
# Seguridad en Redes

Laboratorio de confianza entre organizaciones utilizando certificación cruzada

Ing. Edy Javier Milla

Ing. Hugo Pagola

Ing. Alberto Dams

# Objetivos

Disponer de un laboratorio que permita a los alumnos de nuestro posgrado:

- Ejercitar lo aprendido en las clases teóricas y reforzar los conceptos de PKI.
- Orientar en la construcción de una infraestructura PKI.
- Simular ambientes corporativos utilizando diversos S.O.
- Incorporar nuevas destrezas y competencias.

# Pautas didácticas

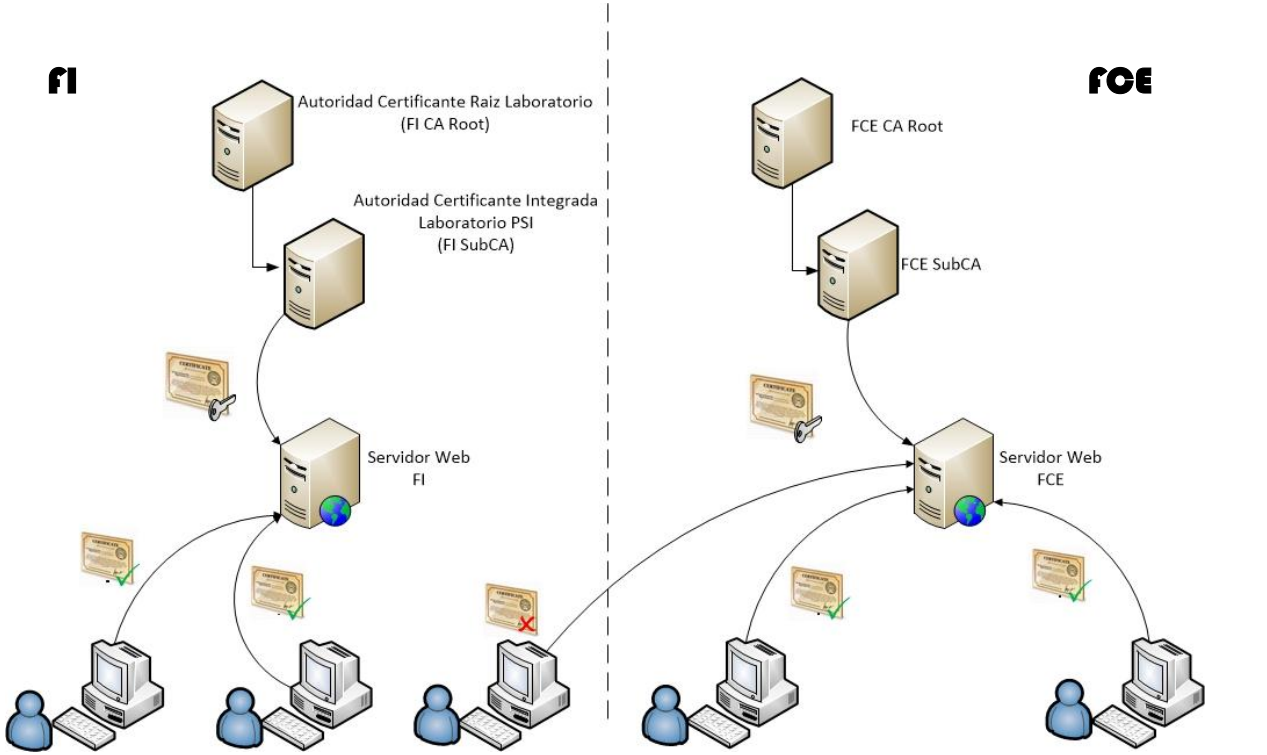
- Presentar un caso real
- Desarrollar en horas de clase para resolver las inquietudes y consolidar el conocimiento.
- Se utilizaron máquinas virtuales para disminuir tiempos de preparación del entorno.
- Plantear situaciones alternativas con desafíos a resolver.

# Escenario: Interfaz entre organizaciones

Donde residen los usuarios.

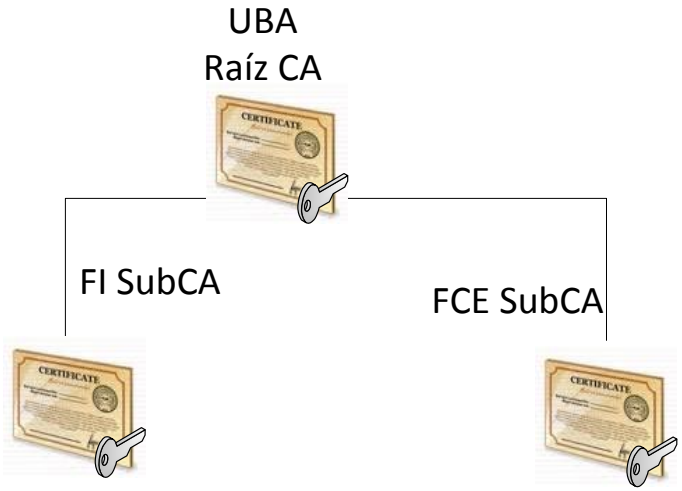
Control de acceso y autenticación

Modelo de Confianza



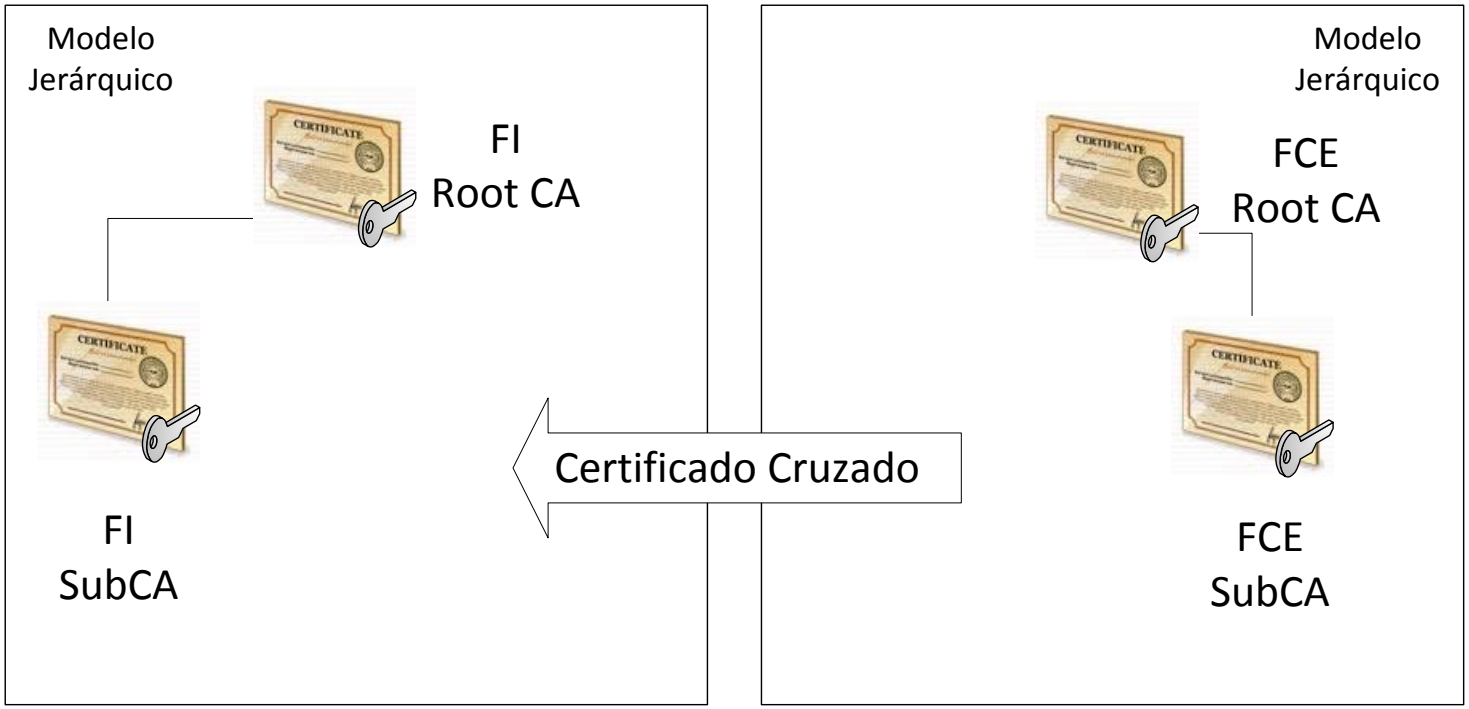
# Modelos de confianza: Jerárquico

- Autoridad Certificante Raíz
- Autoridades Certificantes Subordinadas
- Administración de certificados eficiente delegado en Autoridades Certificantes subordinadas
- Establecimiento de la cadena de certificación



# Modelos de confianza: Certificación Cruzada

- Confianza entre Autoridades Certificantes
- La CA raíz o subordinada de una jerarquía (FI) firma el certificado raíz o subordinado de la otra (FCE)
- Se establecen criterios de validación



# Experiencia de laboratorio

- Caso de aplicación entre FI y FCE
  - Cada facultad tiene su propia jerarquía PKI
  - La FI va a tener acceso a una aplicación web de la FCE.
  - Equipos de la FI deben confiar en los certificados emitidos por la FCE (bajo ciertos criterios)
- La FI efectúa el proceso de Certificación Cruzada.
  - La FI solicita a la FCE el certificado de la SubCA
  - La SubCA de FI firma el certificado de la SubCA FCE

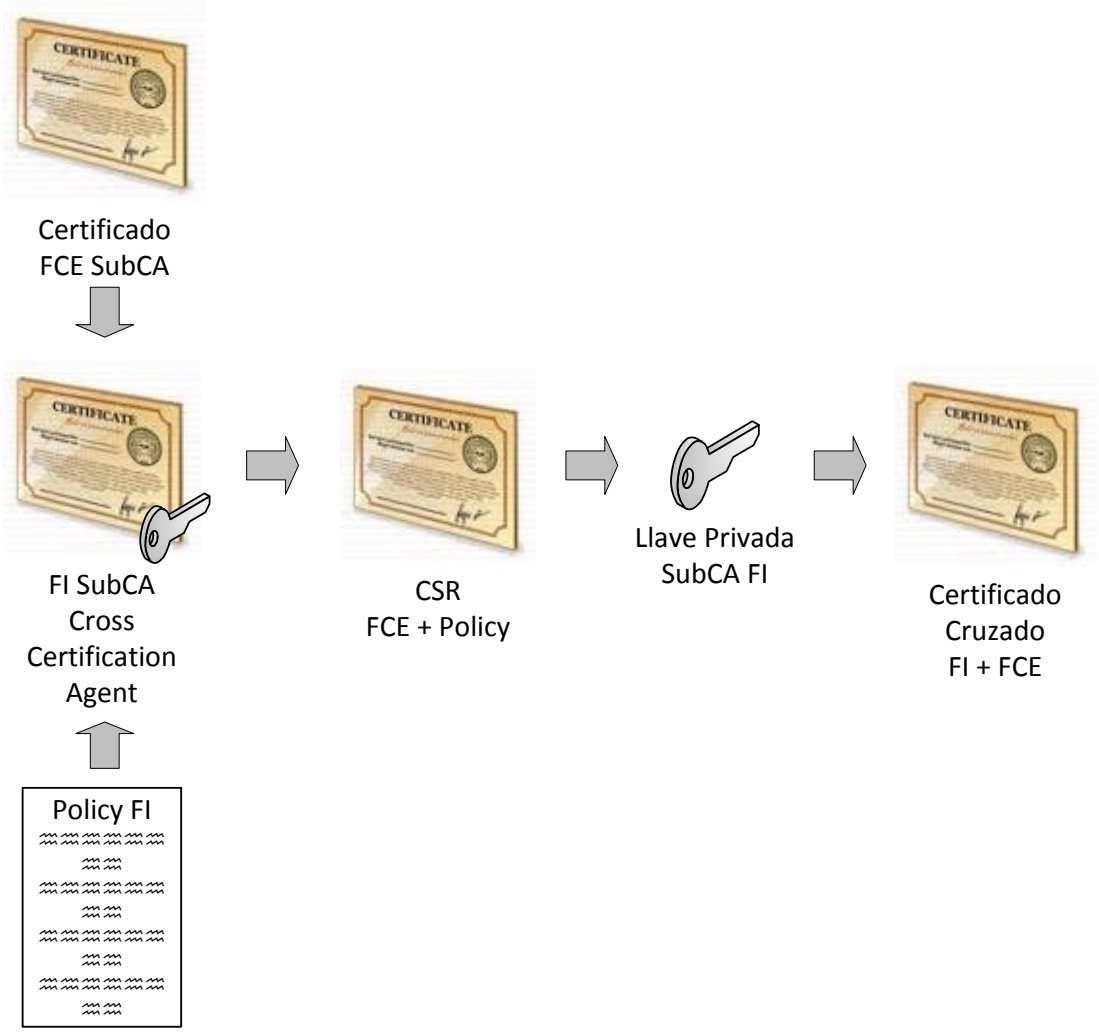
# Criterios de Validación

**Criterios en base al Subject del Certificado**

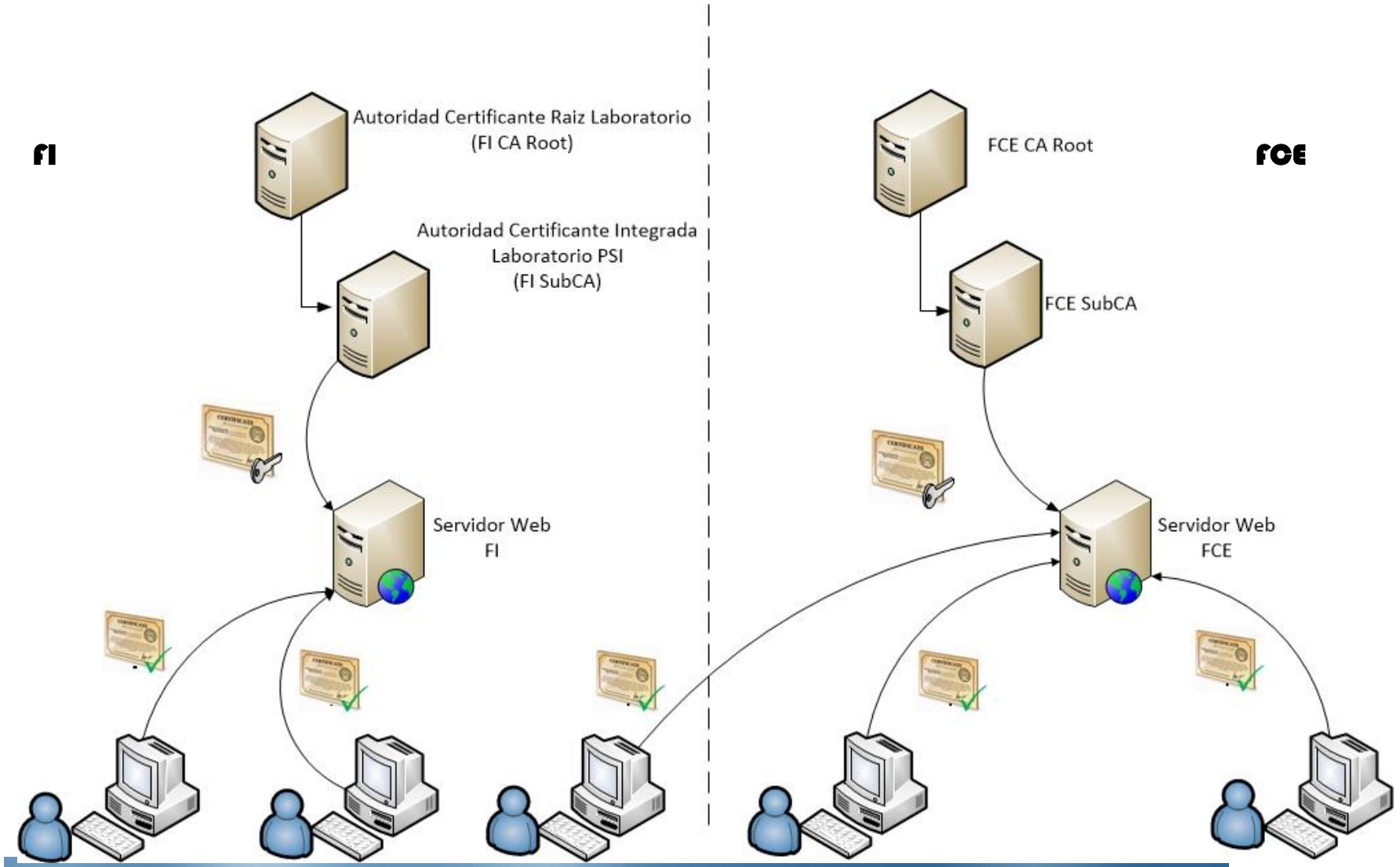
- **RDN (Relative Distinguished Name): o=uba, dc=uba,dc=ar**
- **DNS/SAN (Domain Name Service): websrv.uba.ar**
- **URI (Universal Resource Identifiers): https://websrv.uba.ar**
- **E-mail y UPN (User Principal Name): @uba.ar**
- **IP address: 172.16.1.100**

***(Subject Alternative Name)***

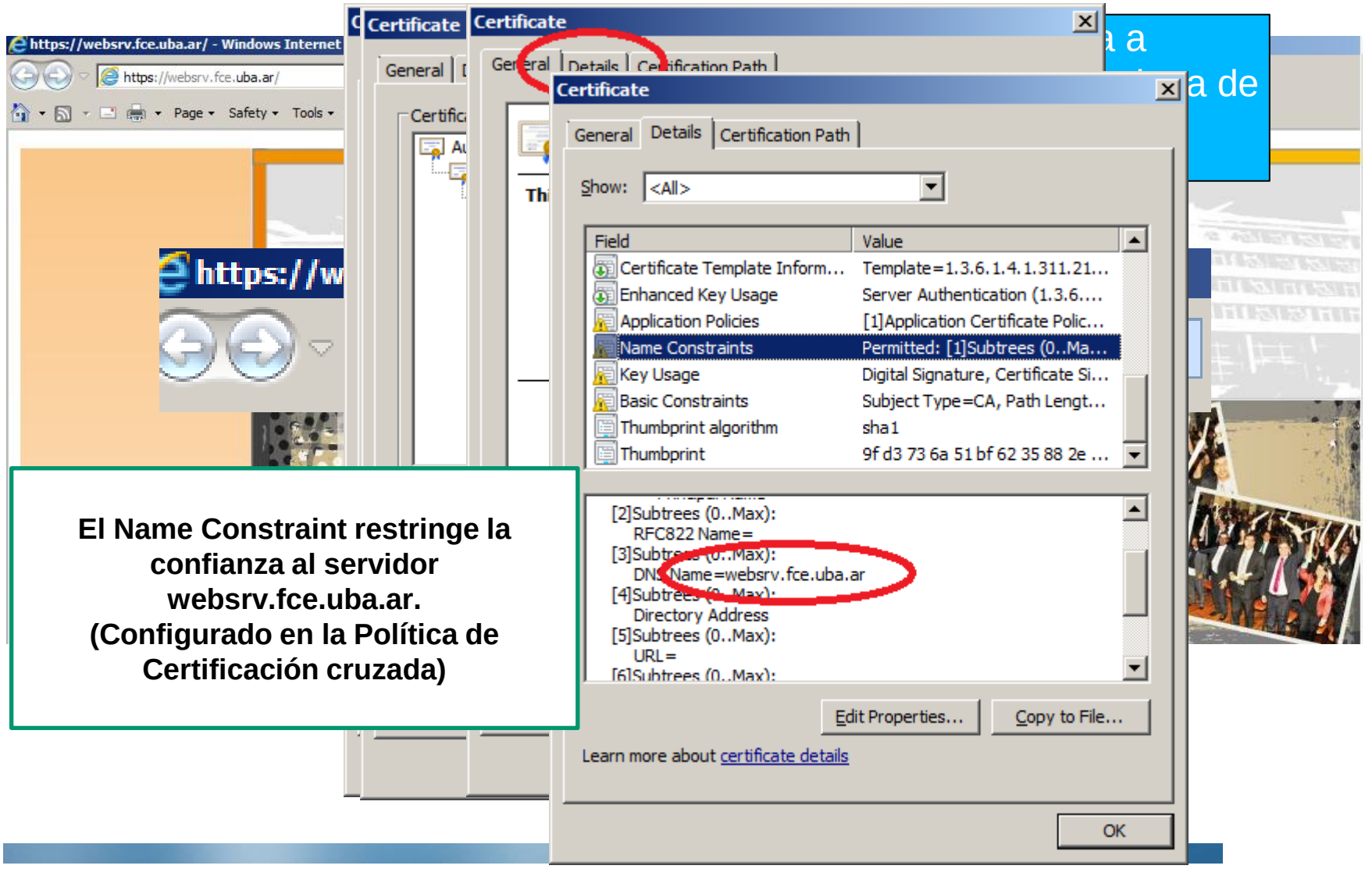
# Proceso de certificación cruzada



# Modelo Certificación Cruzada

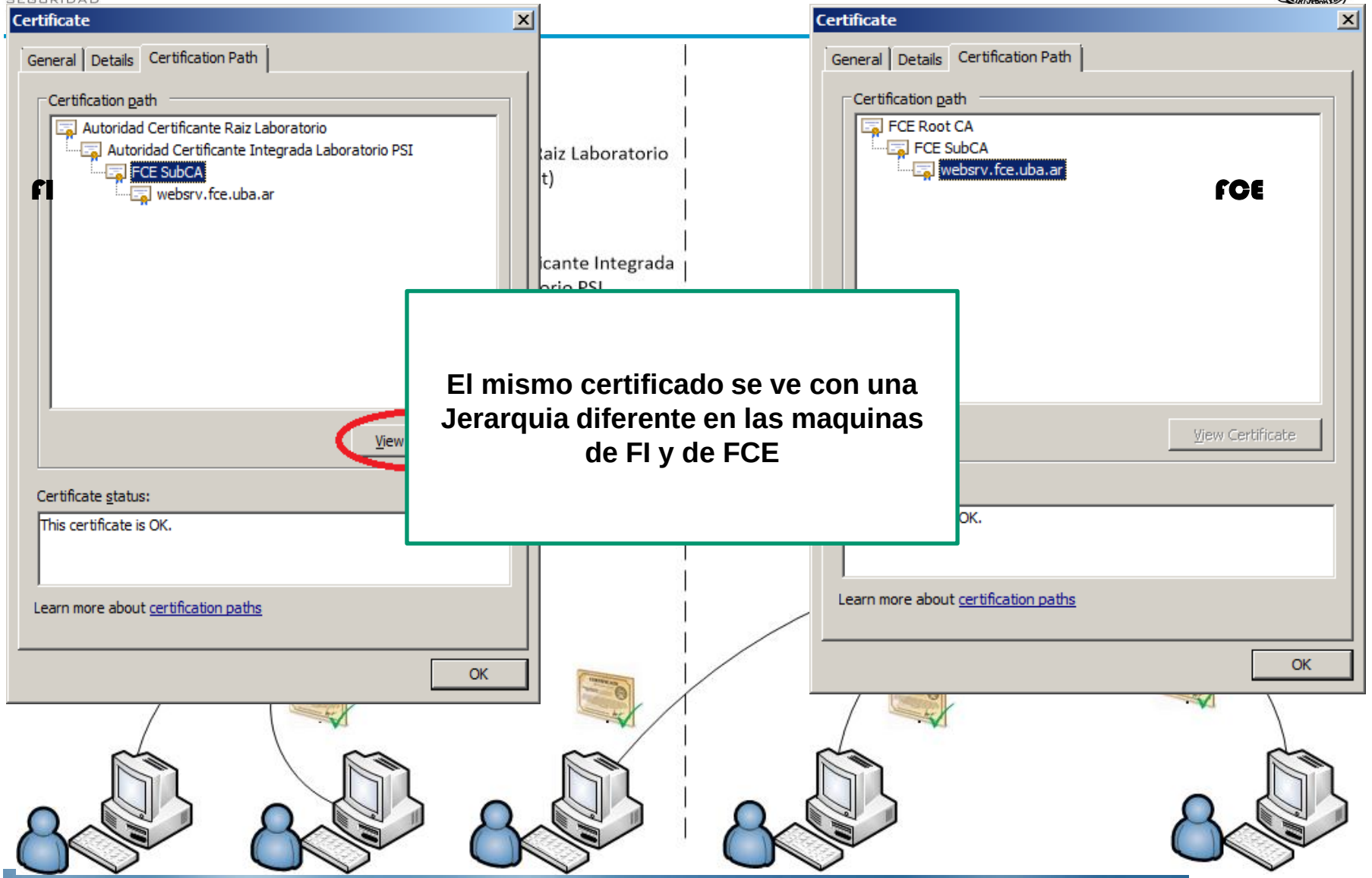


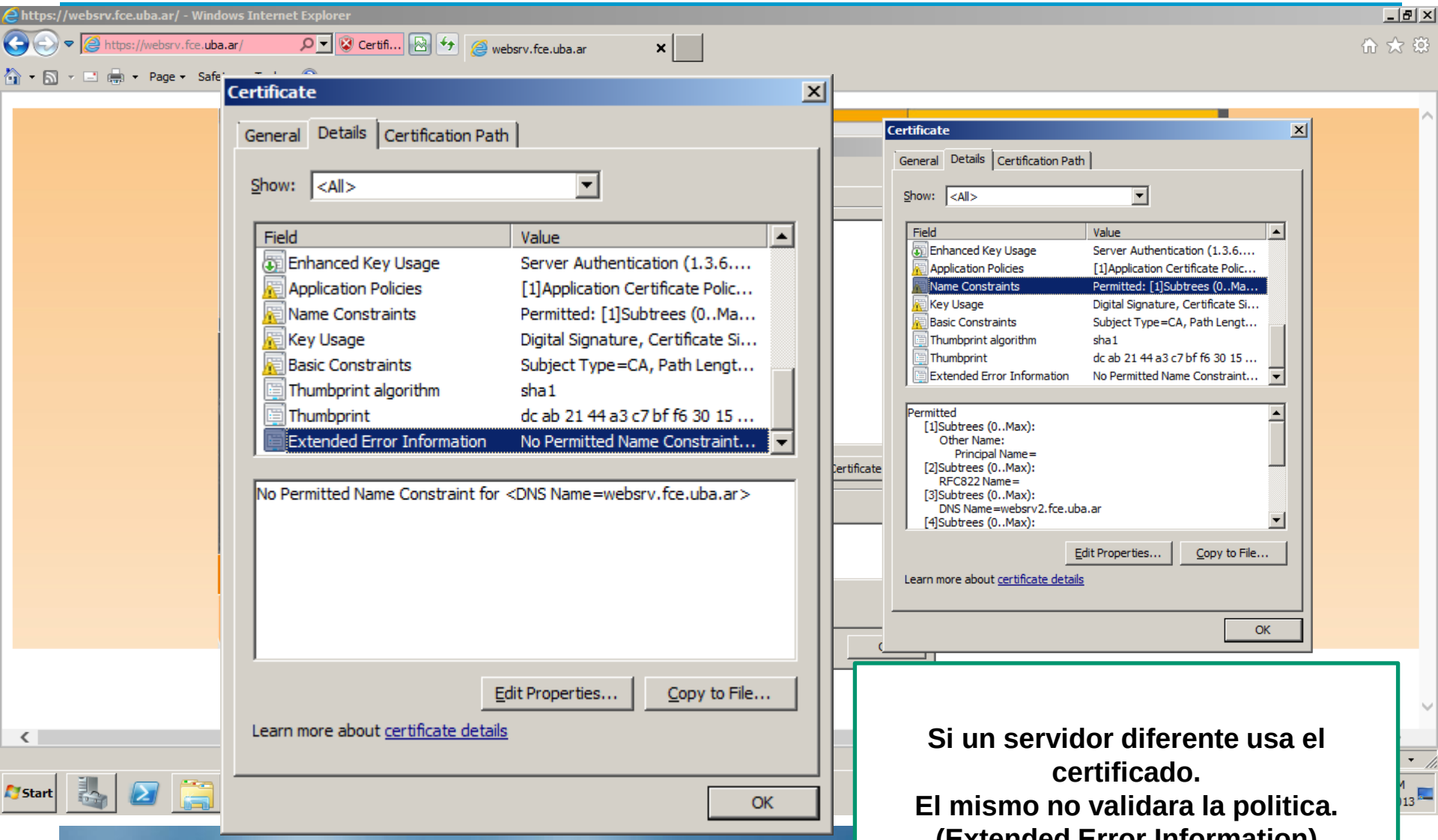
# Acceso a un Web con




**El Name Constraint restringe la confianza al servidor websrv.fce.uba.ar. (Configurado en la Política de Certificación cruzada)**

# Modelo Certificación Cruzada






**Si un servidor diferente usa el certificado.**
**El mismo no validara la politica.**
**(Extended Error Information)**

# Detalle de las practicas

Practicas de CA

- CA Raíz y Subordinada Win2k8 (fi)
- CA Raíz y Subordinada Lnx (fce)
- Certificación Cruzada

Otras Practicas Relacionadas

- Federación SAML
- Análisis de seguridad de SSL
- ipsec linux2linux & ipsec cisco2linux (GNS3)

# Software Utilizado

- Ambientes operativos virtualizados
  - VMWare Workstation/Player v.8 v.9
  - Windows Server 2008 Enterprise: Microsoft CA (FI)
  - GNU Linux (FCE)
    - Debian  CryptoCD
    - Ubuntu: Versión 12.10 64 bits
    - OpenSSL, EJBCA.

# Resultados

- Hemos tenido una muy buena recepción del material por los alumnos quienes han sugerido numerosos cambios y mejoras.
- El material permitió que los estudiantes desarrollen las configuraciones de los laboratorios en forma rápida y con buenos resultados.
- Las encuestas aplicadas permitieron medir el nivel de aceptación de los laboratorios e identificar los aspectos de mejora para las siguientes clases.

# Conclusiones

- Mediante esta práctica los estudiantes adquieren destrezas y competencias que hoy día son requeridas por las organizaciones.
- Este laboratorio nos ha permitido trabajar el concepto de Confianza establecida entre organizaciones utilizando ambientes heterogéneos..
- La primer experiencia piloto fue el año pasado. Este año fue utilizado por todos los estudiantes exitosamente.

# Gracias por su atención.