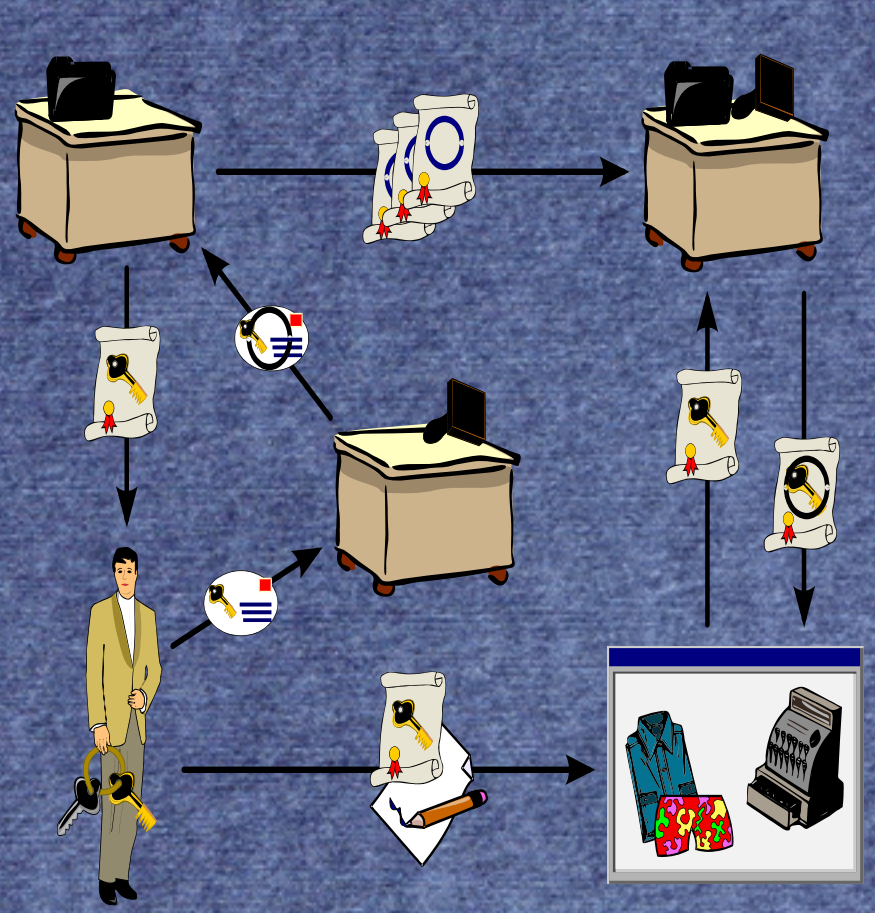
UOC
Enginyeria Tècnica d'Informàtica de Sistemes
TFC

Autoritat de certificació PKI amb serveis en línia

Eugeni Queralt, 15 de juny 2011

Definició i descripció del TFC

- Creacció de l'autoritat de certificació (CA).
- Definir les funcionalitats i serveis.
- Escollir les eines i el suport.
- Disseny de l'aplicació.
- Implementar el problema.



Creació CA

- Eina Openssl
- Cerificat Autosignat
- Funcions de la CA
  - Signar
  - Revocar
  - Emetre
  - Publicar CRL

Definició de funcionalitats

- Requeriments del TFC
  - Peticions
  - Signatura
  - Revocació
  - Llistes de revocació
  - Autenticació
    - Usuaris
    - Administrador

Escollir les eines i el suport

- Ubuntu server
- Apache2
- PHP
- MySQL
- PhpMyAdmin
- Openssl

Execució de l'Openssl

- Funció exec(), paràmetres.
- Permissos d'execució amb visudo

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' com
#
# See the man page for details on how to write a
#

Defaults        env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL
www-data ALL=NOPASSWD: /usr/bin/openssl
```

```
string exec ( string $command [, array &$output [, int &$return_var ]] )
```

Disseny de l'aplicació

- Interfície web

Funcions de seguretat de PHP

- Xifratge de contrasenyes
- Sanejar les entrades dels formularis
- Sessions d'usuari I administrador

Disseny de la BD

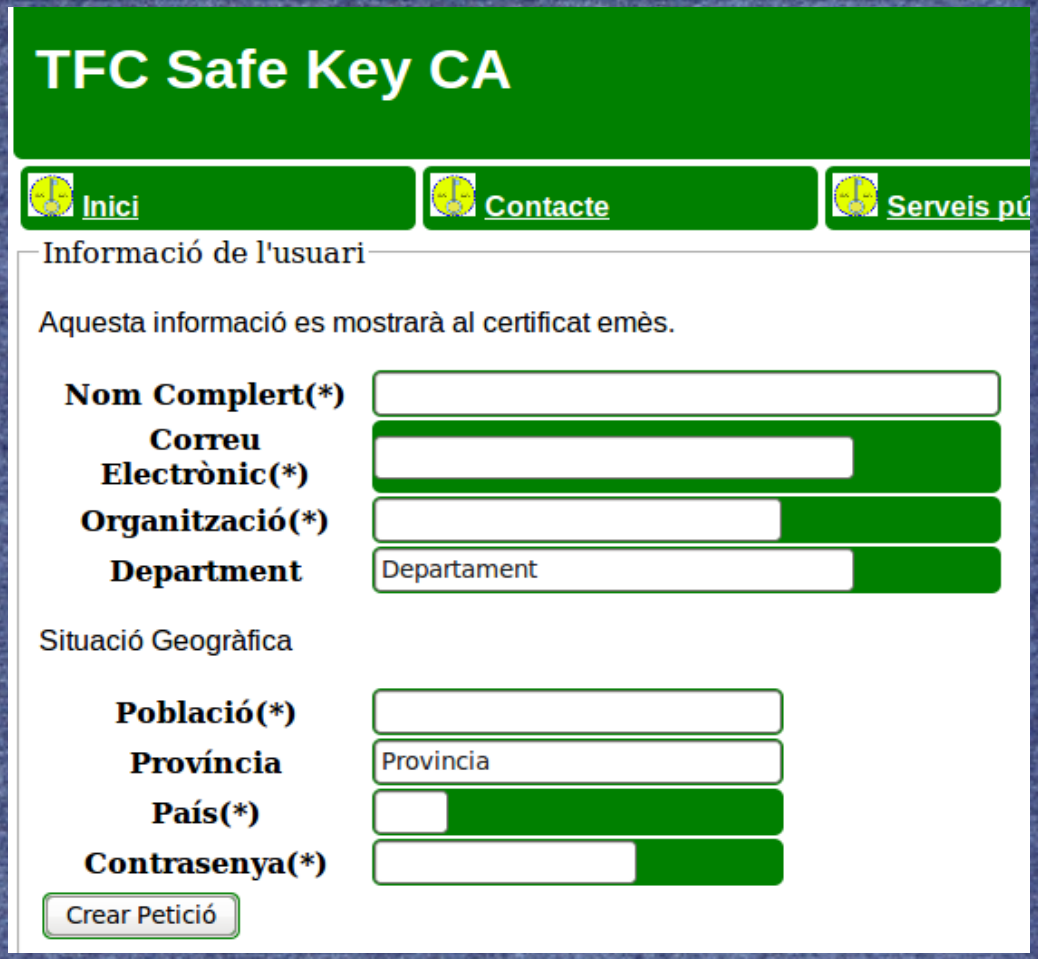
- Estructura de les dades.
- Contrasenyes xifrades.
- PhpMyAdmin. Gestió de la BD.

Configuració de l'Apache

- Modul ssl
- HTTPS
- Regles d'accés al directori web

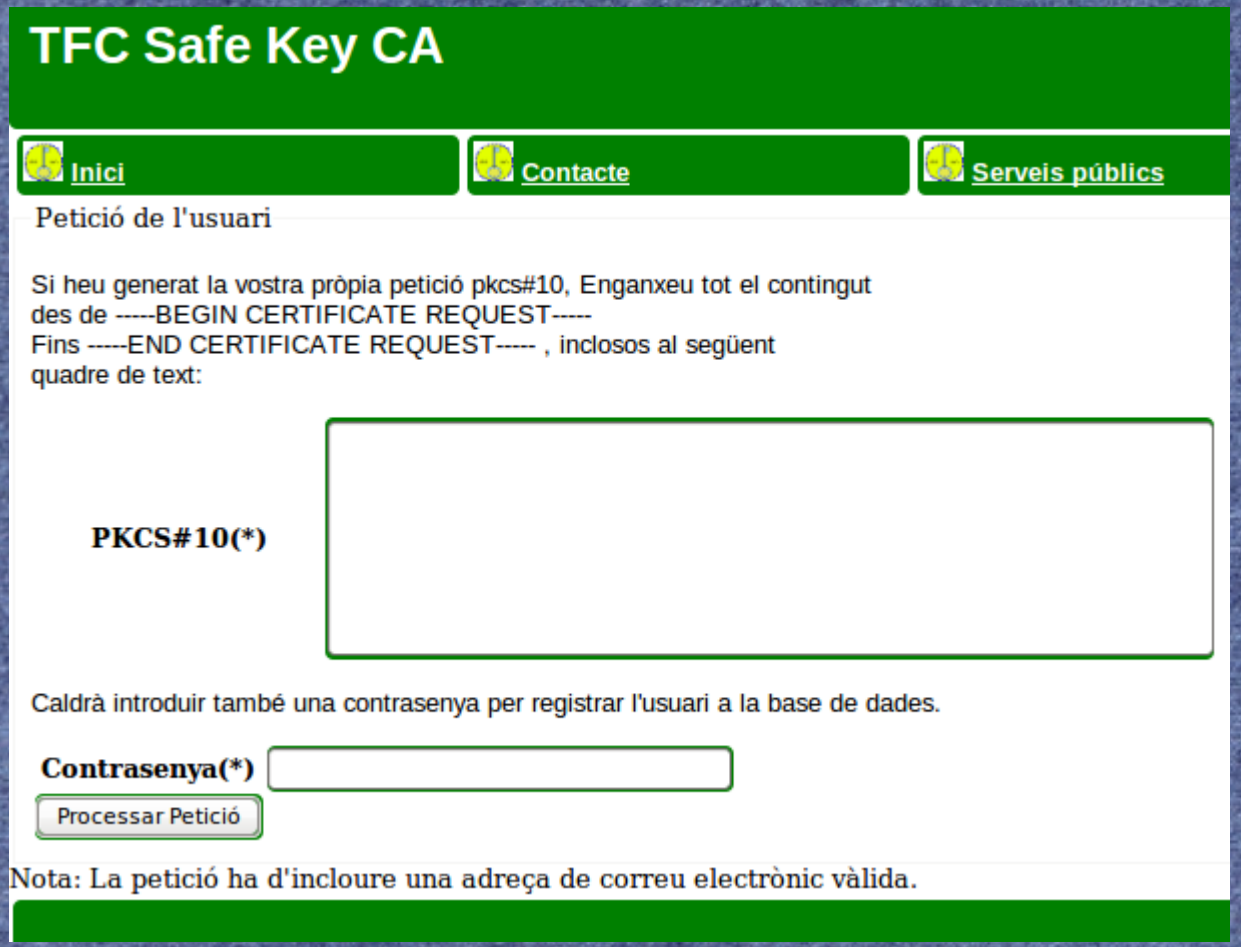
Peticions de signatura

- Generar la clau I la petició



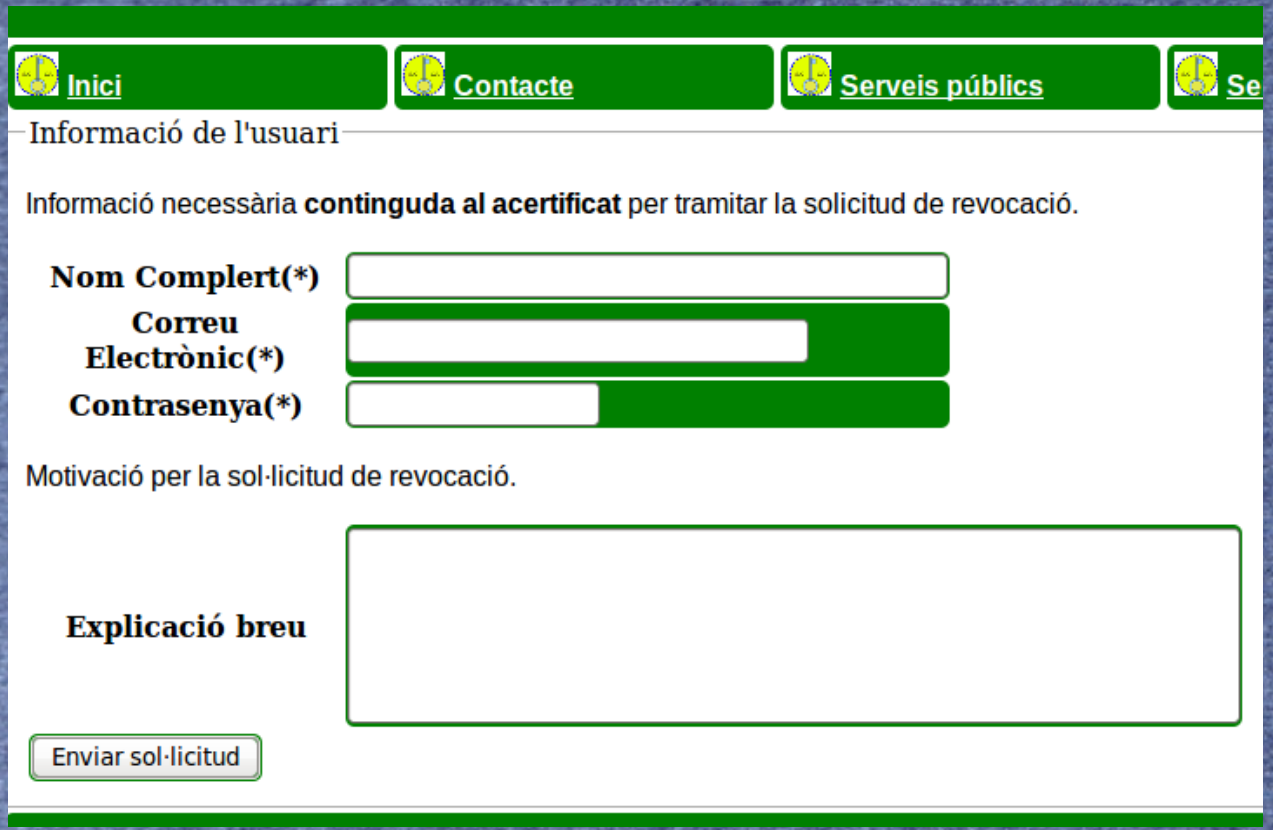
Peticions de signatura

- Processar la petició de l'usuari



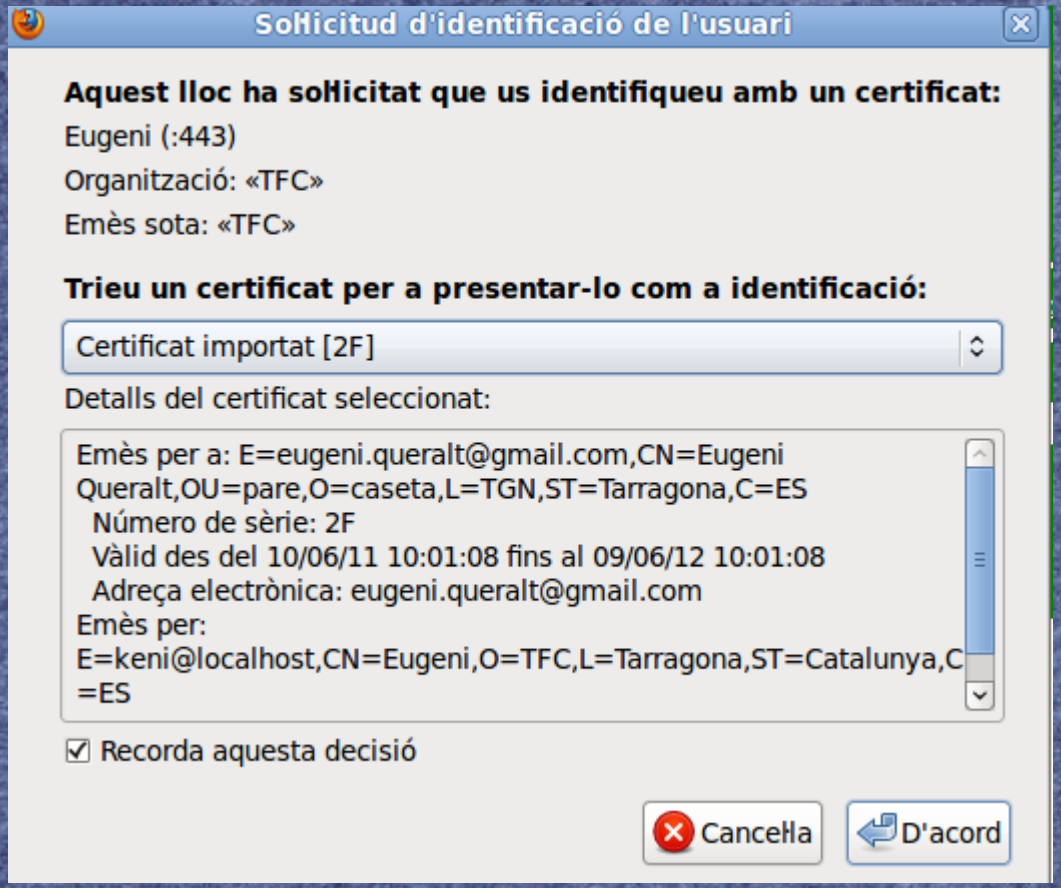
Sol·licitar la revocació

- Autenticació dels usuaris
- Trametre la sol·licitud



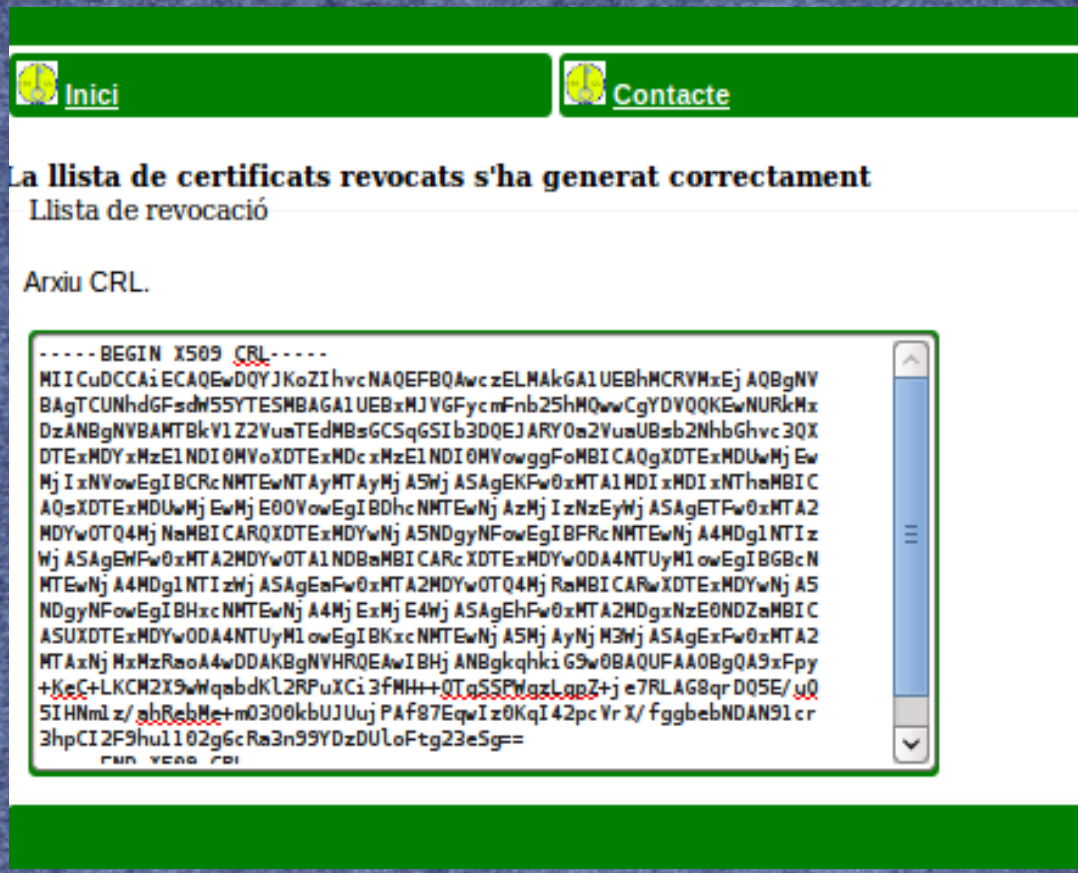
Revocació de certificats

- Autenticació de l'administrador amb certificat de client.
- Llista de selecció per revocar els certificats.



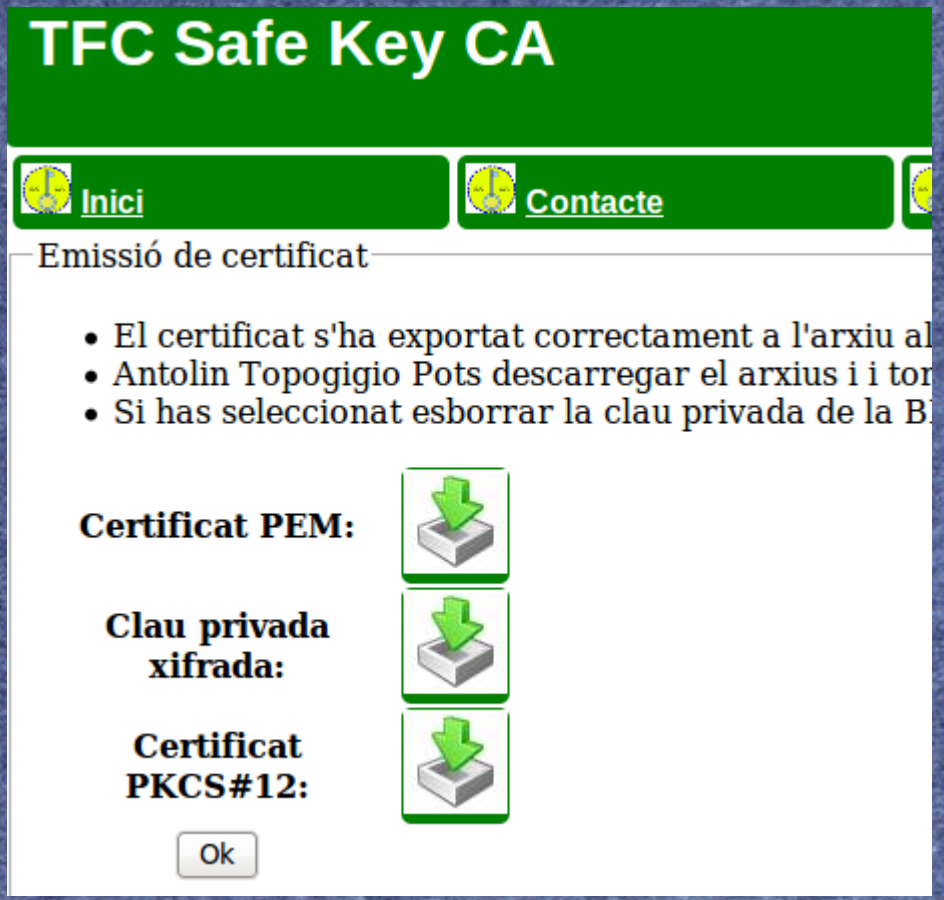
Generar la llista de revocació

- Autenticació de l'usuari administrador.
- Generació de la llista de revocació per part de l'administrador.



Emissió de certificats i de claus

- Autenticació del usuaris amb certificat
- Descàrrega dels certificats.
- Importació dels certificats al navegador



Publicació de la llista de revocació

- Genaració de la llista I descàrrega.

Juanito Valderrana	Zapateao.com	keni@localhost.local.lan
Cipriano Frutero	frutas SA	keni@localhost.local.lan

Arxiu CRL.

```
-----BEGIN X509 CRL-----
MIICuDCCAiECAQEwDQYJKoZIhvcNAQEFBQAwczELMAkGA1UEBhMCRVMxEjAQBgNV
BAgTCUNhdGFsdW55YTESMBAGA1UEBxMJVGFycmFnb25hMQwwCgYDVQQKEwNURkMx
DzANBgNVBAMTBkV1Z2YuaTEdMBsGCSqGSIb3DQEJARYOa2VuaUBsb2NhbGhvc3QX
DTExMDYxMDE2MzE1M1oXDTExMDcxMDE2MzE1M1owggFoMBICAQgXDTExMDUwMjEw
MjIxNVowEgIBCRcNMTEwNTAyMTAyMjA5WjASAgEKFw0xMTA1MDIxMDIxNThaMBIC
AQsXDTExMDUwMjEwMjE0OVowEgIBDhcNMTEwNjAzMjIzNzEyWjASAgETFw0xMTA2
MDYwOTQ4MjNaMBICARQXDTExMDYwNjA5NDgyNFowEgIBFRcNMTEwNjA4MDglNTIz
WjASAgEWFw0xMTA2MDYwOTA1NDBaMBICARcXDTExMDYwODA4NTUyM1owEgIBGBcN
MTEwNjA4MDglNTIzWjASAgEaFw0xMTA2MDYwOTQ4MjRaMBICARwXDTExMDYwNjA5
NDgyNFowEgIBHxcNMTEwNjA4MjExMjE4WjASAgEhFw0xMTA2MDgxNzE0NDZaMBIC
ASUXDTExMDYwODA4NTUyM1owEgIBKxcNMTEwNjA5MjAyNjM3WjASAgExFw0xMTA2
MTAxNjMxMzRaoA4wDDAKBgNVHRQEAwIBHTANBgkqhkiG9w0BAQUFAA0BgQA3A4hq
0/rxUPkY24GNHbbJdtWr69iEuPME/BMY60fwBZr/F+ihH3P7gMuGpwokWCW4J3a3
p+CrSuiaVhZoM8HSRKVzCQoencCzDSfDb2Exu8t8NiZy0VRWqJU8mWwsow8HK3aU
RSc01u90g04zh85ioHKjORtWjcFRW+n/WbxtiQ==
-----END X509 CRL-----
```