HowTo ASIX

Certificats Digitals:

- Certificats Digitals x509
- Autoritats de certificació CA
- Seus Virtuals
- Certificats autosignats

Índex de continguts

Escola del treball de Barcelona

Departament d'informàtica

ASIX 2011

TSL/SSL Conexions segures (HTTPS)

Creació/Gestió de certificats digitals

Certificas digitals

- Crear un certificat auto-signat per fer tests
- Crear certificats per ser una pròpia CA.
- Crear els certificats del servidor basats en una CA (pròpia o externa)
- Afegir/modificar/eliminar una *passfrase* a una clau privada.

Crear certificats autosignats

- Vàlid per a fer de CA i per ser un certificat de servidor autosignat (sense que calgui una altra CA).
- Genera:
  - autosigned.server.cert és el certificat.
  - autosigned.server.key és la clau privada (“serverkey”)
- La clau privada generada no conté *passfrase*, una frase de seguretat que es demana com un password per poder desxifrar el fitxer. Se li pot afegir/modificar.

```
# Generar el certificat + clau privada autosignats

# openssl req -new -x509 -nodes -out autosigned.server.crt -keyout autosigned.server.key
Generating a 2048 bit RSA private key
..+++
.......+++
writing new private key to 'autosigned.server.key'
-----
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) [XX]:ca
State or Province Name (full name) []:Barcelona
Locality Name (eg, city) [Default City]:Barcelona
Organization Name (eg, company) [Default Company Ltd]:escola del treball de barcelona
Organizational Unit Name (eg, section) []:departament informatica
Common Name (eg, your name or your server's hostname) []:www.edt.org
Email Address []:admin@edt.org
# ll auto*
-rw-r--r-- 1 root root 1489 29 nov 16:28 autosigned.server.crt
```

```
-rw-r--r-- 1 root root 1704 29 nov 16:28 autosigned.server.key

# cat autosigned.server.crt
-----BEGIN CERTIFICATE-----
MIIEHTCCAwWgAwIBAgIJAMf0OqXXwvGYMA0GCSqGSIb3DQEBBQUAMIGkMQ
... output suprimit ...
PgCgnrTzCgSrMdWsvuFyaorcV6u9HaZoMDHkC5F4Bt76UbIZVo8F23s2Fhjl7Tjh
Sg==
-----END CERTIFICATE-----

# cat autosigned.server.key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC8VYl8jRqW5Pdm
... output suprimit ...
sbuv4mqD0dQrZHFPPGzPn+g=
-----END PRIVATE KEY-----
```

```
# Afegir passfrase a la clau privada (generem un nou fitxer de clau privada)

# openssl rsa -des3 -in autosigned.server.key -out autosigned.passfrase.server.key
writing RSA key
Enter PEM pass phrase: serverkey
Verifying - Enter PEM pass phrase: serverkey

# cat autosigned.passfrase.server.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,159C3F65D3CECAE4

pZpIBwsjVZoM9w2ZHrhfTrW6bRyvG/yTu3+93E+M9Sord3+CipWR9c9lMdEZyxik
... output suprimit ...
SkiF9OkA+9S2rYNkcnuDt4GXs+afzkMWSIqRRkPCsXXoaJ0n8zjWyQ==
-----END RSA PRIVATE KEY-----
```

Crear una CA pròpia: Certificate Authority

- Fer-ho manulment pas a pas:
  - generar la clau privada (observar amb cat el contingut físic i amb openssl el lògic)
  - generar el certificat x509 propi de la CA.
- Usar els scripts ja preparats de openssl (CA.sh o CA.pl).

```
# Crear una entitat CA pròpia
```

```
# generar la clau privada, encriptada amb 3des i amb passfrase (format PEM)
# openssl genrsa -des3 -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
..........++++++
.........................++++++
e is 65537 (0x10001)
Enter pass phrase for ca.key: cakey
Verifying - Enter pass phrase for ca.key:  cakey

# generar el certificat x509 pròpi de l'entitat CA (per a 365 dies) en format PEM
# openssl req -new -x509 -nodes -sha1 -days 365 -key ca.key -out ca.crt
Enter pass phrase for ca.key:  cakey
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) [XX]:ca
State or Province Name (full name) []:Bercelona
Locality Name (eg, city) [Default City]:Barcelona
Organization Name (eg, company) [Default Company Ltd]:Veritat Absoluta
Organizational Unit Name (eg, section) []:Departament de certificats
Common Name (eg, your name or your server's hostname) []:VeritatAbsoluta
Email Address []:admin@edt.org

# ll
-rw-r--r-- 1 root root 1159 29 nov 17:40 ca.crt
-rw-r--r-- 1 root root  963 29 nov 17:24 ca.key
```

```
# Observar la clau privada de la CA

# mostrar el contingut físic
# cat ca.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,770703FF70C7B96F

dx25QunUljFCtQJrSJQAgAtbnpCLhtxkVtozRsDv6SjbwtFbshaxm6hms6tANSmg
... output suprimit ...
8yAB1+vj72huDV2r4PVgXouRJcxCDKjMlrbWhRjJEWqPSgLdNC7z3Q==
-----END RSA PRIVATE KEY-----

# mostrar el contingut lògic
# openssl rsa -noout -text -in ca.key
```

```
Enter pass phrase for ca.key:
Private-Key: (1024 bit)
modulus:
    00:de:1c:ec:6c:2e:bf:4d:b6:ca:8d:93:d3:9d:41:
    ... output suprimit ...
    c8:90:13:34:ba:31:d1:b3:f5
publicExponent: 65537 (0x10001)
privateExponent:
    7d:8e:8e:1b:4d:85:b8:f1:a6:a8:c7:b2:ed:07:8d:
    ... output suprimit ...
    0f:03:eb:ef:ed:45:ba:b5
prime1:
    00:f2:44:ed:97:c3:e2:9a:aa:95:ae:67:26:86:0f:
    ... output suprimit ...
    13:50:0d:e0:4b
prime2:
    00:ea:b3:8c:97:c6:a4:95:57:39:e0:de:74:f1:b3:
    ... output suprimit ...
    71:ad:e4:94:bf
exponent1:
    70:b0:87:23:94:c6:0e:d3:52:14:71:7e:85:d5:5a:
    ... output suprimit ...
    c8:8e:eb:c9
exponent2:
    00:91:af:dc:80:c6:3c:99:bb:28:61:4e:95:57:07:
    ... output suprimit ...
    e0:b3:e9:a4:ef
coefficient:
    5a:92:81:89:a7:83:52:b5:33:16:ed:79:0e:25:c7:
    ... output suprimit ...
    2a:a2:bf:df
```

```
# Observar el certificat x509 de la CA

# mostrar el contingut físic del certificat x509
# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIDKjCCApOgAwIBAgIJANWdpn/8oUijMA0GCSqGSIb3DQEBBQUAMIGtMQswCQYD
... output suprimit ...
7zBltLVl0unEnCIxY0jNhWkLdwPz/CKuDCIl6c8XAVCfJRHMhWpi8EGUi4GW2A==
-----END CERTIFICATE-----

# mostrar el contingut lògic del certificat x509
# openssl x509 -noout -text -in ca.crt
Certificate:
    Data:
```

```
        Version: 3 (0x2)
        Serial Number:
            d5:9d:a6:7f:fc:a1:48:a3
        Signature Algorithm: sha1WithRSAEncryption
            Issuer: C=ca, ST=Bercelona, L=Barcelona, O=Veritat Absoluta, OU=Departament de
certificats, CN=VeritatAbsoluta/emailAddress=admin@edt.org
        Validity
            Not Before: Nov 29 16:40:57 2011 GMT
            Not After : Nov 28 16:40:57 2012 GMT
            Subject: C=ca, ST=Bercelona, L=Barcelona, O=Veritat Absoluta, OU=Departament de
certificats, CN=VeritatAbsoluta/emailAddress=admin@edt.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:de:1c:ec:6c:2e:bf:4d:b6:ca:8d:93:d3:9d:41:
                    ... output suprimit ...
                    c8:90:13:34:ba:31:d1:b3:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                35:7C:15:36:20:F3:B5:87:E2:C4:C8:71:5A:B2:87:16:7F:B8:13:63
            X509v3 Authority Key Identifier:
                keyid:35:7C:15:36:20:F3:B5:87:E2:C4:C8:71:5A:B2:87:16:7F:B8:13:63

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        33:39:de:3a:cc:c6:fd:74:a4:5e:40:cd:c9:33:f0:e7:27:32:
        ... output suprimit ...
        96:d8
```

Crear el certificat del servidor (real)

- Crear una clau privada per el servidor (o per el servei web desitjat).
- Crear una petició de certificat request per enviar a una CA:
  - indicar les dades apropiades de qui som quan demanem el certificat.
  - assegurar-se de que el CN (common name) és el de la seu web a usar el certificat.
- La CA genera el certificat .crt signat per ella mateixa i l'envia al client.
  - usar un fitxer de configuració de la CA que undiqui que els certificats a elaborar siguin de tipus “serverAuth”, és a dir, certificats de servidor.
  - Es generarà un número de sèrie dels certificats que l'entitat de certificació CA va emetent.
- “Et voilà” el servidor HTTP ja disposa d'un servificat que diu que “www.edt.org” és qui diu ser. Per tant si es fa la configuració SSL apropiada es podran fer connexions HTTPS.

```
# Crear una clau privada per al servidor
# és en format PEM, de 1024 bits i xifrada en 3DES. Utilitza passfrase
# podeu mirar a l'apartat “afegir/modificar/eliminar passfrases” si la voleu treure

# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for server.key: serverkey
Verifying - Enter pass phrase for server.key: serverkey

# Generar una petició de certificat request per enviar a l'entitat certificadora CA

# openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
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) [XX]:ca
State or Province Name (full name) []:Barcelona
Locality Name (eg, city) [Default City]:Barcelona
Organization Name (eg, company) [Default Company Ltd]:escola del treball de barcelona
Organizational Unit Name (eg, section) []:departament d'informatica
Common Name (eg, your name or your server's hostname) []:www.edt.org
Email Address []:admin@edt.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:request password
An optional company name []:edt

# ll
-rw-r--r-- 1 root root  10 29 nov 17:51 key.txt
-rw-r--r-- 1 root root 830 29 nov 17:58 server.csr
-rw-r--r-- 1 root root 963 29 nov 17:50 server.key

# Observar la petició de certificat

# openssl req -noout -text -in server.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
```

```
            Subject: C=ca, ST=Barcelona, L=Barcelona, O=escola del treball de barcelona,
OU=departament d'informatica, CN=www.edt.org/emailAddress=admin@edt.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:bc:6f:02:72:f2:f9:3f:19:62:2e:d8:46:61:46:
                    ... output suprimit ...
                    2c:6a:47:5b:db:99:14:28:af
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName        :unable to print attribute
            challengePassword       :unable to print attribute
    Signature Algorithm: sha1WithRSAEncryption
        10:8d:61:05:7f:12:76:41:e4:d6:09:d4:fc:a6:56:be:36:fa:
         ... output suprimit ...
        ee:99
```

```
# Una entitat CA ha de signar la petició request de certificat i retornar un certificat .crt.
# en aquest cas com que som CA nosaltres mateixos generarem el certificat (com a "Veritat
Absoluta") del client ("www.edt.org") que ha fet el request.

$ man x509
$ man ca

# Fitxer de configuració de la generació de certificats: indica què certifiquen
# cat ssl/ca/ca.conf
basicConstraints = critical,CA:FALSE
extendedKeyUsage = serverAuth,emailProtection

# L'autoritat CA ha de signar el certificat
# openssl x509 -CA ssl/ca/ca.crt -CAkey ssl/ca/ca.key -req -in ssl/server/server.csr -days 365
-sha1 -extfile ssl/ca/ca.conf  -CAcreateserial -out ssl/server/server.crt
Signature ok
subject=/C=ca/ST=Barcelona/L=Barcelona/O=escola del treball de barcelona/OU=departament
d'informatica/CN=www.edt.org/emailAddress=admin@edt.org
Getting CA Private Key
Enter pass phrase for ssl/ca/ca.key: cakey

# Mostrar el nº de sèrie que genera la CA  per a cada certificat que emet.
# cat ssl/ca/ca.srl
F96F36F4897271FF
```

```
# L'entitat li enviarà al client el certificat generat: server.crt
# ll
-rw-r--r-- 1 root root 1184 29 nov 18:09 server.crt
-rw-r--r-- 1 root root  830 29 nov 17:58 server.csr
-rw-r--r-- 1 root root  963 29 nov 17:50 server.key

# El client que ha sol·licitat el certificat pot validar el certificat respecte la seva clau privada
# openssl x509 -noout -modulus -in ssl/server/server.crt | openssl md5
(stdin)= 3b5cc670b2312990f4e53efc37194108
# openssl rsa -noout -modulus -in ssl/server/server.key | openssl md5
Enter pass phrase for ssl/server/server.key: serverkey
(stdin)= 3b5cc670b2312990f4e53efc37194108

# També pot examinar el contingut del certificat per veure si és realment el seu
# openssl x509 -noout -text -in ssl/server/server.crt
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         f9:6f:36:f4:89:72:71:ff
      Signature Algorithm: sha1WithRSAEncryption
          Issuer: C=ca, ST=Bercelona, L=Barcelona, O=Veritat Absoluta, OU=Departament de
certificats, CN=VeritatAbsoluta/emailAddress=admin@edt.org
      Validity
         Not Before: Nov 30 20:24:15 2011 GMT
         Not After : Nov 29 20:24:15 2012 GMT
          Subject: C=ca, ST=Barcelona, L=Barcelona, O=escola del treball de barcelona,
OU=departament d'informatica, CN=www.edt.org/emailAddress=admin@edt.org
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (1024 bit)
            Modulus:
               00:bc:6f:02:72:f2:f9:3f:19:62:2e:d8:46:61:46:
               ... output suprimit ...
               2c:6a:47:5b:db:99:14:28:af
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Basic Constraints: critical
            CA:FALSE
         X509v3 Extended Key Usage:
            TLS Web Server Authentication, E-mail Protection
   Signature Algorithm: sha1WithRSAEncryption
      4b:d1:73:d4:56:9b:5e:05:27:75:56:34:49:7d:c5:5f:7c:7d:
      ... output suprimit ...
      08:6e
```

Afegir/modificar/eliminar una passfrase de la clau privada

- Afegir a la clau <nom>.key per disposar de seguretat a la clau privada. Sense la passfrase ningú podrà utilitzar la clau privada. Cal la passfrase per desxifrar la clau privada per poder-la usar.
- Inconvenient: en engegar Apache demanarà la passfrase necessària per a cada certificat de servidor que en tingui una.
- Avantatge: seguretat de la clau privada. Si algú la pot obtenir es pot fer passar per nosaltres.
- Accions a saber fer:
  - afegir una passfrase a una clau privada que no en té: genera una nova key.
  - eliminar una passfrase d'una clau privada que ja en té: genera una nova key no xifrada (perill!).
  - modificar una passfrase d'una clau provada que ja en té una: genera una nova key.

```
# Afegir passfrase a la clau privada (generem un nou fitxer de clau privada)

# openssl rsa -des3 -in server.key -out passfrase.server.key
writing RSA key
Enter PEM pass phrase: serverkey
Verifying - Enter PEM pass phrase: serverkey
## mv passfrase.server.key server.key

# Modificar la passfrase existent

# openssl rsa -des3 -in passfrase.server.key -out passfrase.new.server.key
Enter pass phrase for passfrase.server.key:
writing RSA key
Enter PEM pass phrase: serverkey
Verifying - Enter PEM pass phrase: newserverkey
## mv passfrase.new.server.key passfrase.server.key

# Eliminar la passfrase d'una clau privada

# openssl rsa -in passfrase.server.key -out deleted-passfrase.server.key
Enter pass phrase for autosigned.passfrase.server.key: serverkey
writing RSA key
## mv deleted-passfrase.server.key server-key

# Llistat de tot el que s'ha anat generant
# ll
-rw-r--r-- 1 root root 1675 29 nov 16:55 deleted-passfrase.server.key
-rw-r--r-- 1 root root 1743 29 nov 16:48 passfrase.new.server.key
-rw-r--r-- 1 root root 1743 29 nov 16:37 passfrase.server.key
-rw-r--r-- 1 root root 1489 29 nov 16:28 server.crt
-rw-r--r-- 1 root root 1704 29 nov 16:28 server.key
```

Examinar els continguts de certificats i claus privades

- Examinar el contingut de certificats.
- Examinar el contingut de claus privades.
- Verificar si corresponen com a parella “certificat / clau-privada”

```
# Examinar el contingut de certificats:

# openssl x509 -noout -text -in autosigned.server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            c7:f4:3a:a5:d7:c2:f1:98
        Signature Algorithm: sha1WithRSAEncryption
            Issuer: C=ca, ST=Barcelona, L=Barcelona, O=escola del treball de barcelona, OU=depaca,
CN=www.edt.org/emailAddress=admin@edt.org
        Validity
            Not Before: Nov 29 15:28:02 2011 GMT
            Not After : Dec 29 15:28:02 2011 GMT
        Subject: C=ca, ST=Barcelona, L=Barcelona, O=escola del treball de barcelona, OU=depaca,
CN=www.edt.org/emailAddress=admin@edt.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bc:55:89:7c:8d:1a:96:e4:f7:66:91:87:e9:63:
                    ... output suprimit ...
                    86:35
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                3F:3A:CC:C3:50:4C:28:89:B4:07:76:B3:3A:45:C9:40:63:40:E1:12
            X509v3 Authority Key Identifier:
                keyid:3F:3A:CC:C3:50:4C:28:89:B4:07:76:B3:3A:45:C9:40:63:40:E1:12

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        32:fd:29:72:57:81:ff:ae:55:d9:46:87:df:3b:31:8c:27:12:
        ... output suprimit ...
        ed:38:e1:4a
```

```
# Mostrar el contingut de la clau privada
```

```
# openssl rsa -noout -text -in autosigned.server.key
Private-Key: (2048 bit)
modulus:
    00:bc:55:89:7c:8d:1a:96:e4:f7:66:91:87:e9:63:
    ... output suprimit ...
    86:35
publicExponent: 65537 (0x10001)
privateExponent:
    40:3a:33:8f:04:58:03:09:c6:cd:75:e8:11:d1:b3:
    ... output suprimit ...
    41
prime1:
    00:f5:7b:53:1f:8e:53:d5:e0:0c:19:2c:25:91:a5:
    ... output suprimit ...
    53:8e:50:bd:1e:7e:72:e9:a9
prime2:
    00:c4:67:5d:0c:aa:76:c3:35:3a:e0:c8:96:f4:f9:
    ... output suprimit ...
    d6:a6:17:09:bd:9f:b4:07:ad
exponent1:
    49:24:68:bd:03:44:59:7a:7b:40:58:d6:0c:d2:83:
    ... output suprimit ...
    71:2d:ff:5b:81:a3:ad:99
exponent2:
    00:83:6f:70:d3:d3:18:1b:56:fa:0a:07:f3:0e:0a:
    ... output suprimit ...
    88:de:29:b8:b9:0f:b1:59:19
coefficient:
    5f:44:60:85:5c:44:41:92:91:da:c2:c4:70:d8:ed:
    ... output suprimit ...
    64:71:4f:3c:6c:cf:9f:e8
```

```
# Verificar que el certificat i la clau-privada són conjuntats, es corresponen

# openssl x509 -noout -modulus -in autosigned.server.crt | openssl md5
(stdin)= db5c2f5add8d40d76b9ce4b962d94ab8
# openssl rsa -noout -modulus -in autosigned.server.key | openssl md5
(stdin)= db5c2f5add8d40d76b9ce4b962d94ab8
```

Estructura de directoris usada en els exemples

```
# Des d'un directori de proves (/tmp/ssl) s'ha generat:
```

```
# tree
.
├── autosigned
│   ├── autosigned.deleted-passfrase.server.key
│   ├── autosigned.passfrase.new.server.key
│   ├── autosigned.passfrase.server.key
│   ├── autosigned.server.crt
│   ├── autosigned.server.key
│   ├── dn.txt
│   └── key.txt
├── ca
│   ├── ca.conf
│   ├── ca.crt
│   ├── ca.exemple.conf
│   ├── ca.key
│   ├── ca.srl
│   ├── dn.txt
│   └── key.txt
└── server
    ├── key.txt
    ├── server.crt
    ├── server.csr
    └── server.key
```