

Treball final de Grau

Autoritat de Certificació

Local amb OpenSSL

Manual d'usuari

The logo of the Universitat Oberta de Catalunya (UOC) is displayed in a large, stylized, dark blue font. It consists of the letters 'UOC' in a bold, sans-serif typeface.

Manel Esteban Rivas

Grau d'Enginyeria Informàtica
Seguretat Informàtica

Tutor/a de TF

Gerard Farràs Ballabriga

**Professor/a responsable de
l'assignatura**

Andreu Pere Isern Deyà

Universitat Oberta
de Catalunya

Índex

1.	Introducció	1
2.	Requisits del sistema i instal·lació	2
3.	Jerarquia de la AC Local i estructura de carpetes	2
4.	Tasques inicials	2
4.1.	Creació de l'estructura de carpetes	3
4.2.	Definició de les identitats i polítiques per defecte	3
4.3.	Emissió dels certificats AC Arrel i AC Intermèdia	4
4.4.	Creació del fitxer amb la cadena de certificació	5
5.	Emissió de certificats	5
5.1.	Certificats d'usuari	6
5.2.	Certificats SSL/TLS	7
6.	Revocació de certificats	10
7.	Creació de la llista de certificats revocats (CRL)	10
8.	Altres eines	11

1.Introducció

Avui en dia, l'ús de certificats digitals ofereix una capa de seguretat a les comunicacions tant internes com externes d'una organització, permetent establir comunicacions electròniques amb confiança en la identitat dels extrems, així com la confidencialitat del tràfic entre ells, i també la seva integritat.

Per a les comunicacions externes, serà necessari que cada organització triï quin és el proveïdor de serveis de certificació més adient per les seves necessitats i pressupost, però, per a les comunicacions internes, el poder disposar d'una autoritat de certificació (AC) local que permeti emetre certificats digitals a demanda i amb un cost mínim, proporciona un enorme grau d'autonomia i estalvi econòmic.

Aquest manual d'usuari especifica els procediments i actuacions per a poder desplegar una AC Local a una organització.

Crèdits / Copyright

Tot el codi contingut a aquest treball es troba subjecte a la Llicència MIT.

MIT License

Copyright (c) 2023 Esteban Rivas, Manel

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

2.Requisits del sistema i instal·lació

Aquest manual d'usuari parteix de la premissa que l'organització usuària disposa d'una màquina (física o virtual) Linux dins la seva infraestructura, amb un accés controlat i limitat als administradors i operadors de l'AC.

Així mateix, cal que la màquina tingui instal·lada alguna versió d'OpenSSL, preferiblement la darrera versió LTS (*Long Term Support*) o la darrera versió publicada. Les versions d'OpenSSL disponibles es poden descarregar des de <https://www.openssl.org/source/>.

Una vegada decidida la carpeta on s'hi desplegarà l'AC Local, cal descarregar el conjunt d'*scripts* d'administració i fitxers de configuració amb la comanda

```
git clone https://github.com/MEstebanUOC/AutoritatCertificacio
```

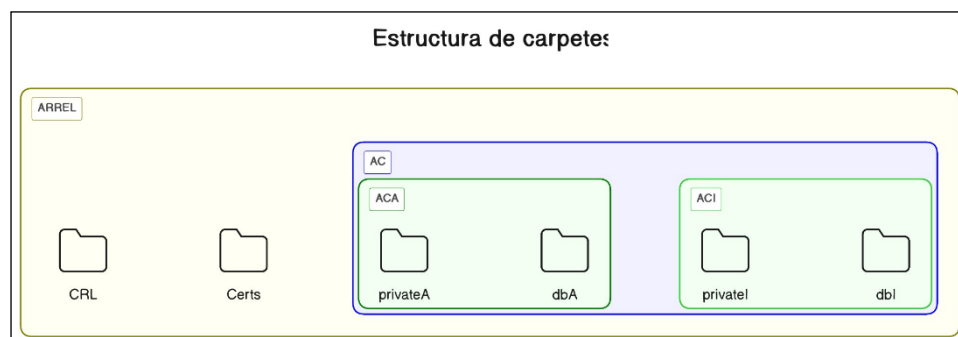
Si l'organització usuària utilitza un altre Sistema Operatiu o vol emprar una altra jerarquia o estructura de carpetes diferent de la proposada, caldrà que modifiqui els scripts conseqüentment.

3.Jerarquia de la AC Local i estructura de carpetes

L'AC Local tindrà una jerarquia en dos nivells, una AC Arrel, i una AC Intermèdia que serà la que emetrà els certificats finals SSL/TLS i d'usuari.

Aquesta jerarquia tindrà el seu reflex en l'estructura de carpetes:

- . / (Carpeta arrel). Hi contindrà tots els scripts i arxius de configuració de l'AC Local.
- ./ac. Hi contindrà tots els arxius relatius a l'AC: certificats de l'AC Arrel i Intermèdia, fitxer de cadena de certificats, etc.
- ./ac/acA. Hi contindrà tots els arxius relatius a l'AC Arrel: fitxers de números de sèrie de certificats i CRL, arxíu de base de dades de certificats, etc.
- ./ac/acI. Com en el cas anterior, contindrà tots els arxius relatius a l'AC Intermèdia.
- ./certs. Hi contindrà tots els fitxers CSR, certificats i claus, així com els arxius PFX resultants de les exportacions a PKCS#12.
- ./crl. Hi contindrà els arxius CRL.



4.Tasques inicials

Cal que comproveu que els scripts de gestió de l'AC i d'altres utilitats que heu descarregat tenen els privilegis d'execució per als usuaris o grups que seran els operadors de l'AC Local.

Tots els scripts que conformen aquest projecte disposen del prefix `ac_`, i per tant, per a garantir que l'usuari actual tingui privilegis d'execució sobre aquesta col·lecció d'utilitats, podeu utilitzar

```
chmod u+x ac_*
```

4.1. Creació de l'estructura de carpetes

Per a construir l'estructura bàsica de carpetes, podeu utilitzar la comanda

```
./ac_init
```

Aquesta comanda crearà l'estructura, així com inicialitzarà els diferents fitxers de base de dades i números de sèrie de l'AC.

4.2. Definició de les identitats i polítiques per defecte

Les identitats i polítiques de l'AC Local, així com els valors predeterminats d'alguns atributs i extensions els podeu trobar als diferents fitxers de configuració ubicats a la carpeta arrel. En concret són

Fitxer	Secció	Usos i exemples
acA.conf	[ac_dn]	Camps del <i>Distinguished Name</i> (DN) de l'AC Arrel.
	[req]	Es pot triar la mida de la clau, l'algorisme de hash. És important mantenir el camp <code>encrypt_key=yes</code> per a xifrar la clau privada.
	[acA]	Polítiques per defecte, per exemple, període de validesa, declarat a <code>default_days</code> . També cal modificar aquesta secció si es modifica l'estructura de carpetes predeterminada.
acI.conf	[ac_dn]	Camps del <i>Distinguished Name</i> (DN) de l'AC Intermèdia.
	[req]	Polítiques per defecte. Es pot triar la mida de la clau, l'algorisme de hash. És important mantenir el camp <code>encrypt_key=yes</code> per a xifrar la clau privada.
	[acA]	Polítiques per defecte, per exemple, període de validesa, declarat a <code>default_days</code> . També cal modificar aquesta secció si es modifica l'estructura de carpetes predeterminada.
usuari.conf	[req]	Polítiques per defecte dels certificats d'usuari.
	[usuari_dn]	Polítiques i valors per defecte dels camps que composaran el DN dels certificats d'usuari.
	[usuari_reqext]	Extensions que s'incorporaran als certificats d'usuari. Dins aquesta secció es pot definir el punt de distribució de les CRL (<code>crlDistributionPoints</code>).
servidor.conf	[req]	Polítiques per defecte dels certificats SSL/TLS. El camp <code>encrypt_key</code> està definit com a <code>no</code> per a evitar que alguns serveis, com ara un servidor Apache, demani la contrasenya de cada certificat instal·lat quan arranqui.
	[tls_dn]	Polítiques i valors per defecte dels camps que composaran el DN dels certificats SSL/TLS.
	[tls_reqext]	Extensions que s'incorporaran als certificats SSL/TLS. Dins aquesta secció es pot definir el punt de distribució de les CRL (<code>crlDistributionPoints</code>). L' <code>extendedKeyUsage</code> està definit per defecte per a permetre tant <code>serverAuth</code> com <code>clientAuth</code> .


```
manel@blackie: ~/AutoritatCertificacio
Signature ok
Certificate Details:
  Serial Number: 1 (0x1)
  Validity
    Not Before: Oct 30 18:06:15 2023 GMT
    Not After : Oct 29 18:06:15 2033 GMT
  Subject:
    organizationName       = Organitzacio Prova
    organizationalUnitName = AC Interna
    commonName             = AC Interna Arrel
    countryName            = ES
    stateOrProvinceName    = Illes Balears
  X509v3 extensions:
    X509v3 Key Usage: critical
      Certificate Sign, CRL Sign
    X509v3 Basic Constraints: critical
      CA:TRUE
    X509v3 Subject Key Identifier:
      51:82:92:07:15:31:C5:92:BD:CA:DF:93:0E:3C:80:09:94:49:29:F4
    X509v3 Authority Key Identifier:
      51:82:92:07:15:31:C5:92:BD:CA:DF:93:0E:3C:80:09:94:49:29:F4
Certificate is to be certified until Oct 29 18:06:15 2033 GMT (3652 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
manel@blackie: ~/AutoritatCertificacio$
```

A continuació, cal emetre el certificat per a l'AC Intermèdia, amb la comanda

```
./ac_crear_acI
```

Que, de manera similar a la creació del certificat per a l'AC Arrel, demanarà una contrasenya per a la clau privada del certificat de l'AC Intermèdia. Aquest certificat el signarà l'AC Arrel, i, per tant, caldrà introduir la contrasenya de la seva clau privada. Finalment, també es demanarà conformitat per a signar el nou certificat, i per a introduir-lo a la base de dades.

Els certificats de l'AC Arrel i l'AC Intermèdia es guarden a la carpeta `./ac`, amb format PEM i extensió `.crt`.

Es pot veure el contingut dels certificats amb la comanda

```
./ac_mostrar_cert <fitxer>
```

Que mostrarà el contingut de qualsevol certificat X.509, en format llegible pels humans i també en format PEM.

4.4. Creació del fitxer amb la cadena de certificació

Una vegada creats els certificats de l'AC Arrel i l'AC Intermèdia, cal generar el fitxer amb la cadena de certificació, que serà útil per diferents tasques posteriors, així com per a definir la cadena de validació de certificats en diferents aplicacions, com ara el servidor Apache.

Per a crear aquest fitxer, es pot utilitzar la comanda

```
./ac_crear_cacert
```

Aquesta comanda deixarà a la carpeta `./ac` el fitxer `cacert.pem`.

5. Emissió de certificats

L'objectiu d'aquest projecte és construir una infraestructura d'AC Local que permeti emetre dos tipus de certificats: d'usuari i SSL/TLS.

Les comandes per a emetre aquests certificats tenen un paràmetre obligatori un nom identificador del certificat que es vulgui generar. Els processos s'aturaran si ja existeix un fitxer de certificat amb un nom ja utilitzat.

Aquestes comandes Els utilitzaran la carpeta `./certs` per a desar els fitxers producte de la seva acció:

Fitxer	Contingut
<nom_identificador>.csr	<i>Certificate Signature Request (CSR)</i> del certificat.
<nom_identificador>.crt	El certificat emès, en format PEM.
<nom_identificador>.key	La clau privada del certificat.

5.1. Certificats d'usuari

Abans de començar amb l'emissió de certificats d'usuari cal que s'hagin definit les seccions del fitxer de configuració `usuari.conf` segons els requisits necessaris.

Per a emetre aquest tipus de certificat, cal fer servir la comanda

```
./ac crear usuari <nom identificador certificat>
```

Cal utilitzar un nom prou identificador per al certificat, per a simplificar la seva gestió posterior, com ara l'exportació a PKCS#12 o la seva revocació. Amb aquest nom es crearan tres fitxers a `./certs`:

En funció de com s'hagi definit la secció [usuari_dn] de l'arxiu de configuració, la composició dels diferents camps del subjecte del certificat poden variar, així com els seus valors per defecte i les seves polítiques de validació (mida mínima i màxima, etc.).

Amb la configuració per defecte, el procés d'emissió d'un certificat d'usuari es mostraria com a l'exemple següent.

[illegible]

Els camps amb valors per defecte es mostren amb aquests indicats entre claudàtors, com ara [ORGANITZACIO DE PROVA]. Si aquests camps s'accepten amb **ENTER**, s'acceptarà el valor predeterminat, tot i que també poden ser modificats, introduint un valor diferent.


```
manel@blackie: ~/prova/AutoritatCertificacio
Enter pass phrase for ./ac/acI/private/acI.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 1 (0x1)
  Validity
    Not Before: Dec 14 17:53:53 2023 GMT
    Not After : Dec 13 17:53:53 2027 GMT
  Subject:
    organizationName      = ORGANITZACIO DE PROVA
    organizationalUnitName = DEPARTAMENT DE COMPTABILITAT
    commonName            = JOHN DOE
    countryName            = ES
    stateOrProvinceName   = Illes Balears
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Subject Key Identifier:
      60:5C:AC:29:09:54:A2:52:EC:74:2D:FC:80:0C:1C:E6:7C:74:6B:1C
    X509v3 Authority Key Identifier:
      DD:79:27:76:2A:BB:D1:F9:D8:B3:58:67:51:A6:1D:43:F5:38:15:54
    X509v3 Key Usage: critical
      Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Extended Key Usage:
      TLS Web Client Authentication, E-mail Protection
    X509v3 Subject Alternative Name:
      email:jd@organitacio.com
    X509v3 CRL Distribution Points:
      Full Name:
        URI:http://www.intranet.local/crl/acintermedia.crl
Certificate is to be certified until Dec 13 17:53:53 2027 GMT (1460 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
Database updated
Certificat creat a certs/prova.crt correctament. Podeu usar ./ac_exportar_p12 per a exportar el certificat a PFX.
manel@blackie:~/prova/AutoritatCertificacio$
```

Cal tenir present que els certificats finals són signats per l'AC Intermèdia, i per tant, caldrà fer servir la seva contrasenya de la seva clau privada.

Així mateix, com en el cas dels certificats de les AC Arrel i Intermèdies, el sistema ens demanarà si es vol signar el nou certificat, i si aquest cal que sigui guardat a la base de dades.

5.2. Certificats SSL/TLS

L'altre tipus de certificats prevista en aquest projecte són els certificats SSL/TLS, pensats per a identificar una màquina o lloc web individual, tot el subdomini d'un domini o una combinació d'aquests.

Tradicionalment, s'ha fet servir l'atribut *CommonName* (CN) del *DistinguishedName* (DN) com a nom del subjecte d'un certificat SSL/TLS, però, el fet que es trobi limitat a un únic nom per certificat ha fet que es prefereixi la utilització de l'extensió *SubjectAlternativeName* (SAN), que, a més, de permetre múltiples noms de domini, també accepta altres valors, com, per exemple, IPs.

Abans de començar amb l'emissió de certificats SSL/TLS cal que s'hagin definit les seccions del fitxer de configuració `servidor.conf` segons els requisits necessaris de l'organització.

La comanda per a emetre aquests tipus de certificat acceptarà un paràmetre obligatori amb un nom identificador del certificat, com ja s'ha vist amb el cas d'emissió de certificats d'usuari, però, a més, acceptarà un paràmetre opcional que permetrà proporcionar a la comanda les dades que es voldran desar a l'extensió SAN.

```
./ac_crear_servidor <nom_identificador_certificat> [fitxer_SAN]
```

La comanda utilitzarà dos variables d'entorn (`AC_TLS_CN` i `AC_TLS_SAN`), que el fitxer `servidor.conf` recollirà com a valor per defecte del CN del subjecte, i com a valor de

l'extensió SAN, respectivament. Aquestes variables d'entorn es carregaran de diferents formes, en funció del tipus de certificat:

Certificat simple (màquina o lloc web individual). La comanda sol·licitarà a l'operador que introdueixi per teclat un valor *Full Qualified Domain Name* (FQDN), que es carregará sobre ambdues variables d'entorn. Per exemple, `www.intranet.local`. El certificat es podrà utilitzar per a identificar `www.intranet.local` únicament.

Certificat *wildcard*. Com en el cas anterior, la comanda sol·licitarà a l'operador que introdueixi un valor FQDN. En aquest cas, l'operador haurà d'introduir un comodí (*wildcard*) amb el caràcter "*", que substituirà tot un subdomini. Per exemple, `*.intranet.local`. El certificat es podrà utilitzar per a identificar qualsevol subdomini del domini `intranet.local` (com ara `www.intranet.local`, `crl.intranet.local`, etc).

Certificat SAN. En aquest cas, també es sol·licitarà a l'operador el valor FQDN per a l'atribut CN, però, a més caldrà generar un fitxer que contingui els valors que es vulguin carregar a l'extensió SAN del certificat, que s'utilitzarà com a paràmetre opcional de la comanda.

S'accepten dos tipus de valors a l'extensió SAN: DNS i IP, que es poden combinar per a representar diferents mètodes d'identificació:

Valor	Sintaxi	Exemple
FQDN	DNS:<FQDN>	DNS:www.intranet.local
Wildcard	DNS:*.domini.TLD	DNS:*.intranet.local
IP	IP:<IP>	IP:192.168.0.254

Entre un valor i el següent, cal emprar un caràcter "," com a separador. Per exemple, si es volgués utilitzar el certificat per a identificar una màquina o lloc web `www.intranet.local`, però també tot el subdominis `*.wildcard.local` i la IP `10.215.0.1`, es podria usar una cadena com la següent:

```
DNS:www.intranet.local,DNS:*.wildcard.local,IP:192.168.0.254
```

S'han desat aquestes dades d'exemple al fitxer `san.txt` que podreu trobar entre els arxius del projecte.

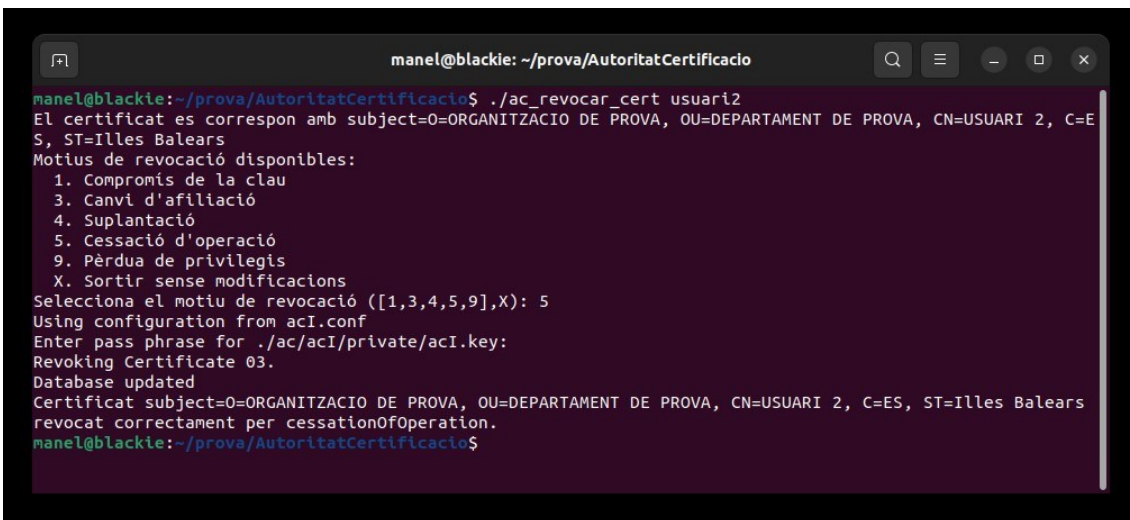
6.Revocació de certificats

Els certificats emesos arribaran, eventualment, a la seva data d'expiració, indicada per l'atribut `Not After` del certificat. Ara bé, es poden produir circumstàncies que puguin exigir que un certificat en concret hagi de ser revocat abans d'aquesta data, per exemple, en cas d'un usuari, que hagi deixat de desenvolupar tasques a l'organització, o bé, en el cas d'un servidor o pàgina web, que hagi canviat de nom.

En aquests escenaris, cal procedir a revocar els certificats amb la comanda

```
./ac_revocar_cert <nom_identificador_certificat>
```

Durant el procés de revocació, caldrà indicar el motiu de revocació, d'entre la llista que proposarà la comanda, que es basa en les causes de revocació dels certificats TLS/SSL de Mozilla Foundation. És possible modificar el codi de la comanda per a afegir-hi més motius.



```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_revocar_cert usuari2
El certificat es correspon amb subject=O=ORGANITZACIO DE PROVA, OU=DEPARTAMENT DE PROVA, CN=USUARI 2, C=ES, ST=Illes Balears
Motius de revocació disponibles:
  1. Compromís de la clau
  3. Canvi d'afiliació
  4. Suplantació
  5. Cessació d'operació
  9. Pèrdua de privilegis
  X. Sortir sense modificacions
Selecciona el motiu de revocació ([1,3,4,5,9],X): 5
Using configuration from acI.conf
Enter pass phrase for ./ac/acI/private/acI.key:
Revoking Certificate 03.
Database updated
Certificat subject=O=ORGANITZACIO DE PROVA, OU=DEPARTAMENT DE PROVA, CN=USUARI 2, C=ES, ST=Illes Balears
revocat correctament per cessationOfOperation.
manel@blackie:~/prova/AutoritatCertificacio$
```

L'acció de revocació d'un certificat cal que sigui signada per l'AC Intermèdia, que va ser l'autoritat emissora del certificat.

7.Creació de la llista de certificats revocats (CRL)

La informació dels certificats revocats per l'AC cal distribuir-la periòdicament als llocs que l'organització necessiti. Per defecte, els fitxers de configuració preveuen un punt de distribució de CRL, indicada a l'extensió `crlDistributionPoints` dels fitxers `usuari.conf` i `servidor.conf`, que caldrà modificar pel punt correcte, o eliminar si els mecanismes de distribució de CRL són diferents.

Per a crear la CRL, caldrà usar la comanda

```
./ac_construir_crl
```

```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_construir_crl
Using configuration from acI.conf
Enter pass phrase for ./ac/acI/private/acI.key:
S'ha generat la nova CRL per a l'AC Intermedia a crl/acintermedia.crl. Assegura-vos de distribuir-la
als punts de distribució necessaris.
manel@blackie:~/prova/AutoritatCertificacio$
```

8. Altres eines

El projecte també incorpora tot un conjunt de comandes addicionals per a gestionar l'AC Local, dissenyades per a recolzar l'activitat dels operadors.

`./ac_exportar_p12 <nom_identificador_certificat>`

Un dels sistemes més difosos per a distribuir els certificats finals (especialment en els casos de certificats d'usuaris), és utilitzar el format PFX o PKCS#12. Amb aquesta comanda podrem exportar qualsevol dels certificats emesos en aquest format, especificant una contrasenya per a l'exportació/importació del certificat.

```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_exportar_p12 prova
Exportant el certificat certs/prova.crt com a Personal Information eXchange (PFX).
Enter Export Password:
Verifying - Enter Export Password:
S'ha exportat el fitxer certs/prova.p12 correctament.
manel@blackie:~/prova/AutoritatCertificacio$
```

`./ac_mostrar_cert <nom_identificador_certificat>`

Amb aquesta comanda es mostrarà la informació continguda a qualsevol dels certificats emesos per l'AC Local, o qualsevol altre que es trobi a la carpeta `./certs` amb extensió `.crt`, la qual cosa pot ser útil per a mostrar certificats emesos per altres AC.


```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_mostrar_cert prova | more
Mostrant un certificat a prova...
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: O=Organitzacio Prova, OU=AC Interna, CN=AC Intermedia, C=ES, ST=Illes Balears
    Validity
      Not Before: Dec 14 17:53:53 2023 GMT
      Not After : Dec 13 17:53:53 2027 GMT
    Subject: O=ORGANITZACIO DE PROVA, OU=DEPARTAMENT DE COMPTABILITAT, CN=JOHN DOE, C=ES, ST=Illes Balears
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        00:c0:b7:0b:74:cb:3f:f7:55:f8:a4:ca:90:3c:e6:
        f9:97:a7:48:95:d4:99:1c:fa:c3:72:23:aa:be:55:
        ad:dd:74:83:ce:fe:e5:a7:d4:1d:6b:4a:10:af:eb:
        23:10:c2:3f:28:92:19:06:a4:40:3e:16:e1:48:a6:
        bb:34:bc:5c:ae:c6:69:ad:37:b2:cd:fa:79:c1:13:
        ac:3c:6d:67:17:45:b7:0e:9d:d5:c1:57:98:6c:99:
        f1:15:da:8a:df:34:02:4b:a6:1c:74:83:b9:50:59:
        97:c6:86:d9:59:39:20:0f:5e:6d:b6:ad:24:bd:1e:
        ed:c4:20:9e:d7:c2:20:bf:5a:00:93:19:d1:d5:c5:
        93:dc:a8:50:b8:9e:01:6b:8b:2f:38:fb:d8:65:61:
        a2:6a:12:a4:0b:ef:ed:46:26:85:cb:4a:f3:91:a4:
        82:ab:84:b5:dc:23:20:f4:12:af:c1:cf:6c:98:d8:
        bc:0f:ea:ba:f6:8b:f5:2c:a8:4d:67:19:dd:f3:0b:
        e3:62:e1:6c:4f:52:5e:ab:d5:8a:c0:5a:86:6b:10:
        cd:32:ae:62:dd:22:3a:16:9b:60:37:1b:93:ee:87:

```

`./ac_mostrar_csr <nom_identificador_certificat>`

Aquesta eina mostrarà la informació del CSR utilitzat per a generar el certificat que tingui com a identificador el que s'hagi passat com a paràmetre. Com passa amb la comanda `./ac_mostrar_cert`, també es pot utilitzar per a mostrar el contingut de qualsevol arxiu `.csr` que hi hagi a la carpeta `./certs`.

```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_mostrar_csr ssl1
Certificate Request:
  Data:
    Version: 1 (0x0)
    Subject: O=ORGANITZACIO DE PROVA, OU=DEPARTAMENT INFORMATICA, CN=www.intranet.local, ST=Illes Balears, C=ES
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:aa:27:c2:05:e2:53:71:0e:5b:be:76:96:cd:b2:
        37:75:af:2c:8e:b9:83:53:37:68:1c:27:6a:12:29:
        aa:99:7e:b5:2d:12:cb:a5:0a:22:1a:c5:37:95:53:
        e4:08:f9:6f:c4:e2:4f:c9:b9:5a:97:49:3b:23:0d:
        00:73:47:e0:c6:e9:68:75:78:ce:1e:dc:ea:26:d1:
        ec:77:14:1a:09:79:af:32:ee:c8:3a:d1:85:7e:16:
        56:6b:16:f1:6f:ab:82:aa:de:52:62:f3:f2:29:47:
        74:b3:aa:e6:df:92:0c:68:00:5f:96:b7:93:2d:42:
        f1:84:3f:20:2a:31:5a:00:5c:29:89:d8:2c:cb:b9:
        51:de:7a:57:84:ab:c9:05:ba:33:04:ae:31:5e:ae:
        0f:5b:e5:cc:82:c4:16:7c:e0:93:9d:ee:59:b0:07:
        c0:5d:b3:8e:3b:62:56:fa:9d:98:85:af:5b:21:02:
        c5:f9:ad:70:fc:e4:ca:63:9a:9c:0d:3a:7e:cd:53:
        08:05:a4:02:d2:00:2c:b9:e7:d8:c7:46:d1:1a:76:
        92:f0:ac:19:88:59:d5:a5:ad:cc:f3:49:8e:db:2b:
        68:f3:a9:aa:bd:d2:89:27:78:11:86:0d:1c:c7:c2:
        90:fb:f4:99:6d:2a:87:77:56:23:b2:d9:45:bf:e3:
        26:87
      Exponent: 65537 (0x10001)
    Attributes:
      Requested Extensions:
        X509v3 Key Usage: critical
          Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
          TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Subject Key Identifier:
          28:AC:A5:05:32:25:6E:6C:BB:AD:FF:F8:24:CA:20:1D:6A:B5:59:49
        X509v3 Subject Alternative Name:
          DNS:www.intranet.local, DNS:*.wildcard.local, IP Address:192.168.0.254
        X509v3 CRL Distribution Points:
          Full Name:
            URI:http://www.intranet.local/crl/acintermedia.crl

```

`./ac_mostrar_crl`

Aquesta comanda mostrarà el contingut de la CRL de l'AC Intermedà.

```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_mostrar_crl
Mostrant la llista CRL de l'AC Intermedia.
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: O=Organitzacio Prova, OU=AC Interna, CN=AC Intermedia, C=ES, ST=Illes Balears
  Last Update: Dec 16 17:31:16 2023 GMT
  Next Update: Dec 15 17:31:16 2024 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      DD:79:27:76:2A:BB:D1:F9:D8:B3:58:67:51:A6:1D:43:F5:38:15:54
    X509v3 CRL Number:
      1
Revoked Certificates:
  Serial Number: 03
  Revocation Date: Dec 16 17:23:05 2023 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Cessation Of Operation
  Signature Algorithm: sha256WithRSAEncryption
  Signature Value:
    3d:a1:eb:d0:b0:8d:9d:01:fb:ff:f0:71:41:79:07:f7:31:e0:
    5c:84:35:5d:eb:0f:e3:e2:39:af:1a:c3:8c:92:6d:40:eb:df:
```

`./ac_verificar_cert <nom_identificador_certificat>`

Aquesta eina permetrà verificar si un certificat emès per l'AC Local és vàlid, i no està revocat.

```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_verificar_cert prova
Verificant el certificat prova.
./certs/prova.crt: OK
El certificat ./certs/prova.crt (subject=O=ORGANITZACIO DE PROVA, OU=DEPARTAMENT DE COMPTABILITAT, CN=JOHN DOE, C=ES, ST=Illes Balears) i s'ha validat correctament.
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_verificar_cert usuari2
Verificant el certificat usuari2.
O=ORGANITZACIO DE PROVA, OU=DEPARTAMENT DE PROVA, CN=USUARI 2, C=ES, ST=Illes Balears
error 23 at 0 depth lookup: certificate revoked
error ./certs/usuari2.crt: verification failed
Error! Error de validació del certificat ./certs/usuari2.crt (subject=O=ORGANITZACIO DE PROVA, OU=DEPARTAMENT DE PROVA, CN=USUARI 2, C=ES, ST=Illes Balears).
```

`./ac_llistar_certs <[acA | acI]>`

Aquesta comanda mostrarà tots els certificats emesos per l'AC que se li passi com a paràmetre, la qual cosa serà útil per a determinar els certificats emesos, o bé la seva data d'expiració. Aquesta informació s'extreu de la base de dades de cada AC (`./ac/acA/db/acA.db` per a l'AC Arrel o bé `./ac/acI/db/acI.db` per a l'AC Intermedia).


```
manel@blackie: ~/prova/AutoritatCertificacio
manel@blackie:~/prova/AutoritatCertificacio$ ./ac_llistar_certs acI
Certificats a ac/acI/db/acI.db

Número de sèrie..... 01
DN..... /O=ORGANITZACIO DE PROVA/OU=DEPARTAMENT DE COMPTABILITAT/CN=JOHN DOE/C=ES/ST=Illes Balears
Expira..... 13/12/27 17:53:53
Estat..... VALID
Revocació i motiu... No revocat!

Número de sèrie..... 02
DN..... /O=ORGANITZACIO DE PROVA/OU=DEPARTAMENT INFORMATICA/CN=www.intranet.local/C=ES/ST=Illes Balears
Expira..... 15/12/27 17:05:04
Estat..... VALID
Revocació i motiu... No revocat!

Número de sèrie..... 03
DN..... /O=ORGANITZACIO DE PROVA/OU=DEPARTAMENT DE PROVA/CN=USUARI 2/C=ES/ST=Illes Balears
Expira..... 15/12/27 17:17:56
Estat..... REVOCAT
Revocació i motiu... 16/12/23 17:23:05 (cessationOfOperation)

manel@blackie:~/prova/AutoritatCertificacio$
```

`./ac_rm`

Amb aquesta eina s'elimina tot el contingut de l'AC Local, excepte la carpeta arrel. Cal usar-la exclusivament durant el període de proves del sistema, per a esborrar l'AC Local i tornar a executar les tasques inicials.