demandeur reçoit par mail un lien qui fournit le certificat signé ainsi que la chaine de certification à intégrer au serveur.

4.1 Génération de la requête

Pour plus de renseignements on pourra se référer au MAN (man req) ou sur le site original : http://www.openssl.org/docs/apps/req.html

Vous devez utiliser un logiciel permettant de générer une requête PKCS#10. par exemple avec OpenSSL et le keytool JAVA. Nous recommandons l'usage d'OpenSSL.
Ces logiciels demandent de renseigner la valeur de plusieurs attributs pour générer une requête de certificat au format PKCS#10 contenant ces attributs et les valeurs renseignées. Certains attributs sont obligatoires dans la requête, voici leurs valeurs pour une demande qui concerne le serveur « logiciels.inserm.fr », à partir de cet exemple vous remplacerez le Common Name (CN ici nommé *logiciels.inserm.fr*) par le nom pleinement qualifié (FQDN) de votre serveur :

- *C ou Country Name=FR*
- *O ou Organization Name=INST NAT SANTE ET LA RECHERCHE MEDICALE*
- *CN=logiciels.inserm.fr*

Vous pouvez renseigner également les attributs suivants qui sont optionnels (sauf cas particuliers, ils sont inutiles) :

- *OU ou Organization Unit (multivalué)*
- *DC ou Domain Component (multivalué)*
- *L ou Locality (monovalué)*
- *S ou State (monovalué))*
- *emailAddress (monovalué)*

Outre la génération d'un fichier au format PKCS#10 qui servira à créer le certificat, cette génération va produire la clé privée associée sur votre machine, dans un fichier qu'il vous faut donc conserver (pour JAVA keytool la clé privée est contenu dans le keystore).

Avec OpenSSL vous pouvez exécuter la commande suivante dans un terminal, **sur une seule ligne,** pour générer la clé privée et une requête au format PKCS#10 :

- Si vous ne voulez pas protéger la clef privée par un mot de passe (recommandé) :

```
openssl req -newkey rsa:2048 -keyout logiciels.inserm.fr.key \
-nodes  -subj \
"/C=FR/O=INST NAT SANTE ET LA RECHERCHE
MEDICALE/OU=DSI/CN=logiciels.inserm.fr/"
```

- Si vous voulez que cette clef soit protégée par un mot de passe (attention impose de fournir le mot de passe à chaque redémarrage du serveur) :

```
openssl req -newkey rsa:2048 -keyout logiciels.inserm.fr.key \
-subj \
"/C=FR/O=INST NAT SANTE ET LA RECHERCHE MEDICALE/OU=DSI/CN=logiciels.inserm.fr"
```

→Le fichier généré *« logiciels.inserm.fr.key »* contient la clé privée qui sera associée à votre certificat : conservez-le avec tout le soin et la confidentialité requis.
Cette clé privée sera installée sur le serveur à l’endroit adéquat en ayant des droits d’accès strictement réservés au programme qui a besoin de lire cette clé.

→ Attention, faire un copier-coller de ces commandes depuis le fichier PDF que vous lisez actuellement vers un terminal peut donner des résultats imprévisibles. Le mieux est de dactylographier ces commandes dans votre terminal.

Pour certaines applications, il est conseillé d’ajouter le champ *« emailAddress »*, c’est le cas pour ce qui est relatif au courrier électronique, dans de tels cas ajoutez l’attribut *« emailAddress »* dans l’argument *« subj »* de la commande :

```
openssl req -newkey rsa:2048 -keyout logiciels.inserm.fr.key -nodes \
-subj "/C=FR/O=INST NAT SANTE ET LA RECHERCHE MEDICALE\
/OU=DSI/L=Villejuif\
/emailAddress=Resnat.DSI@inserm.fr/CN=logiciels.inserm.fr"
```

Il est impératif dans ce cas d’utiliser des adresses électroniques fonctionnelles, toute adresse personnelle sera refusée.

La requête PKCS#10 (voir ci-dessous) s'affiche sur la sortie standard, entre les lignes `-----BEGIN CERTIFICATE REQUEST-----` et `-----END CERTIFICATE REQUEST-----`.

→Si vous ajoutez l’option « `–out logiciels.inserm.fr.csr` » à votre commande la requête PKCS#10 sera enregistrée dans un fichier, plutôt qu’affichée sur l’écran avec le risque d’un copier-coller oublié.

```
Generating a 2048 bit RSA private key
.....................++++++
...++++++
writing new private key to 'logiciels.inserm.fr.key'
-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBvzCCASgCAQAwfzELMAkGA1UEBhMCRlIxMDAuBgNVBAoTJ0lOU1QgTkFUIFNB
TlRFIEVUIExBIFJFQ0hFUkNIRSBNRURJQ0FMRTEMMAoGA1UECxMDRFNJMRIwEAYD
VQQHEwlWaWxsZWp1aWYxHDAaBgNVBAMTE2xvZ2ljaWVscy5pbnNlcm0uZnIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALoFrmYFvwz2C8hkX2R7YD/ZdUYGUNX0
2JHqjI2SRrzp2VM0vEpA4RM77RpHQ6q1SHryZMNx4StCa9CnLVt/yCyft1A5ZtM/
2TurANBpmG/UyBgDZAxi/D3AHz5GOXPfDk1PzFzG0jRbcqJf0RgpplF5yZXe5JKR
6Wt51k63Qg+/AgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQAEe0//Dbsw2kcfX4W9
xK0CEG/ohhazndoqt12y2hp0fukR1ee+cCTT7NgErhS8Ad+gRsNQxfetkqd9yVTr
CKL4W0YdmKUCXdYPfwF04ESwhvb2bu3meUJcPWR5SidgGfefGQ4XFOULxpgM/cK/
GaiRoRbuL7lLuodfxmH0VAgaVA==
```

```
-----END CERTIFICATE REQUEST-----
```

Les arguments fournis à votre requête peuvent être lus avec la commande

```
openssl req -text –noout
```

à laquelle on fournit la requête entre
`-----BEGIN CERTIFICATE REQUEST-----`
et
`-----END CERTIFICATE REQUEST-----.`
inclus, sous forme de copier-coller au prompt.

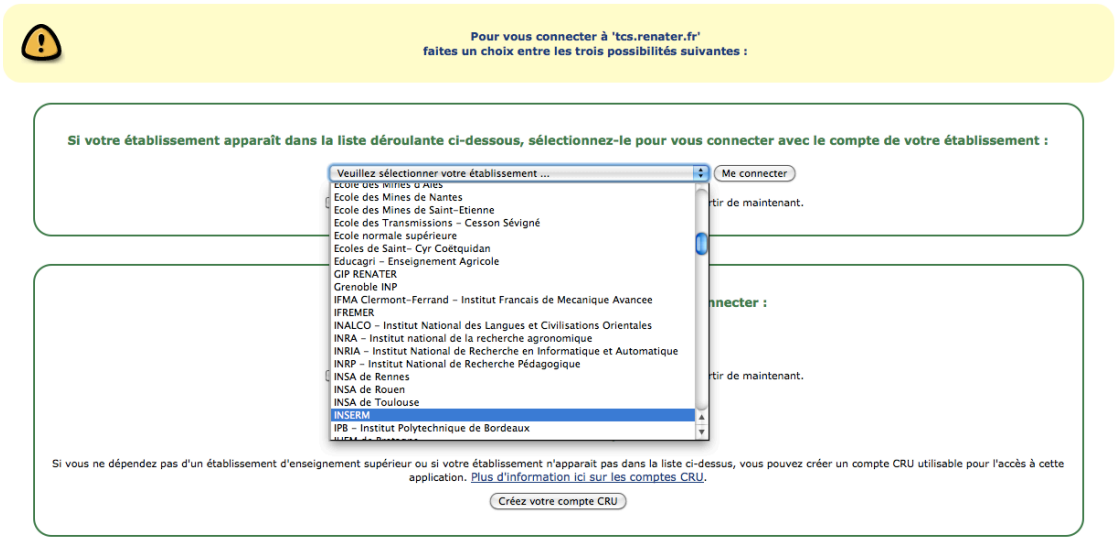
4.2 Soumission de la requête

Connectez vous à l’adresse ci-dessous, vous serez pris en charge par une page d’authentification de la fédération d’identité

https://certificats.renater.fr/tcs/apply/18003604800015/

Le numéro terminant l’adresse est le numéro de SIRET de l’INSERM.

Faites le choix « **Veuillez sélectionner votre établissement …** » puis déroulez la liste et prenez INSERM avant de cliquer « **Me connecter** »



L’utilisation des comptes du CRU n’est pas traitée ici.

Arrivé sur la page d’authentification de l’Inserm indiquez vos identifiants propres à l’Inserm, les mêmes que ceux de votre messagerie électronique :

Si tout ce passe correctement, vous arrivez enfin à la page de soumission, où vous collerez la requête et indiquerez à quelle adresse doit être remis le résultat, dans ce cas indiquez bien votre adresse personnelle :

La page de soumission contient également un lien d'aide à la génération d'une CSR. Le dispositif mis en place par RENATER, contient un workflow qui prévient l’un des trois valideurs possibles, cependant il est conseillé de faire une demande de travaux auprès du point central infrastructures (pci.dsi@inserm.fr) afin que celui qui est disponible puisse vous valider la demande.

Dans le cas le plus optimal, l’obtention d’un certificat signé ne prend pas plus de cinq minutes, cependant cela peut prendre plusieurs jours.

Vous recevrez dans votre messagerie deux courriels de *Terena Certificate Service* :

- Le premier sera reçu après votre demande, il contient dans le sujet *(certificate request)*. Il résume votre commande ;
- Le second sera reçu après validation de notre part, il contient dans le sujet *(certificate issued)*. Il contient l’URL de retrait du certificat :

Vous pouvez récupérer le certificat ainsi que la chaine de certification avec les deux liens PEM format. Votre certificat correspond au premier lien, le deuxième lien est la chaine de certification qui correspond à l’autorité de certification.

Elle peut être vue avec la commande :

```
openssl x509 -noout -text -in FichierDeLaChaineDeCertification
```

qui vous fournit :

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA
Root
        Validity
            Not Before: May 30 10:48:38 2000 GMT
            Not After : May 30 10:48:38 2020 GMT
        Subject: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External
CA Root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b7:f7:1a:33:e6:f2:00:04:2d:39:e0:4e:5b:ed:
                    1f:bc:6c:0f:cd:b5:fa:23:b6:ce:de:9b:11:33:97:
                    a4:29:4c:7d:93:9f:bd:4a:bc:93:ed:03:1a:e3:8f:
                    cf:e5:6d:50:5a:d6:97:29:94:5a:80:b0:49:7a:db:
```

```
                    2e:95:fd:b8:ca:bf:37:38:2d:1e:3e:91:41:ad:70:
                    56:c7:f0:4f:3f:e8:32:9e:74:ca:c8:90:54:e9:c6:
                    5f:0f:78:9d:9a:40:3c:0e:ac:61:aa:5e:14:8f:9e:
                    87:a1:6a:50:dc:d7:9a:4e:af:05:b3:a6:71:94:9c:
                    71:b3:50:60:0a:c7:13:9d:38:07:86:02:a8:e9:a8:
                    69:26:18:90:ab:4c:b0:4f:23:ab:3a:4f:84:d8:df:
                    ce:9f:e1:69:6f:bb:d7:42:d7:6b:44:e4:c7:ad:ee:
                    6d:41:5f:72:5a:71:08:37:b3:79:65:a4:59:a0:94:
                    37:f7:00:2f:0d:c2:92:72:da:d0:38:72:db:14:a8:
                    45:c4:5d:2a:7d:b7:b4:d6:c4:ee:ac:cd:13:44:b7:
                    c9:2b:dd:43:00:25:fa:61:b9:69:6a:58:23:11:b7:
                    a7:33:8f:56:75:59:f5:cd:29:d7:46:b7:0a:2b:65:
                    b6:d3:42:6f:15:b2:b8:7b:fb:ef:e9:5d:53:d5:34:
                    5a:27
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                AD:BD:98:7A:34:B4:26:F7:FA:C4:26:54:EF:03:BD:E0:24:CB:54:1A
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:
                keyid:AD:BD:98:7A:34:B4:26:F7:FA:C4:26:54:EF:03:BD:E0:24:CB:54:1A
                DirName:/C=SE/O=AddTrust   AB/OU=AddTrust   External   TTP   Network/CN=AddTrust
External CA Root
                serial:01

    Signature Algorithm: sha1WithRSAEncryption
        b0:9b:e0:85:25:c2:d6:23:e2:0f:96:06:92:9d:41:98:9c:d9:
        84:79:81:d9:1e:5b:14:07:23:36:65:8f:b0:d8:77:bb:ac:41:
        6c:47:60:83:51:b0:f9:32:3d:e7:fc:f6:26:13:c7:80:16:a5:
        bf:5a:fc:87:cf:78:79:89:21:9a:e2:4c:07:0a:86:35:bc:f2:
        de:51:c4:d2:96:b7:dc:7e:4e:ee:70:fd:1c:39:eb:0c:02:51:
        14:2d:8e:bd:16:e0:c1:df:46:75:e7:24:ad:ec:f4:42:b4:85:
        93:70:10:67:ba:9d:06:35:4a:18:d3:2b:7a:cc:51:42:a1:7a:
        63:d1:e6:bb:a1:c5:2b:c2:36:be:13:0d:e6:bd:63:7e:79:7b:
        a7:09:0d:40:ab:6a:dd:8f:8a:c3:f6:f6:8c:1a:42:05:51:d4:
        45:f5:9f:a7:62:21:68:15:20:43:3c:99:e7:7c:bd:24:d8:a9:
        91:17:73:88:3f:56:1b:31:38:18:b4:71:0f:9a:cd:c8:0e:9e:
        8e:2e:1b:e1:8c:98:83:cb:1f:31:f1:44:4c:c6:04:73:49:76:
        60:0f:c7:f8:bd:17:80:6b:2e:e9:cc:4c:0e:5a:9a:79:0f:20:
        0a:2e:d5:9e:63:26:1e:55:92:94:d8:82:17:5a:7b:d0:bc:c7:
        8f:4e:86:04
```