

UOC

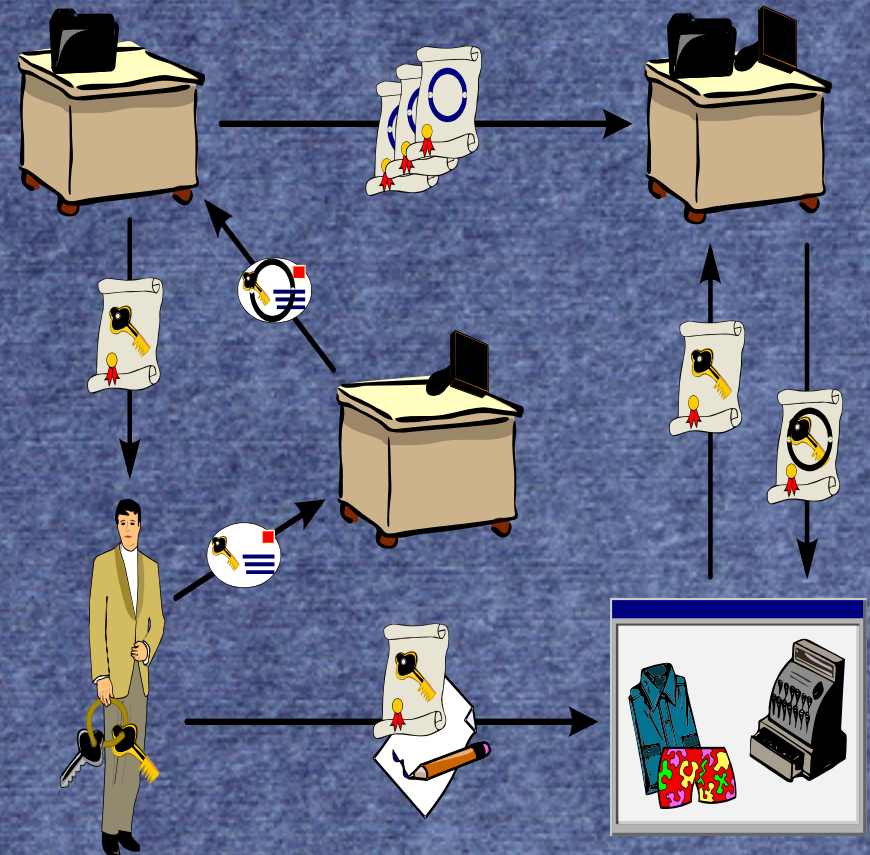
**Enginyeria Tècnica d'Informàtica de Sistemes
TFC**

**Autoritat de certificació PKI amb serveis
en línia**

Eugeni Queralt, 15 de juny 2011

Definició i descripció del TFC

- Creació 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
- Certificat 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' command
# 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

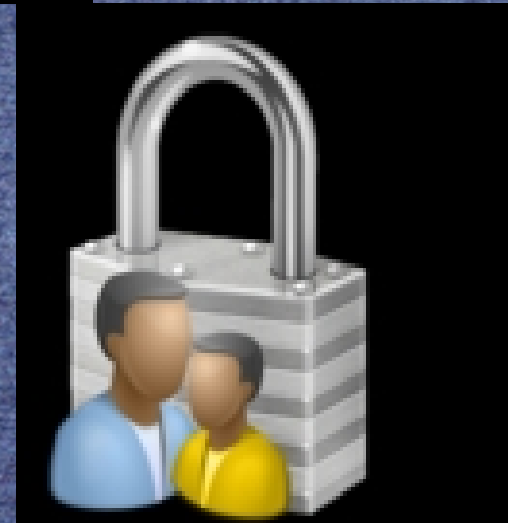
- Interfície web



The screenshot shows the web application interface for TFC Safe Key CA. It features a green header with a logo (a yellow circle with a key and 'SK CA') and the text 'TFC Safe Key CA'. Below the header is a navigation bar with five buttons: 'Inici', 'Contacte', 'Serveis públics', 'Serveis amb certificat', and 'Administrador'. The main content area contains a paragraph of text: 'CA SK, és una autoritat de certificació creada per donar una sèrie de serveis de signatura de certificats i autenticació en línia. Tant per les tasques administratives (**Administrador**) com per als **Serveis amb certificat** es demana una autenticació a través del certificat de client corresponent.' At the bottom, there is a footer with the text 'TFC Safe Key CA Ltd.', a Creative Commons Attribution 3.0 Unported License logo, and the text 'This work is licensed under a [Creative Commons Attribution 3.0 Unported License](#).'

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.
- Contrasenyas xifrades.
- PhpMyAdmin. Gestió de la BD.



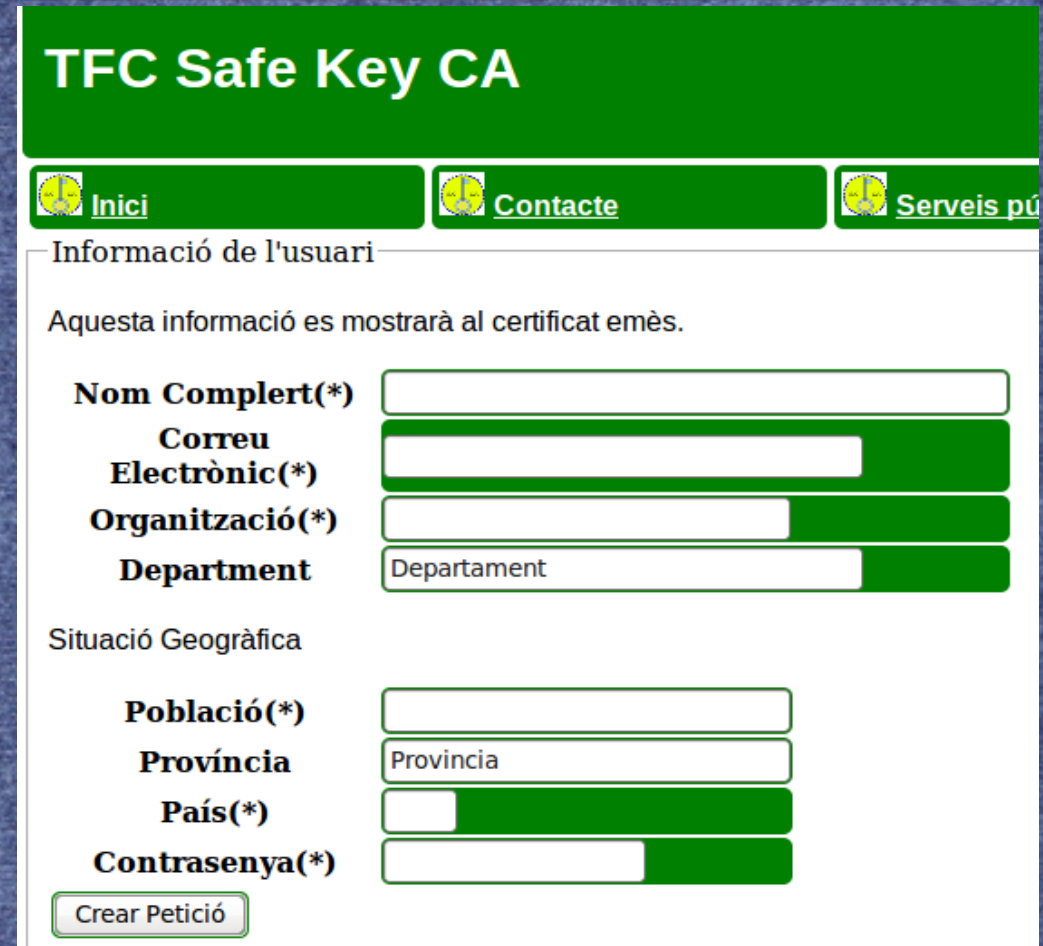
Configuració de l'Apache

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



Peticions de signatura

- Generar la clau I la petició



TFC Safe Key CA

[Inici](#) [Contacte](#) [Serveis públics](#)

Informació de l'usuari

Aquesta informació es mostrarà al certificat emès.

Nom Complet(*)

Correu Electrònic(*)

Organització(*)

Department

Situació Geogràfica

Població(*)

Província

País(*)

Contrasenya(*)

Peticions de signatura

- Processar la petició de l'usuari

TFC Safe Key CA

[Inici](#) [Contacte](#) [Serveis públics](#)

Petició de l'usuari

Si heu generat la vostra pròpia petició pkcs#10, Enganxeu tot el contingut des de -----BEGIN CERTIFICATE REQUEST----- Fins -----END CERTIFICATE REQUEST----- , inclosos al següent quadre de text:

PKCS#10(*)

Caldrà introduir també una contrasenya per registrar l'usuari a la base de dades.

Contrasenya(*)

Nota: La petició ha d'incloure una adreça de correu electrònic vàlida.

Sol·licitar la revocació

- Autenticació dels usuaris
- Trametre la sol·licitud

[Inici](#) [Contacte](#) [Serveis públics](#) [Se](#)

Informació de l'usuari

Informació necessària **continguda al certificat** per tramitar la sol·licitud de revocació.

Nom Complert(*)

Correu Electrònic(*)

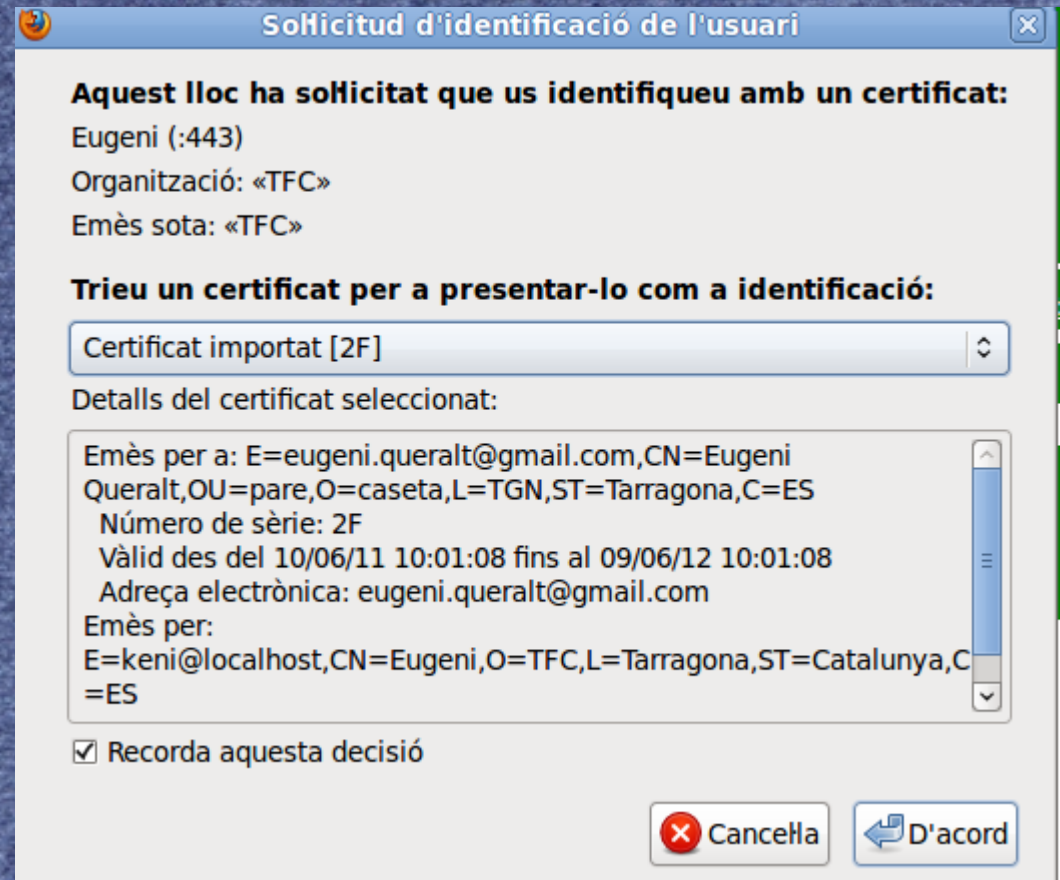
Contrasenya(*)

Motivació per la sol·licitud de revocació.

Explicació breu

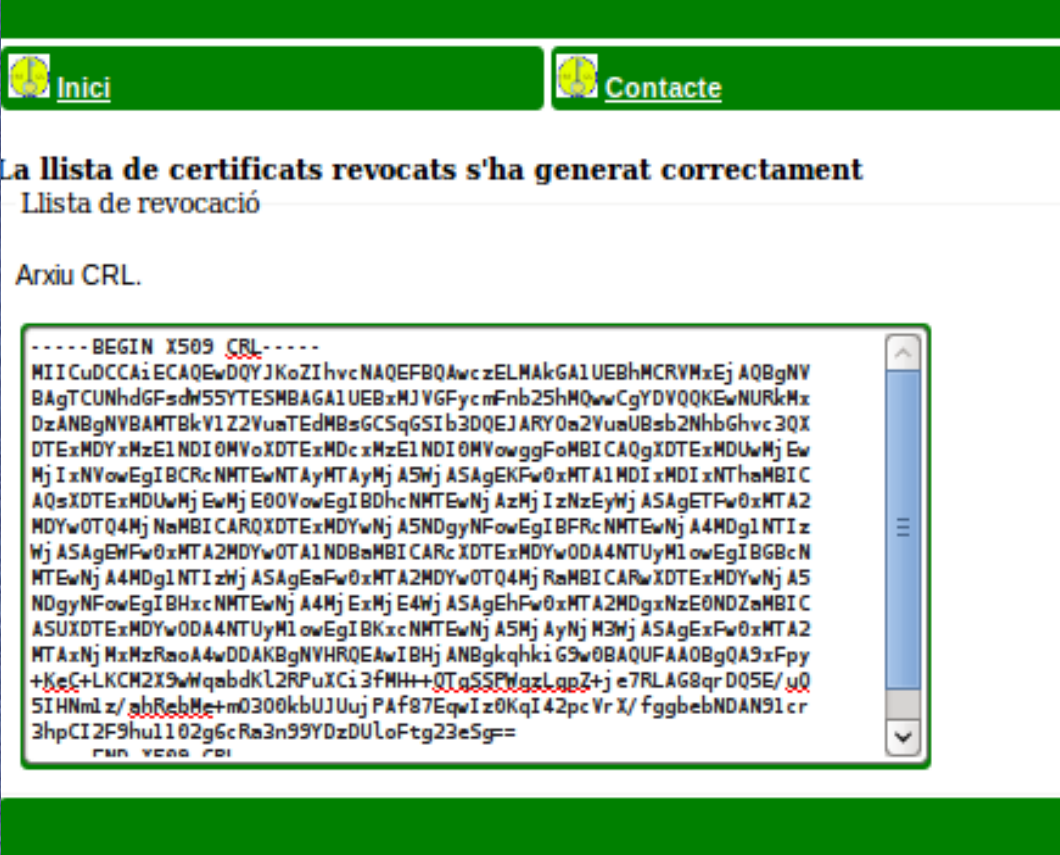
Revocació de certificats

- 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.



The screenshot shows a web application interface with a green header. On the left, there is a button labeled "Inici" with a yellow icon. On the right, there is a button labeled "Contacte" with a yellow icon. Below the header, a message reads: "La llista de certificats revocats s'ha generat correctament" (The list of revoked certificates has been generated correctly). Underneath, it says "Llista de revocació" (Revocation list) and "Arxiu CRL." (CRL file). A text area displays the content of the CRL file, starting with "-----BEGIN X509 CRL-----" and ending with "-----". The text contains various alphanumeric strings and symbols, including "MII", "CuDCCA", "E", "CAQ", "E", "w", "D", "Q", "Y", "J", "K", "o", "Z", "I", "h", "v", "c", "N", "A", "Q", "E", "F", "B", "Q", "A", "w", "c", "z", "E", "L", "M", "A", "k", "G", "A", "1", "U", "E", "B", "H", "M", "C", "R", "V", "M", "x", "E", "j", "A", "Q", "B", "g", "N", "V", "B", "A", "g", "T", "C", "U", "N", "h", "d", "G", "F", "s", "d", "W", "S", "Y", "T", "E", "S", "M", "B", "A", "G", "A", "1", "U", "E", "B", "x", "M", "J", "Y", "G", "F", "y", "c", "m", "F", "n", "b", "2", "5", "h", "M", "Q", "w", "w", "C", "g", "Y", "D", "V", "Q", "Q", "E", "w", "N", "U", "R", "k", "M", "x", "D", "z", "A", "N", "B", "g", "N", "V", "B", "A", "M", "T", "B", "k", "V", "1", "Z", "2", "V", "u", "a", "T", "E", "d", "M", "B", "s", "G", "C", "S", "q", "G", "S", "I", "b", "3", "D", "Q", "E", "J", "A", "R", "Y", "0", "a", "2", "Y", "u", "a", "U", "B", "s", "b", "2", "N", "h", "b", "G", "h", "v", "c", "3", "Q", "X", "D", "T", "E", "x", "M", "D", "Y", "x", "M", "z", "E", "1", "N", "D", "I", "0", "M", "V", "o", "X", "D", "T", "E", "x", "M", "D", "c", "x", "M", "z", "E", "1", "N", "D", "I", "0", "M", "V", "o", "w", "g", "g", "F", "o", "M", "B", "I", "C", "A", "Q", "g", "X", "D", "T", "E", "x", "M", "D", "U", "w", "M", "j", "E", "w", "M", "j", "I", "x", "N", "V", "o", "w", "E", "g", "I", "B", "C", "R", "c", "N", "M", "T", "E", "w", "N", "T", "A", "y", "M", "T", "A", "y", "M", "j", "A", "5", "M", "j", "A", "S", "A", "g", "E", "K", "F", "w", "0", "x", "M", "T", "A", "1", "M", "D", "I", "x", "M", "D", "I", "x", "N", "T", "h", "M", "B", "I", "C", "A", "Q", "s", "X", "D", "T", "E", "x", "M", "D", "U", "w", "M", "j", "E", "w", "M", "j", "E", "0", "0", "Y", "o", "w", "E", "g", "I", "B", "D", "h", "c", "N", "M", "T", "E", "w", "N", "j", "A", "z", "M", "j", "I", "z", "N", "z", "E", "y", "M", "j", "A", "S", "A", "g", "E", "T", "F", "w", "0", "x", "M", "T", "A", "2", "M", "D", "Y", "w", "0", "T", "Q", "4", "M", "j", "N", "a", "M", "B", "I", "C", "A", "R", "Q", "X", "D", "T", "E", "x", "M", "D", "Y", "w", "N", "j", "A", "5", "N", "D", "g", "y", "N", "F", "o", "w", "E", "g", "I", "B", "F", "R", "c", "N", "M", "T", "E", "w", "N", "j", "A", "4", "M", "D", "g", "1", "N", "T", "I", "z", "W", "j", "A", "S", "A", "g", "E", "H", "F", "w", "0", "x", "M", "T", "A", "2", "M", "D", "Y", "w", "0", "T", "A", "1", "N", "D", "B", "a", "M", "B", "I", "C", "A", "R", "c", "X", "D", "T", "E", "x", "M", "D", "Y", "w", "0", "D", "A", "4", "N", "T", "U", "y", "M", "1", "o", "w", "E", "g", "I", "B", "G", "B", "c", "N", "M", "T", "E", "w", "N", "j", "A", "4", "M", "D", "g", "1", "N", "T", "I", "z", "W", "j", "A", "S", "A", "g", "E", "a", "F", "w", "0", "x", "M", "T", "A", "2", "M", "D", "Y", "w", "0", "T", "Q", "4", "M", "j", "R", "a", "M", "B", "I", "C", "A", "R", "w", "X", "D", "T", "E", "x", "M", "D", "Y", "w", "N", "j", "A", "5", "N", "D", "g", "y", "N", "F", "o", "w", "E", "g", "I", "B", "H", "x", "c", "N", "M", "T", "E", "w", "N", "j", "A", "4", "M", "j", "E", "x", "M", "j", "E", "4", "M", "j", "A", "S", "A", "g", "E", "h", "F", "w", "0", "x", "M", "T", "A", "2", "M", "D", "g", "x", "N", "z", "E", "0", "N", "D", "z", "a", "M", "B", "I", "C", "A", "S", "U", "X", "D", "T", "E", "x", "M", "D", "Y", "w", "0", "D", "A", "4", "N", "T", "U", "y", "M", "1", "o", "w", "E", "g", "I", "B", "K", "x", "c", "N", "M", "T", "E", "w", "N", "j", "A", "5", "M", "j", "A", "y", "N", "j", "M", "3", "M", "j", "A", "S", "A", "g", "E", "x", "F", "w", "0", "x", "M", "T", "A", "2", "M", "T", "A", "x", "N", "j", "M", "x", "M", "z", "R", "a", "o", "A", "4", "w", "D", "D", "A", "K", "B", "g", "N", "V", "H", "R", "Q", "E", "A", "w", "I", "B", "h", "j", "A", "N", "B", "g", "k", "q", "h", "k", "i", "G", "9", "w", "0", "B", "A", "Q", "U", "F", "A", "A", "O", "B", "g", "Q", "A", "9", "x", "F", "p", "y", "+", "K", "c", "C", "+", "L", "K", "C", "M", "2", "X", "9", "w", "q", "a", "b", "d", "K", "L", "2", "R", "P", "u", "X", "C", "i", "3", "F", "M", "H", "+", "Q", "T", "q", "S", "S", "F", "w", "z", "L", "q", "p", "Z", "+", "j", "e", "7", "R", "L", "A", "G", "8", "q", "r", "D", "0", "5", "E", "w", "u", "Q", "S", "I", "H", "N", "m", "l", "z", "a", "b", "R", "e", "b", "M", "e", "m", "0", "3", "0", "0", "k", "b", "U", "J", "U", "u", "j", "P", "A", "F", "0", "7", "E", "q", "w", "I", "z", "0", "K", "q", "I", "4", "2", "p", "c", "V", "r", "X", "f", "g", "g", "b", "e", "b", "N", "D", "A", "N", "9", "1", "c", "r", "3", "h", "p", "C", "I", "2", "F", "9", "h", "u", "1", "1", "0", "2", "g", "6", "c", "R", "a", "3", "n", "9", "9", "Y", "D", "z", "D", "U", "L", "o", "F", "t", "g", "2", "3", "e", "5", "g", "f", "="

Emissió de certificats i de claus

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



