Seguridad en Redes

Confianza entre organizaciones

Certificación Cruzada

Ingeniero Edy Javier Milla
Edy.milla@gmail.com

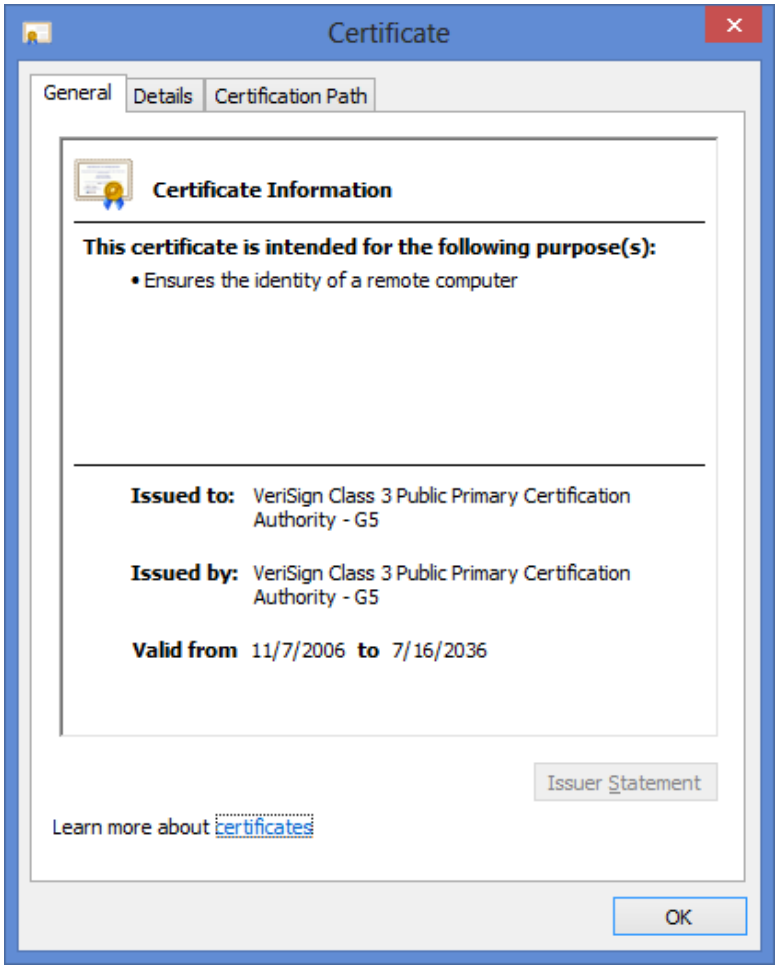
Infraestructura de clave pública (PKI) en las organizaciones

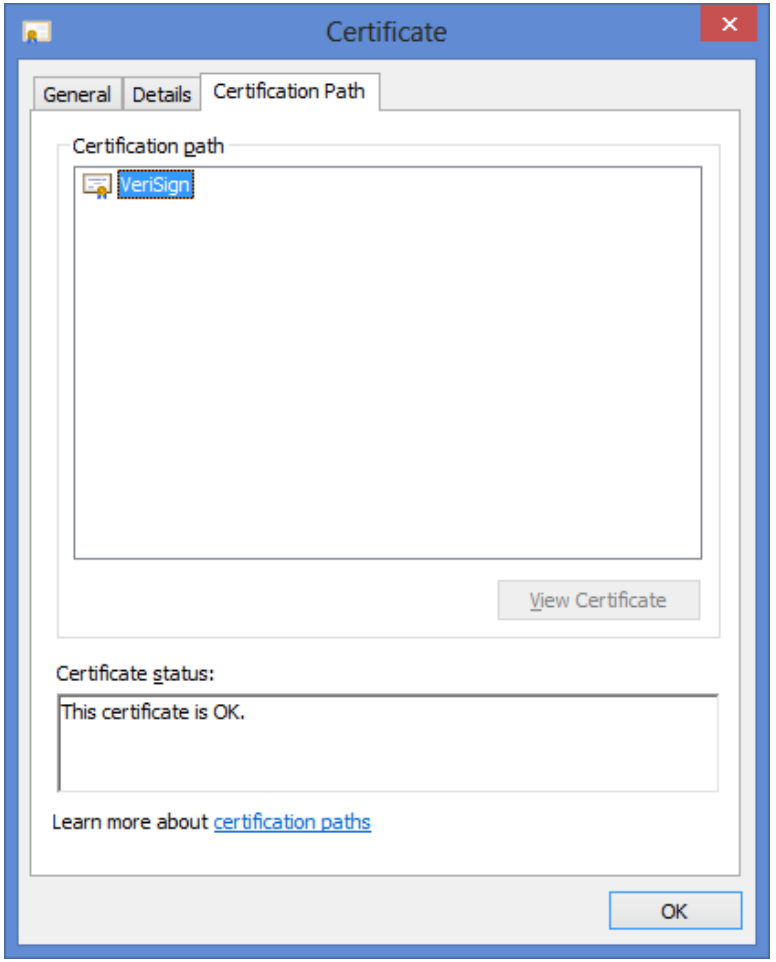
- Organizaciones están utilizando certificados digitales.
- Confiabilidad, Integridad y no Repudio.
- Utilizan Autoridades Certificantes propias.
- Validez a lo interno de la organización.
- Políticas, Normas y Procedimientos.

Implementaciones PKI

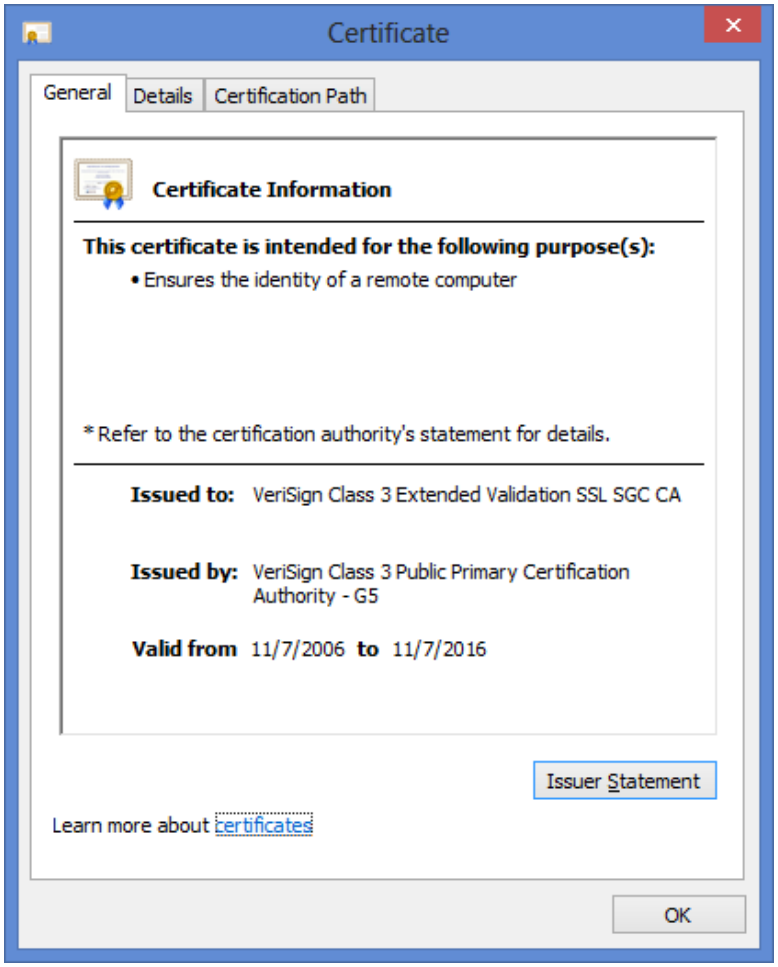
- Autoridades Certificantes Raíz
  - Certificado Autofirmado (selfsign)
  - Inicio de la confianza.
- Autoridades Certificantes Subordinadas
  - Se establecen políticas.
  - Firman CA’s de nivel jerárquico inferior
- Autoridades Certificantes Operativas
  - Emiten certificados para entidades finales
    - Usuarios
    - Equipos

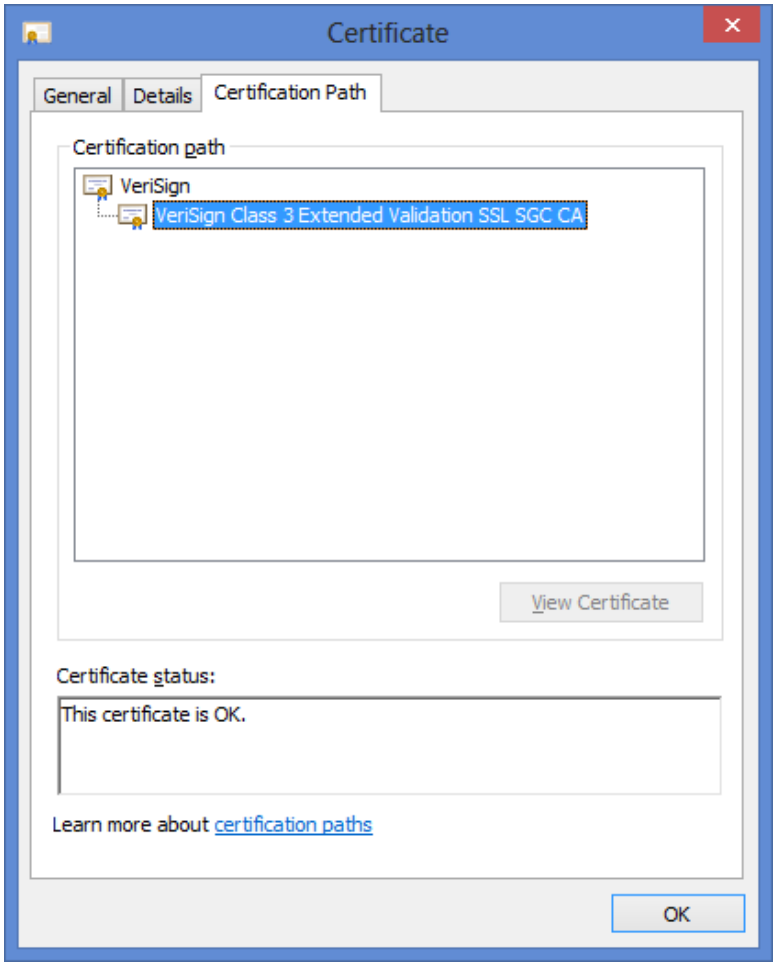
Autoridad Certificante Verisign Raiz





Autoridad Certificante Verisign subordinada





Autoridades Certificantes (AC)

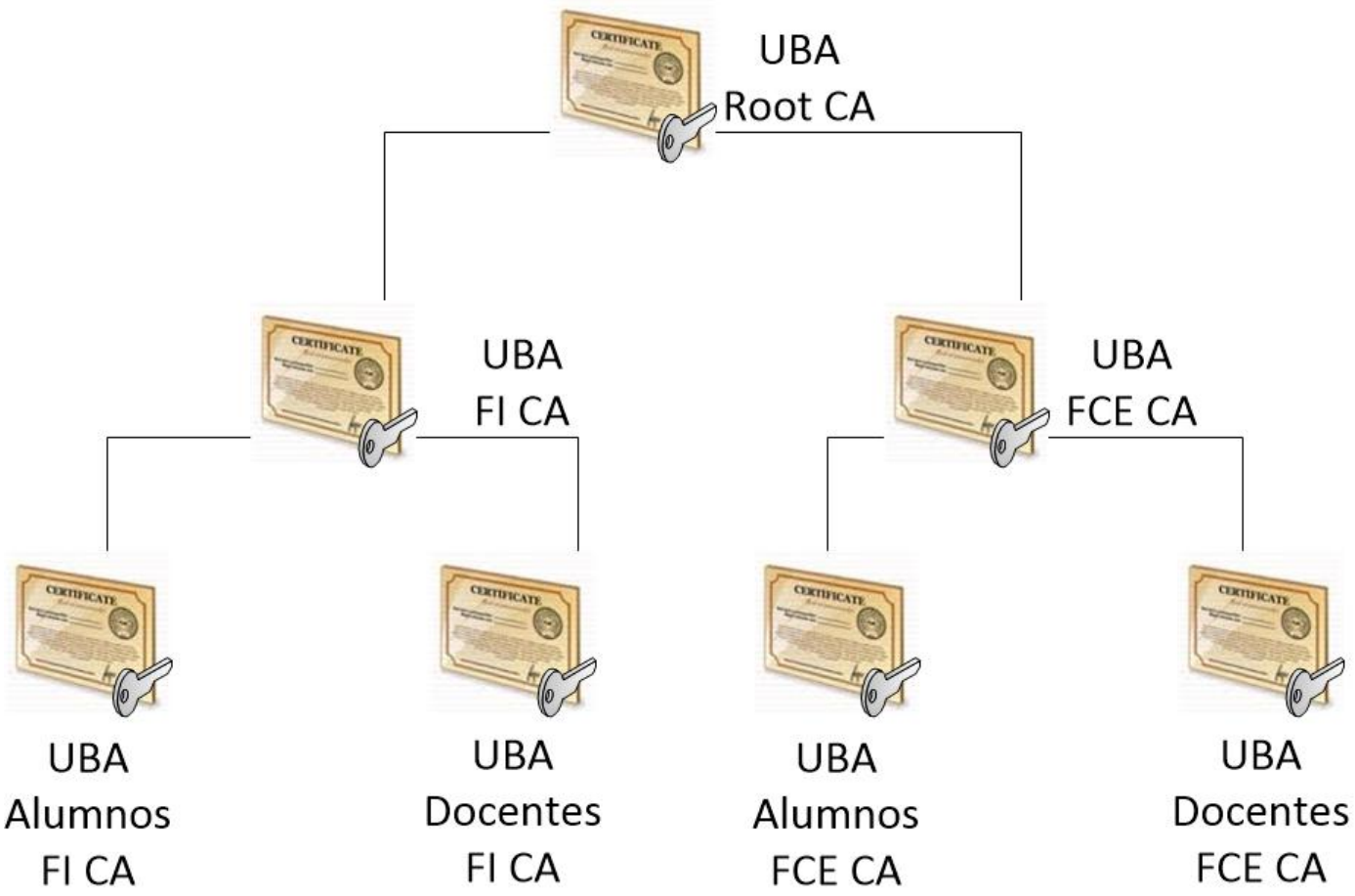
- Los certificados son firmados por las AC
- Esencialmente una AC es un tercero en el que se confía para verificar los atributos del certificado.
- El beneficio de los certificados y ACs se obtienen cuando dos entidades confían en la misma AC.
- Una AC es responsable de verificar la identidad de un solicitante antes de emitir un certificado.
- La llave publica de las ACs son distribuidas en los navegadores o pueden ser importadas manualmente.

Modelos de confianza

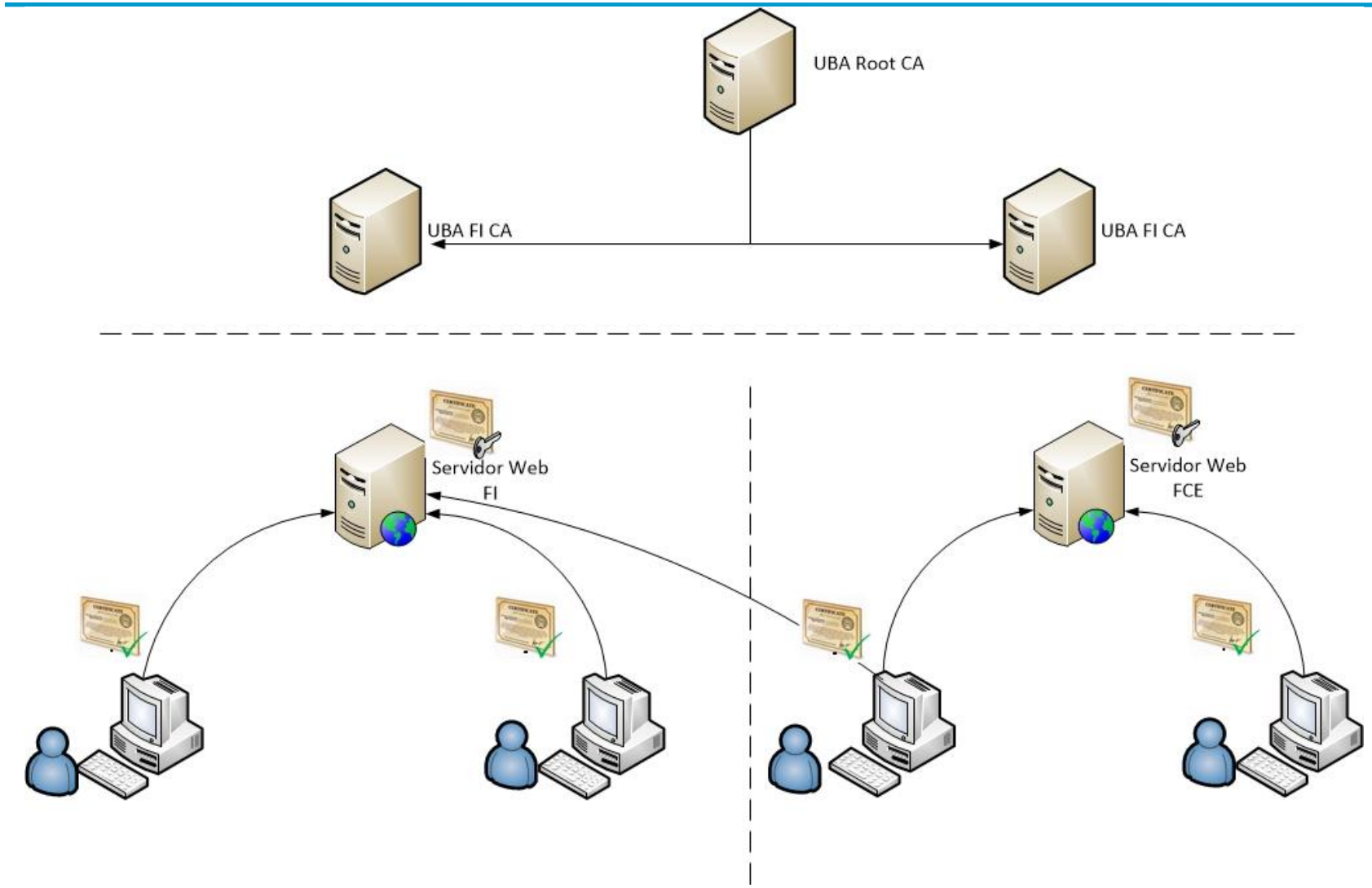
Modelo Jerárquico: Una CA delega la autoridad de emitir certificados a una CA subordinada las cuales pueden delegar la autoridad a otras CA subordinadas.

Modelo Certificación Cruzada: Permite que entidades en una PKI confíen en otras entidades que tiene su propia PKI.

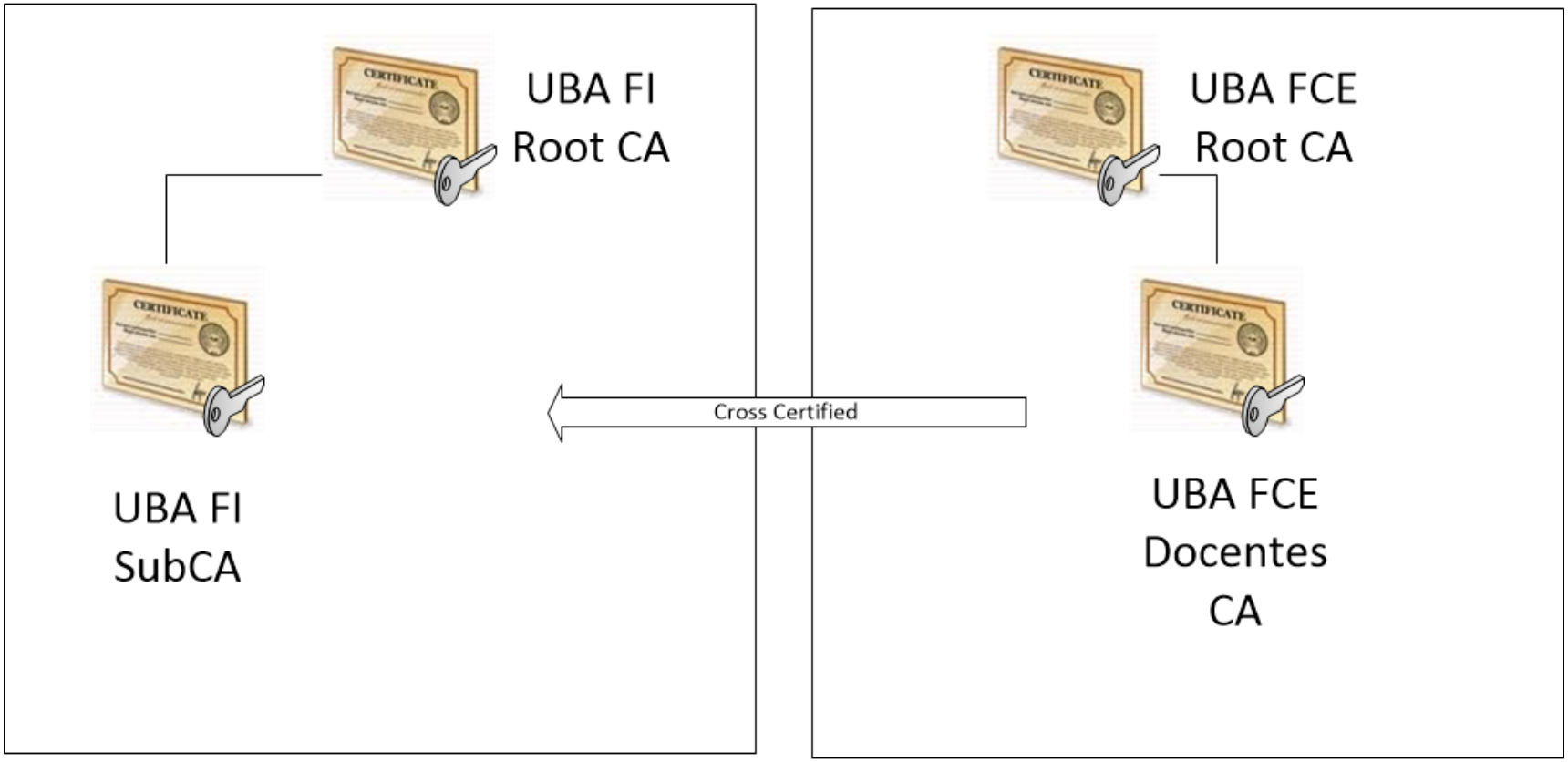
Modelo Jerárquico



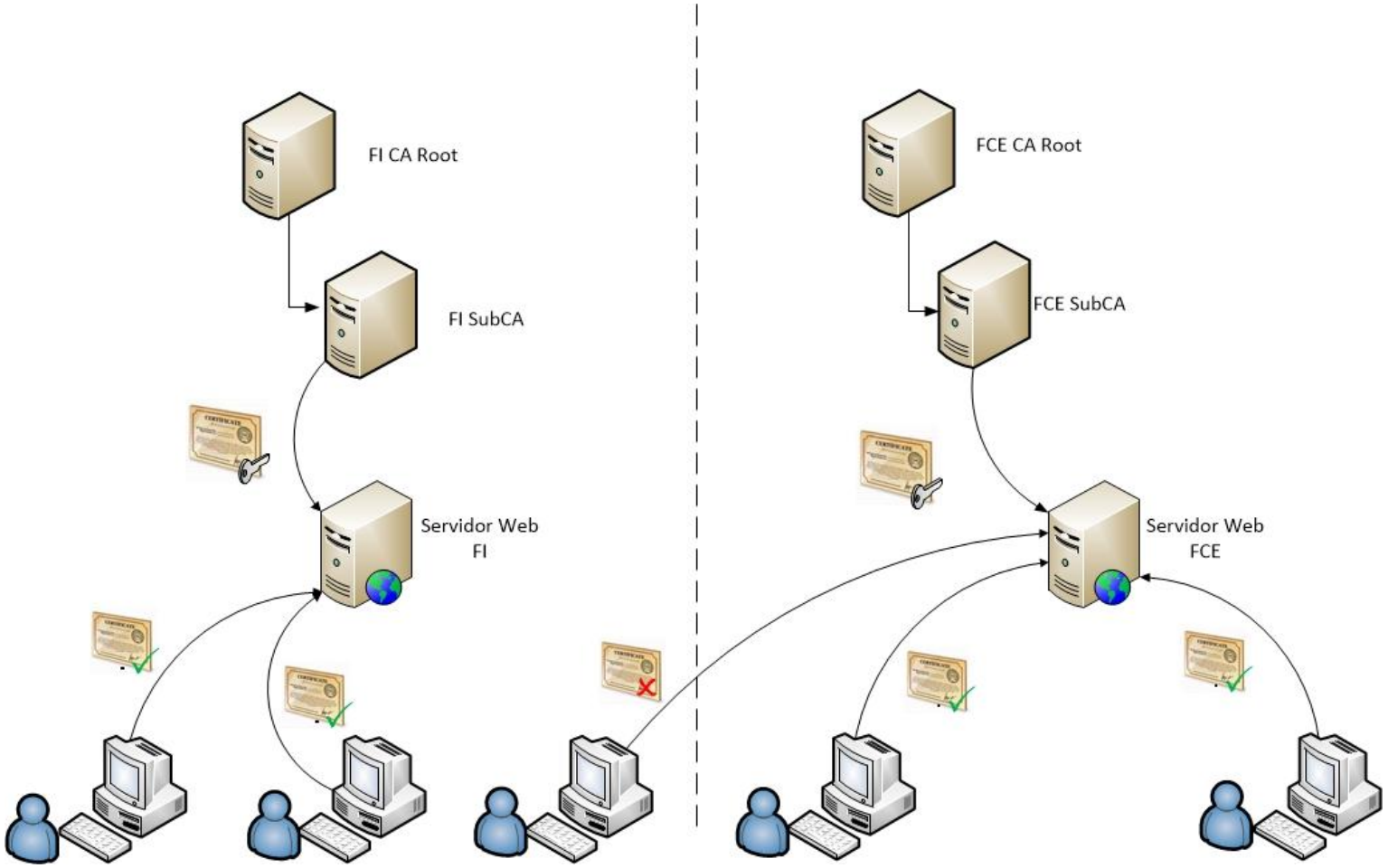
Modelo Jerárquico



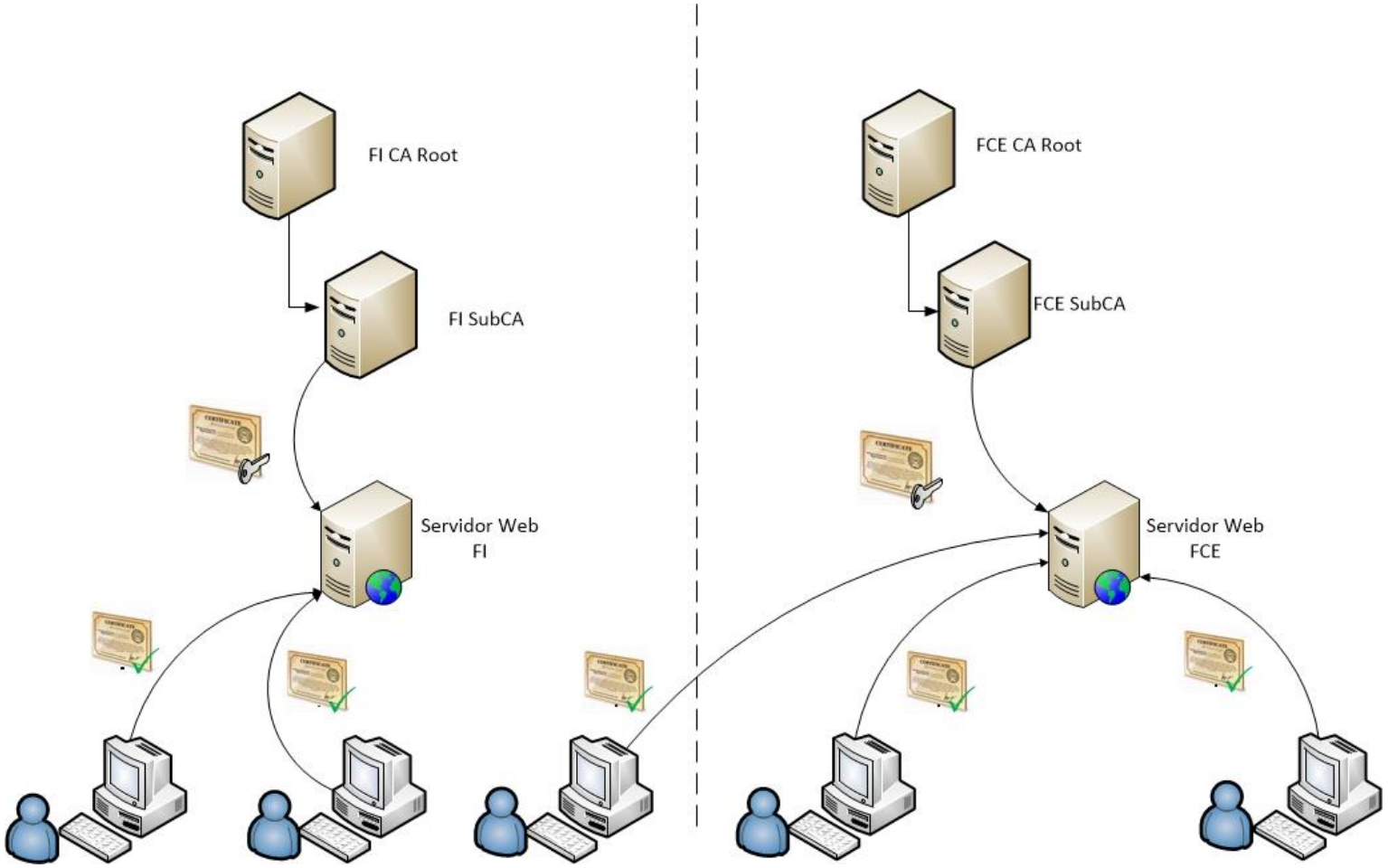
Modelo Certificación Cruzada



Modelo Certificación Cruzada



Modelo Certificación Cruzada



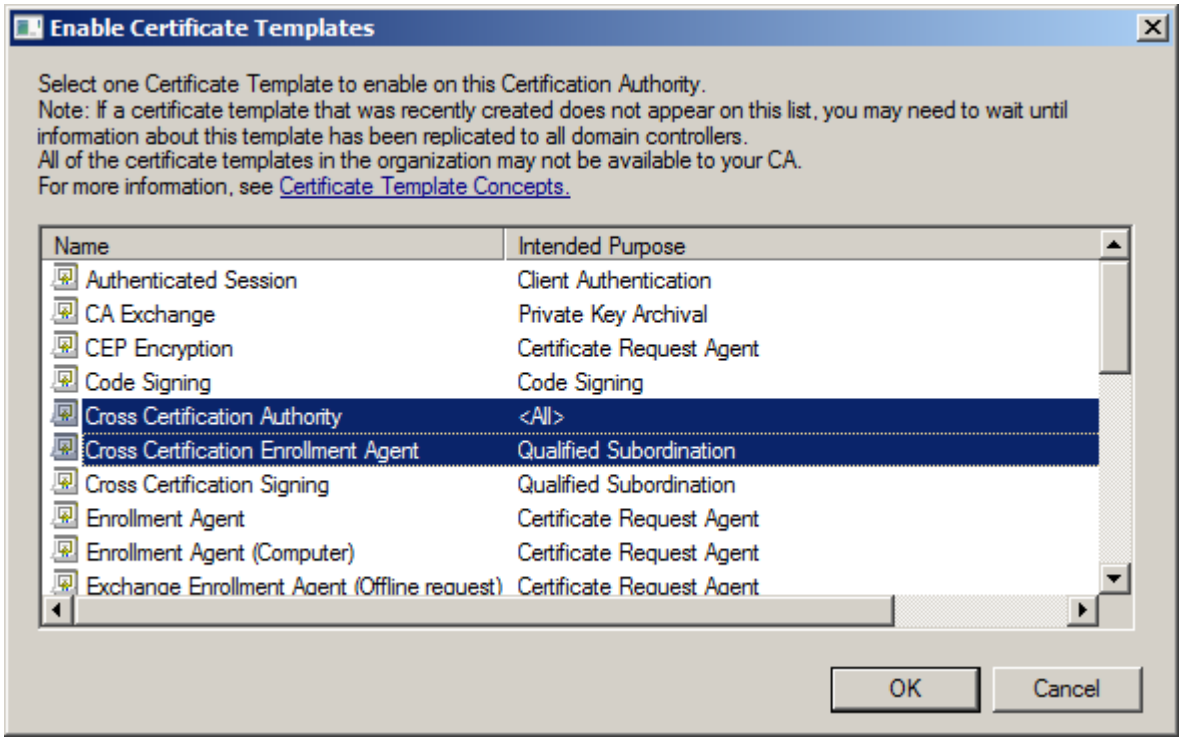
Interoperabilidad

- Las AC emiten certificados de acuerdo a un estándar (X.509)
- Posibilidad de interoperabilidad entre diferentes AC.
- Windows AC vs EJBCA AC
- Windows AC vs OpenSSL AC

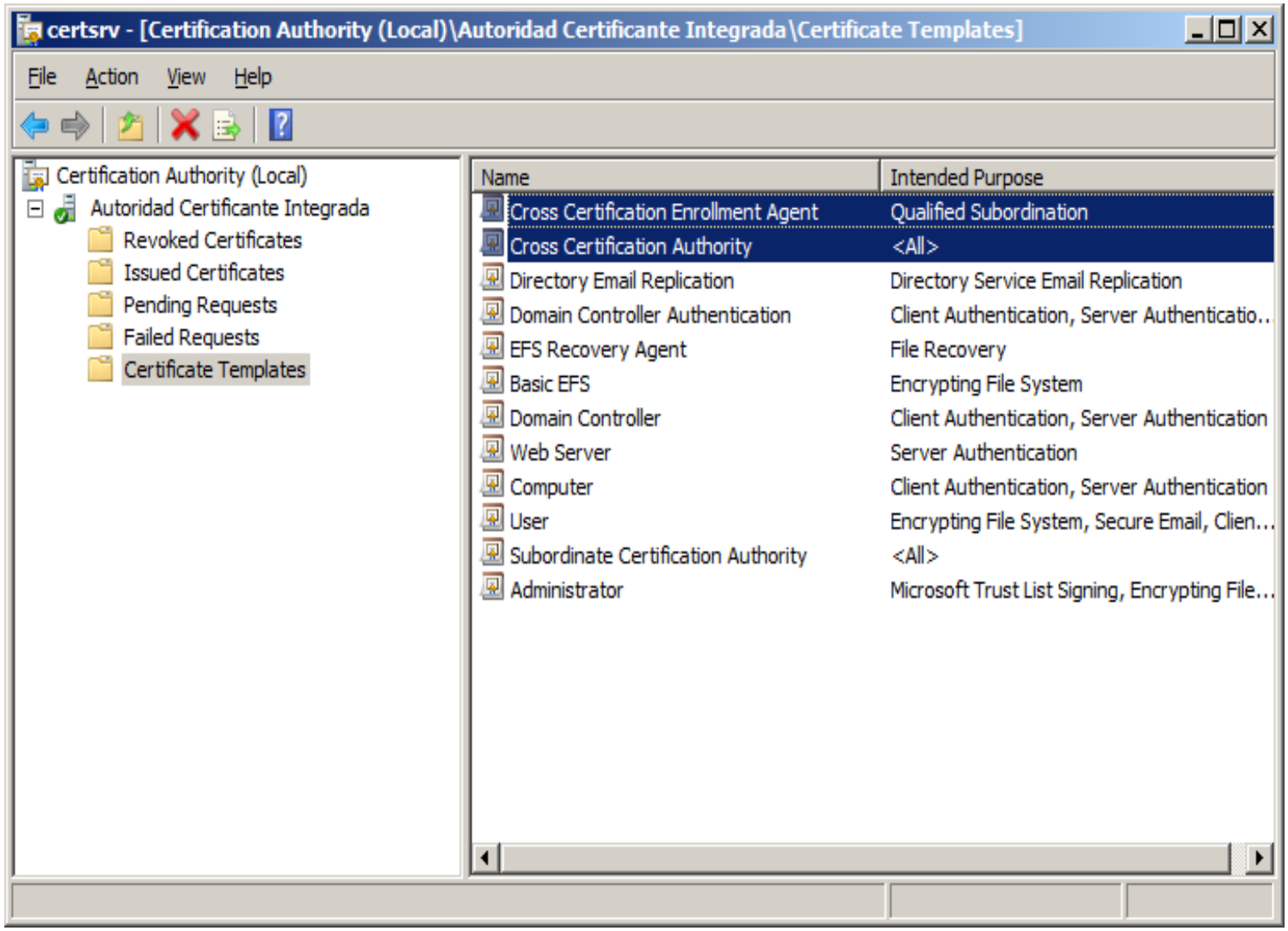
Flujo de proceso de firmado de un certificado para Certificación cruzada

- Crear/agregar de la plantilla del Agente para la solicitud de firmado.
- Incorporación de plantillas Cross Certification Signing y Cross Certificate Authority a la lista de emisión de certificados.
- Emisión del certificado para el Agente Cross Certification Enrollment Agent
- Creación y parametrización del archivo de políticas de certificación (policy.inf)
- Proceso de generación y firmado de la solicitud del certificado (CSR)
- Emisión del certificado cruzado (firmado de la solicitud con la llave privada de la Autoridad Certificante).

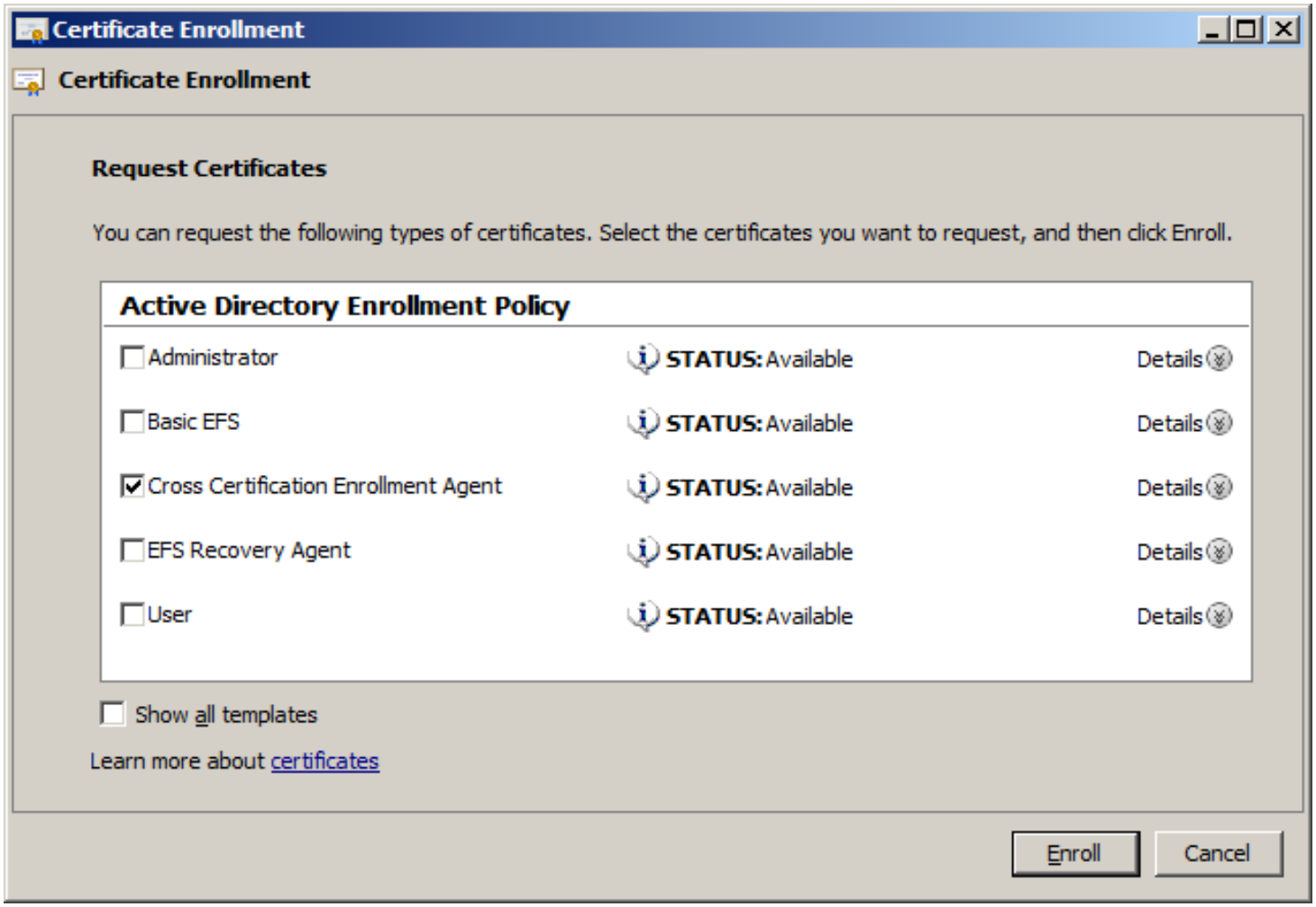
Crear/agregar de la plantilla del Agente para la solicitud de firmado



Incorporación de plantillas Cross Certification Signing y Cross Certificate Authority a la lista de emisión de certificados



Emisión del certificado para el Agente Cross Certification Enrollment Agent



Creación y parametrización del archivo de políticas de certificación (policy.inf)

Policy.inf - Notepad

File Edit Format View Help

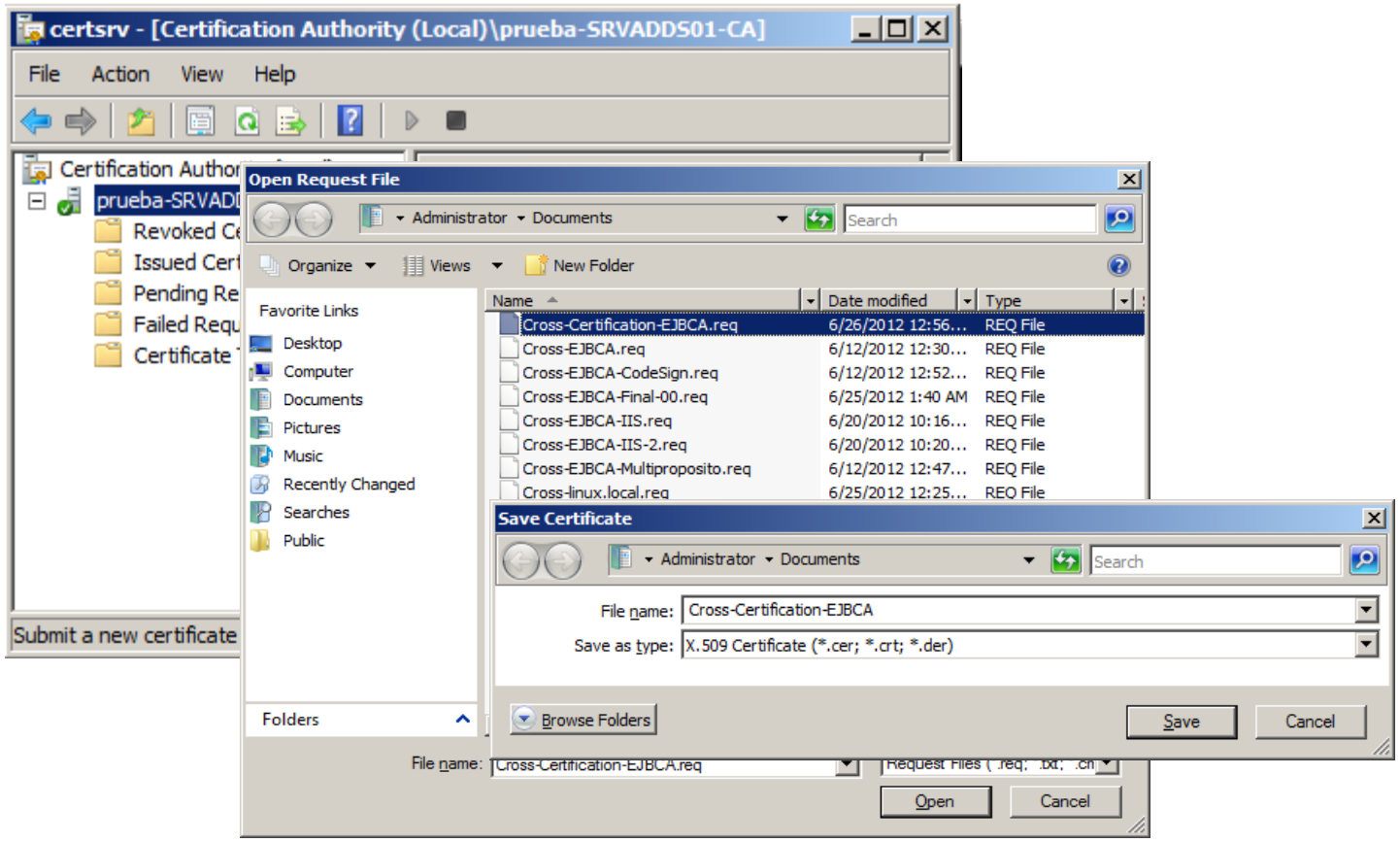
```
[Version]
Signature = $WindowsNT$

[NameConstraintsExtension]
Include = NameConstraintsPermitted
critical = true

[NameConstraintsPermitted]
DirectoryName = "DC=linux, DC=local"
Email = @linux.local
Email = .linux.local
URL = .linux.local
UPN = .linux.local
UPN = @linux.local

[BasicConstraintsExtension]
PathLength = 1


[ApplicationPolicyStatementExtension]
Policies = AppServerAuth,AppCodeSign,AppClientAuth,AppEmailProtection
critical = true

[AppServerAuth]
OID = 1.3.6.1.5.5.7.3.1

[AppClientAuth]
OID = 1.3.6.1.5.5.7.3.2

[AppCodeSign]
OID = 1.3.6.1.5.5.7.3.3

[AppEmailProtection]
OID = 1.3.6.1.5.5.7.3.4

[RequestAttributes]
CertificateTemplate = CrossCA
```

Proceso de generación y firmado de la solicitud del certificado (CSR)

- Generación del CSR
  - Certreq –policy
    - Pide el certificado de la CA que se va a cros-certificar
    - Pide el archivo policy.inf

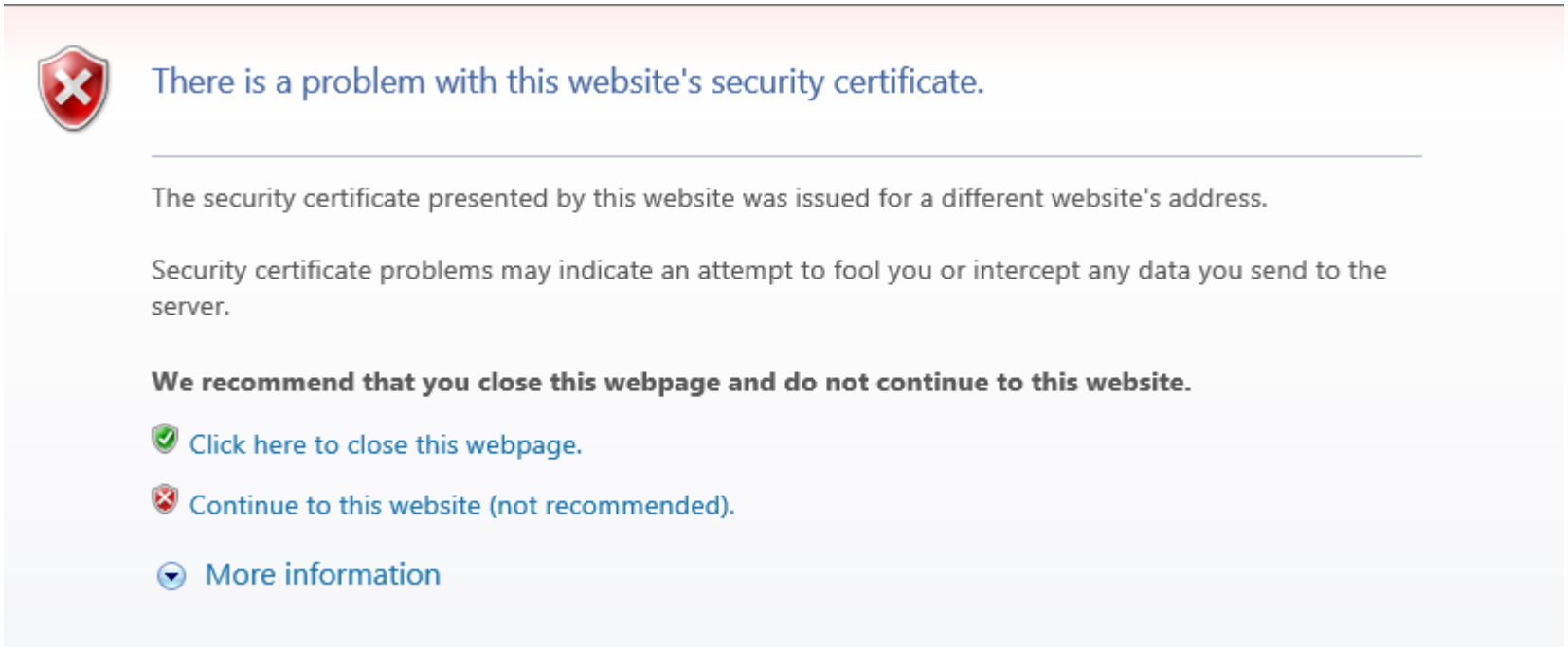
- Firma la solicitud con el agente de certificacion cruzada utilizando la plantilla CrossCA

Emisión del certificado cruzado



Datos Importantes

- Distribuir el nuevo certificado en los equipos que van a tener acceso a entidad que presta los servicios.
-
-



Laboratorios

- Cada facultad tiene su propia PKI
  - AC Raíz
  - AC Subordinada
- La FI va a tener acceso a una aplicación web de la FCE. La FI va a efectuar el proceso de Certificación Cruzada para tener un mejor control de acceso.
- La FI solicita a la FCE el certificado de la SubCA
- La FI efectúa el proceso de certificación

Laboratorios

- Al generar el certificado cruzado, se registra en el repositorio de Autoridades Certificantes Intermedias.
- Nótese que el certificado de la FCE raíz no se registra en los equipos finales.