INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Département Sécurité et Technologies Informatiques

Cryptograhie – TD5

Jérémy Briffaut <jeremy.briffaut@insa-cvl.fr>

Jean-Christophe Deneuville <jean-christophe.deneuville@insa-cvl.fr>

Lundi 22 octobre 2018

Mise en place d'une PKI sur des postes LINUX, Fedora core 8.

Table des matières

1 Accès au VMs

Dans ce TD, nous utiliserons 2 machines virtuelles à l'aide de VMWare®. Pour vous y connecter :

— Administrateur : login "root", password "azerty",

— Utilisateur : login "user", password "user".

Ces deux VMs sont sous Fedora 8.

2 Généralités

Les certificats X.509 sont à la base d'une technique normalisée largement utilisée sur Internet. IPSec va permettre de sécuriser toutes ou une partie des connexions entre deux noeuds du réseau par création de SA (Security Association).

Les certificats créés reposent sur un procédé cryptographique à clés publiques (RSA) afin de garantir la sécurité de la transmission des données sur Internet.

Utilisez VMWare® et l'image `fedora_briffaut.zip` fournie. Créez une machine appelée FEDORA1, puis en clonant cette image mettre en place une machine virtuelle appelée FEDORA2.

Enfin, en clonant l'image VMWare FEDORA1, créez une machine virtuelle que l'on appellera "Centre Certificateur". Démarrez cette machine.

Nous utiliserons OpenSSL pour créer un centre de certification, en générant une clé RSA de 1024 bits, comprenant une clé publique (pour le chiffrement) et une clé privée (pour le déchiffrement). Puis, toujours en utilisant OpennSSL, nous générerons un couple de clés RSA sur chacune des deux machines qui communiqueront en IPSec.

Enfin nous signerons, sous la forme de certicats X.509, les deux clés publiques de FEDORA1 et FEDORA2. Ces certicats seront échangés lors de la connexion IPSec.

3 Transformez la machine "Centre certificateur" en centre de certification

3.1 Visualisation des fichiers

Visualisez le contenu du fichier `/etc/pki/tls/openssl.cnf`. Vérifier en particulier que la taille de la clé RSA (dans le paragraphe `[req]`, valeur de `default_bits`) est bien 1024 bits. À quoi correspond le champ `default_days` ? Assurez-vous que celui-ci est bien à 365.

Visualisez le contenu du script `/etc/pki/tls/misc/CA`. Ce script permettra de rentrer les lignes de commandes OpenSSL.

3.2 Création de l'autorité de certification

Dès à présent, connectez-vous en tant que **root** sur la machine "centre certificateur".

Placez-vous **impérativement** dans le répertoire `/etc/pki/tls`.

Exécutez la commande suivante : `misc/CA --newca`

Vous obtiendrez un affichage similaire.

```
CA certificate filename (or enter to create) (Appuyez sur entrer)
Making CA certificate ...
Generating a 1024 bit RSA private key Génération de la clé RSA sur 1024 bits
.................+++
.....................+++
writing new private key to '/etc/CA/private/cakey.pem' [a]
Enter PEM pass phrase: [b]
Verifying password  Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: FR Code du pays
State or Province Name (full name) [Berkshire]: Centre Région
Locality Name (eg, city) [Newbury]: Bourges
Organization Name (eg, company) [My Company Ltd]: INSA-CVL
Organizational Unit Name (eg, section) []: 4A-STI
Common Name (your server's hostname) []: votre_nom_centre_certificateur
Email Address []: prenom.nom@insa-cvl.fr Adresse mail du contact
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ../../CA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 0 (0x0)
    Validity
        Not Before: Nov 25 19:15:18 2007 GMT
        Not After : Nov 24 19:15:18 2010 GMT
Subject:         countryName = FR
        stateOrProvinceName = Centre
        organizationName = INSA-CVL
        organizationalUnitName = 4A-STI
        commonName = votre_nom_centre_certificateur
        emailAddress = prenom.nom@insa-cvl.fr
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            F0:AF:91:8D:14:4E:77:6C:64:F0:5F:AF:97:4B:F5:F3:9B:F3:31:D8
        X509v3 Authority Key Identifier:
            keyid:F0:AF:91:8D:14:4E:77:6C:64:F0:5F:AF:97:4B:F5:F3:9B:F3:31:D8
Certificate is to be certified until Nov 24 19:15:18 2010 GMT (1095 days)
Write out database with 1 new entries
Data Base Updated
```

a. Donc la clé privée du centre certificateur sera dans le fichier `/etc/CA/private/cakey.pem` et le certificat du centre serveur sera dans `/etc/CA/cacert.pem`

b. Ce mot de passe sera demandé pour la création de tout certificat ! Utilisez votre nom de famille comme mot de passe.

Félicitations, vous venez de créer votre centre de certification.

La clé privée du centre certificateur `votre_nom_centre_certificateur` est dans le fichier `/etc/CA/private/cakey.pem`.

Le certificat du centre serveur est dans `/etc/CA/cacert.pem`.

4 Création d'une paire de clés RSA pour IPSec pour Fedora 1

4.1 Création de la paire de clés pour Fedora 1

Sur la machine virtuelle Fedora 1, dans une session `root` :

— Placez-vous dans le répertoire `/etc/pki/tls`

— Créez les clés de l'hôte : `openssl req -new -nodes -keyout fed1_private.pem -out fed1_request.pem -days 365`

Remarques :

— Cette commande va créer deux fichiers `fed1_private.pem` et `fed1_request.pem`, contenant respectivement les clés privée et publique (clé qui devra être signée par l'AC) de Fedora 1.

— L'option `nodes` est obligatoire, elle permet de ne pas chiffrer la clé privée avec une "passphrase" et qui ne permettrait pas à racoon (programme d'échange de clés de IPSec) de l'utiliser.

Visualisez le contenu de `fed1_private.pem` et `fed1_request.pem`. Copiez la clé privée `fed1_private.pem` dans `/etc/racoon/certs` où racoon viendra la chercher.

```
[root@localhost tls]# openssl req -new -nodes -keyout fed1_private.pem -out
fed1_request.pem -days 365
Generating a 1024 bit RSA private key
............++++++
..................++++++
writing new private key to 'fed1_private.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: FR
State or Province Name (full name) [Berkshire]: Centre
Locality Name (eg, city) [Newbury]: Bourges
Organization Name (eg, company) [My Company Ltd]: INSA-CVL
Organizational Unit Name (eg, section) []: 4A-STI
Common Name (eg, your name or your server's hostname) []: Fedora 1
Email Address []: jeremy.briffaut@insa-cvl.fr
Please enter the following 'extra' attributes to be sent with your certificate
request
A challenge password []:
An optional company name []:
```

4.2 Signature de la clé publique de Fedora 1 par le centre de certification

— Envoyez la clé publique à signer au centre certificateur : Passez le fichier `fed1_request.pem` au centre certificateur par `scp`.
— Sur le centre certificateur, obtenez son adresse IP (eth0) `/sbin/ifconfig`
— Sur fedora transférez la demande de certificat :
`scp fed1_request.pem root@IPCENTRECERTIFICATEUR:/root/`
— Sur la machine virtuelle centre certificateur, copiez le fichier `fed1_request.pem` dans le répertoire `/etc/pki/tls` en le renommant `newreq.pem` : `cp /root/fed1_request.pem /etc/pki/tls/newreq.pem`

Signature de la clé :
— Placez-vous dans `/etc/pki/tls`,
— Saisissez la ligne de commande : `misc/CA -sign`,
— Répondez aux questions.

```
[root@localhost tls]# misc/CA -sign
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ../../CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
        Not Before: Nov 25 19:46:46 2007 GMT
        Not After : Nov 24 19:46:46 2008 GMT
        Subject:
        countryName = FR
        stateOrProvinceName = CENTRE
        localityName = BOURGES
        organizationName = INSA-CVL
        organizationalUnitName = 4A-STI
        commonName = ipsec.fedora1
        emailAddress = jeremy.briffaut@insa-cvl.fr
        X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            7A:F7:1C:7B:C6:88:68:6B:CF:09:43:FC:0B:0B:CB:92:A1:5E:59:80
        X509v3 Authority Key Identifier:
            keyid:F0:AF:91:8D:14:4E:77:6C:64:F0:5F:AF:97:4B:F5:F3:9B:F3:31:D8
Certificate is to be certified until Nov 24 19:46:46 2008 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, ST=Centre, O=INSA-CVL, OU=4A-STI,
CN=briffaut_centre_certificateur/emailAddress=jeremy.briffaut@insa-cvl.fr
```

```
        Validity
            Not Before: Nov 25 19:46:46 2007 GMT
            Not After : Nov 24 19:46:46 2008 GMT
        Subject: C=FR, ST=CENTRE, L=BOURGES, O=INSA-CVL, OU=4A-STI,
CN=ipsec.fedora1/emailAddress=jeremy.briffaut@insa-cvl.fr
        Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:c1:02:f7:f5:0a:84:d0:c5:a6:67:cc:f9:b6:0e:
                f9:a5:21:9a:96:be:7a:c0:d0:c9:b3:64:92:5b:15:
                26:b8:a0:d9:c1:47:47:f1:a6:b0:c9:dc:41:fb:af:
                7f:9d:bb:1a:b7:ae:f9:e9:78:24:53:04:55:9b:87:
                f3:ed:22:15:2b:45:aa:e4:27:ec:1f:09:41:6d:e6:
                23:cd:d7:f3:a4:81:ce:7f:67:a3:91:44:82:64:fc:
                0a:c8:48:92:b2:3d:89:e0:fd:6e:29:da:5d:de:fd:
                83:2a:88:5d:d1:aa:6d:92:78:37:7d:23:93:0d:fc:
                52:f2:c0:af:89:02:ba:5b:81
            Exponent: 65537 (0x10001)
        X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            7A:F7:1C:7B:C6:88:68:6B:CF:09:43:FC:0B:0B:CB:92:A1:5E:59:80
        X509v3 Authority Key Identifier:
            keyid:F0:AF:91:8D:14:4E:77:6C:64:F0:5F:AF:97:4B:F5:F3:9B:F3:31:D8
    Signature Algorithm: sha1WithRSAEncryption
        a9:26:c9:80:d8:88:c6:02:50:1f:34:f9:35:34:3b:09:ef:18:
        5f:58:11:c8:2c:05:8d:3e:1b:ae:b1:48:13:a0:72:46:3a:a1:
        7f:c7:77:50:6a:f2:71:98:50:d3:b1:43:4c:8c:8a:15:94:fb:
        b7:76:ac:59:e2:2a:aa:d5:be:10:2e:81:fd:74:c7:46:28:a8:
        b4:6e:60:67:44:93:27:fa:a6:58:a9:a5:2f:23:f4:42:62:e2:
        f8:28:ee:9c:d8:50:04:c8:b7:2f:a3:e3:65:e1:f3:55:f7:c6:
        a9:31:56:0f:8f:cb:6b:e3:cf:f8:11:26:b3:16:f7:ce:8c:2e:
        59:5b
BEGIN CERTIFICATE
MIIDITCCAoqgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBljELMAkGA1UEBhMCRlIx
DzANBgNVBAgTBkNlbnRyZTEOMAwGA1UEChMFRU5TSUIxDjAMBgNVBAsTBVNUSTJB
MSYwJAYDVQQDDB1icmlmZmF1dF9jZW50cmVfY2VydGlmaWNhdGV1cjEuMCwGCSqG
SIb3DQEJARYfamVyZW15LmJyaWZmYXV0QGVuc2ktYm91cmdlcy5mcjAeFw0wNzEx
MjUxOTQ2NDZaFw0wODExMjQxOTQ2NDZaMIGYMQswCQYDVQQGEwJGUjEPMA0GA1UE
CBMGQ0VOVFJFMRAwDgYDVQQHEwdCT1VSR0VTMQ4wDAYDVQQKEwVFTlNJQjEOMAwG
A1UECxMFU1RJMkExFjAUBgNVBAMTDWlwc2VjLmZlZG9yYTExLjAsBgkqhkiG9w0B
CQEWH2plcmVteS5icmlmZmF1dEBlbnNpLWJvdXJnZXMuZnIwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAMEC9/UKhNDFpmfM+bYO+aUhmpa+esDQybNkklsVJrig
2cFHR/GmsMncQfuvf527Greu+el4JFMEVZuH8+0iFStFquQn7B8JQW3mI83X86SB
zn9no5FEgmT8CshIkrI9ieD9binaXd79gyqIXdGqbZJ4N30jkw38UvLAr4kCuluB
AgMBAAGjezB5MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2Vu
ZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBR69xx7xohoa88JQ/wLC8uSoV5Z
gDAfBgNVHSMEGDAWgBTwr5GNFE53bGTwX6+XS/Xzm/Mx2DANBgkqhkiG9w0BAQUF
AAOBgQCpJsmA2IjGAlAfNPk1NDsJ7xhfWBHILAWNPhuusUgToHJGOqF/x3dQavJx
mFDTsUNMjIoVlPu3dqxZ4iqq1b4QLoH9dMdGKKi0bmBnRJMn+qZYqaUvI/RCYuL4
KO6c2FAEyLcvo+Nl4fNV98apMVYPj8tr48/4ESazFvfOjC5ZWw==
END CERTIFICATE
Signed certificate is in newcert.pem
```

4.3 Importation du certificat signé dans Fedora 1

Retournez sur la machine virtuelle Fedora 1. Récupérez le fichier `fedora1_cert_public.pem` et le placer dans `/etc/racoon/certs` :

```
scp IPCENTRECERTIFICATEUR:/etc/pki/tls/newcert.pem /etc/racoon/certs/fedora1_cert_public.pem
```

4.4 Configuration de Fedora 2

Recommencez les opérations 4.1 à 4.3 pour Fedora 2 en remplaçant les mots “Fedora 1” par “Fedora 2” et “Fed 1” par “Fed 2”.

5 Configuration d’un serveur web sécurisé

5.1 Test de la configuration par défaut

Sur la machine “centre de certification”, démarrez le service Web (en tant que `root`) : `/etc/init.d/httpd start`

Sur la machine “fedora1”, ouvrez `firefox` et connectez-vous au serveur Web du “centre de certification” : `https://IPDUCENTREDECERTIFICATION`.

Cliquez sur “examiner le certificat”, et consultez les différents champs de ce certificat.

5.2 Création d’un certificat personnalisé signé pour le serveur web

Nous allons maintenant créer un certificat signé par notre CA pour le serveur Web. Dans la suite, nous supposons que le domaine associé à ce service est `www.test.com`.

```
[root@localhost  ]# openssl req new nodes keyout www.cacentre_private.pem out
www.cacentre_request.pem days 365
Generating a 1024 bit RSA private key
..........++++++
.............................++++++
writing new private key to 'www.cacentre_private.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: FR
State or Province Name (full name) [Berkshire]: CENTRE
Locality Name (eg, city) [Newbury]: BOURGES
Organization Name (eg, company) [My Company Ltd]: INSA-CVL
Organizational Unit Name (eg, section) []: 4A-STI
Common Name (eg, your name or your server's hostname) []: www.test.com
Email Address []: jeremy.briffaut@insa-cvl.fr
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

5.3 Signature du certificat par le centre de certification

Copiez tout d'abord le certificat à signer dans le fichier `newreq.pem` :

```
cp www.cacentre_request.pem newreq.pem
```

Signez ce certificat par l'autorité de certification :

```
[root@localhost tls]# misc/CA -sign
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ../../CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
        Not Before: Nov 25 20:10:12 2007 GMT
        Not After : Nov 24 20:10:12 2008 GMT
        Subject:
        countryName = FR
        stateOrProvinceName = CENTRE
        localityName = BOURGES
        organizationName = INSA-CVL
        organizationalUnitName = 4A-STI
        commonName = www
        emailAddress = jeremy.briffaut@insa-cvl.fr
        X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            AC:23:6C:16:FE:18:6F:1C:DA:40:C1:E4:8F:32:83:5A:5C:10:DA:C0
        X509v3 Authority Key Identifier:
            keyid:F0:AF:91:8D:14:4E:77:6C:64:F0:5F:AF:97:4B:F5:F3:9B:F3:31:D8
Certificate is to be certified until Nov 24 20:10:12 2008 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, ST=Centre, O=INSA-CVL, OU=4A-STI,
CN=briffaut_centre_certificateur/emailAddress=jeremy.briffaut@insa-cvl.fr
        Validity
        Not Before: Nov 25 20:10:12 2007 GMT
        Not After : Nov 24 20:10:12 2008 GMT
        Subject: C=FR, ST=CENTRE, L=BOURGES, O=INSA-CVL, OU=4A-STI,
CN=www/emailAddress=jeremy.briffaut@insa-cvl.fr
        Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
```

```
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:c1:31:b8:d1:c2:b3:da:93:ba:c7:d4:fc:1d:5f:
                0b:f1:ae:01:a5:ac:2a:27:e0:6f:07:3c:53:e0:31:
                8b:0b:7e:f2:63:84:71:cd:a7:42:2d:10:d2:9d:08:
                83:c5:ba:4b:06:8e:23:f1:b0:e0:d2:81:29:e0:1e:
                d0:ce:c7:78:e0:63:e5:12:24:85:9a:b7:ee:56:83:
                b6:a4:21:7b:ec:66:99:1f:3d:d3:2d:50:63:12:17:
                ba:bd:0b:c7:80:fe:89:bc:0b:9b:6b:4d:e3:a4:50:
                ed:87:89:cd:be:cb:14:3e:ed:50:be:1e:ce:31:d5:
                cd:ca:a6:b8:04:3d:2d:77:11
            Exponent: 65537 (0x10001)
        X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            AC:23:6C:16:FE:18:6F:1C:DA:40:C1:E4:8F:32:83:5A:5C:10:DA:C0
        X509v3 Authority Key Identifier:
            keyid:F0:AF:91:8D:14:4E:77:6C:64:F0:5F:AF:97:4B:F5:F3:9B:F3:31:D8
    Signature Algorithm: sha1WithRSAEncryption
        33:09:25:94:eb:8a:53:31:75:49:e8:de:98:7f:f9:82:9e:66:
        92:4e:48:dc:4f:7a:88:3b:ff:2d:95:50:f8:39:67:4c:f1:00:
        b8:6f:20:8c:23:4c:b9:88:f9:30:b8:c3:02:7f:db:d0:39:a1:
        9c:c0:70:b9:65:63:a8:af:93:4f:24:a9:93:0b:50:c8:97:ee:
        22:6e:ac:cf:a9:04:1b:42:dd:67:6e:d4:8a:fa:18:a8:3c:24:
        70:b6:23:a7:30:35:00:7a:a4:45:4c:96:93:42:ac:54:ce:a5:
        ac:2c:e9:7e:03:eb:c0:3c:2f:b8:42:9f:ea:a8:61:99:ea:fc:
        c2:c2
-----BEGIN CERTIFICATE-----
MIIDFzCCAoCgAwIBAgIBAjANBgkqhkiG9w0BAQUFADCBljELMAkGA1UEBhMCRlIx
DzANBgNVBAgTBkNlbnRyZTEOMAwGA1UEChMFRU5TSUIxDjAMBgNVBAsTBVNUSTJB
MSYwJAYDVQQDDB1icmlmZmF1dF9jZW50cmVfY2VydGlmaWNhdGV1cjEuMCwGCSqG
SIb3DQEJARYfamVyZW15LmJyaWZmYXV0QGVuc2ktYm91cmdlcy5mcjAeFw0wNzEx
MjUyMDEwMTJaFw0wODExMjQyMDEwMTJaMIGOMQswCQYDVQQGEwJGUjEPMA0GA1UE
CBMGQ0VOVFJFMRAwDgYDVQQHEwdCT1VSR0VTMQ4wDAYDVQQKEwVFTlNJQjEOMAwG
A1UECxMFU1RJMkExDDAKBgNVBAMTA3d3dzEuMCwGCSqGSIb3DQEJARYfamVyZW15
LmJyaWZmYXV0QGVuc2ktYm91cmdlcy5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAwTG40cKz2pO6x9T8HV8L8a4BpawqJ+BvBzxT4DGLC37yY4RxzadCLRDS
nQiDxbpLBo4j8bDg0oEp4B7Qzsd44GPlEiSFmrfuVoO2pCF77GaZHz3TLVBjEhe6
vQvHgP6JvAuba03jpFDth4nNvssUPu1Qvh7OMdXNyqa4BD0tdxECAwEAAaN7MHkw
CQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2Vy
dGlmaWNhdGUwHQYDVR0OBBYEFKwjbBb+GG8c2kDB5I8yg1pcENrAMB8GA1UdIwQY
MBaAFPCvkY0UTndsZPBfr5dL9fOb8zHYMA0GCSqGSIb3DQEBBQUAA4GBADMJJZTr
ilMxdUno3ph/+YKeZpJOSNxPeog7/y2VUPg5Z0zxALhvIIwjTLmI+TC4wwJ/29A5
oZzAcLllY6ivk08kqZMLUMiX7iJurM+pBBtC3Wdu1Ir6GKg8JHC2I6cwNQB6pEVM
lpNCrFTOpaws6X4D68A8L7hCn+qoYZnq/MLC
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
```

5.4 Mise en place du certificat sur le serveur web

Copiez tout d'abord le certificat et sa clé privée dans les répertoires dédiés :

```
cp newcert.pem /etc/pki/tls/certs/www.pem
cp www.cacentre_private.pem /etc/pki/tls/private/www.key
```

Nous pouvons vérifier que le certificat est correctement signé à l'aide de la commande :

`openssl verify CAfile /etc/CA/cacert.pem /etc/pki/tls/certs/www.pem`

Modifiez la configuration du serveur Web pour prendre en compte ce certificat :

— Dans `/etc/httpd/conf.d/ssl.conf`, modifier les lignes :
  — `SSLCertificateFile /etc/pki/tls/certs/www.pem`
  — `SSLCertificateKeyFile /etc/pki/tls/private/www.key`
— Puis redémarrer le serveur Web : `/etc/init.d/httpd restart`

5.5 Vérification de la configuration

Sur la machine Fedora 1, connectez-vous de nouveau au serveur Web avec `firefox` : https://IPDUCENTREDECERTIFICATION

Vérifiez les informations du nouveau certificat. Ce certificat est-il correctement reconnu ?

5.6 Installation du certificat root du centre de certification

Afin de vérifier la validité du certificat du serveur Web, nous devons installer le certificat de notre CA sur les postes client. Pourquoi cette étape est-elle nécessaire ?

Sur la machine Fedora 1, copiez le certificat du CA :

`scp IPDUCENTREDECERTIFICATION:/etc/CA/cacert.pem /home/user/`

Importer ce certificat dans `firefox` :

`firefox > edition > preferences > securite > certificats > Autorité > Importer`

Importez le fichier `cacert.pem`. Cochez les 3 cases et validez.

Connectez-vous de nouveau au site Web et vérifier la hiérarchie de certification dans “détails” lorsque vous examiner le certificat.

Pourquoi ce certificat n’est-il pas automatiquement reconnu ?

Dans le fichier `/etc/host` ajouter : `IPDUCENTREDECERTIFICATION www.test.com`

Connectez vous sur https://www.test.com.

Quels sont les problèmes corrigés ?

Quels sont les problèmes résiduels ?

Comment corriger ce problème ?