ESCUELA POLITECNICA DEL EJERCITO

Carrera de Ingeniería de Sistemas e Informática

Desarrollo de una aplicación Sign – On en Smart Cards

Vinicio Ramirez M.

SEGURIDAD INFORMÁTICA

La Seguridad Informática debe vigilar principalmente por los siguientes elementos:

- **INTEGRIDAD**
  Los componentes del sistema permanecen intactos a menos que sean modificados por los usuarios autorizados.

- **DISPONIBILIDAD**
  Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

- **PRIVACIDAD**
  Los componentes del sistema son accesibles sólo por los usuarios autorizados.

SEGURIDAD INFORMÁTICA

- **CONTROL**
  Solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

- **AUTENTICIDAD**
  Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

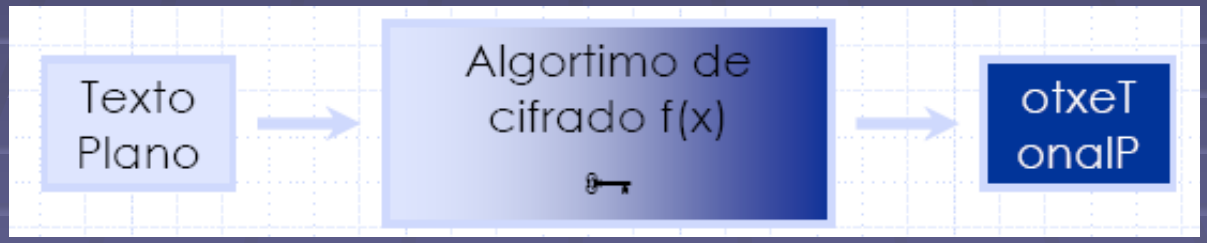
- **NO REPUDIO**
  Evita que cualquier entidad que envíe o reciba información niegue que lo hizo.

- **AUDITORIA**
  Determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

SEGURIDAD INFORMÁTICA

CRIPTOGRAFIA

Transformar un mensaje legible en otro cifrado, mediante la utilización de claves, que solo el emisor y receptor conocen.



Utilidades:

- Genera certificados digitales
- Genera firmas digitales
- Protege información
- Protege tráfico
- Almacena credenciales localmente de una manera muy segura

SEGURIDAD INFORMÁTICA

MÉTODOS CRIPTOGRÁFICOS

- **SIMÉTRICOS O DE CLAVE PRIVADA**

  Se emplea la misma clave para cifrar y descifrar.
  El emisor y receptor deben conocerlas.

- **ASIMÉTRICOS O DE CLAVE PÚBLICA**

  Se emplea una clave privada y una clave pública.
  Una de ellas es utilizada para cifrar y la otra para descifrar.
  El emisor conoce una y el receptor la otra.
  Cada clave no puede obtenerse a partir de la otra.

SEGURIDAD INFORMÁTICA

FIRMA DIGITAL

Verifica que la información no ha sido modificada (integridad) desde su generación.

CERTIFICADOS DIGITALES

Certifican que quien firma un documento electrónico, es quien dice ser, para lo cual se generan previamente la clave pública y privada del remitente.

TARJETAS INTELIGENTES

Tarjetas de plástico similares a las tarjetas de crédito.
Poseen un circuito integrado.
Este circuito puede ser de sola memoria o contener un microprocesador (CPU) con un sistema operativo que le permite:

- Almacenar
- Encriptar información
- Leer y escribir datos, como un ordenador.

TARJETAS INTELIGENTES

CLASIFICACIÓN POR EL TIPO DE CONTACTO

Tarjetas inteligentes de Lectores con Contacto

- Poseen chip y una placa de contactos
- Necesitan lector/grabador para comunicarse con el exterior

Tarjetas inteligentes de Lectores sin Contacto

- Poseen chip y antena para realizar transacciones
- Transacciones rápidas

Tarjetas inteligentes Híbridos (Ambos Lectores)

- Combinación de las anteriores.

TARJETAS INTELIGENTES

CLASIFICACIÓN POR EL TIPO DE MICROCHIP

Tarjetas de Memoria Simple:

- Chip integrado
- Ventaja:
  - Almacenamiento más seguro de la información
- Desventaja:
  - Sólo almacenar información no la procesa

TARJETAS INTELIGENTES

CLASIFICACIÓN POR EL TIPO DE MICROCHIP

Tarjetas de memoria inteligente con Lógica de Seguridad:

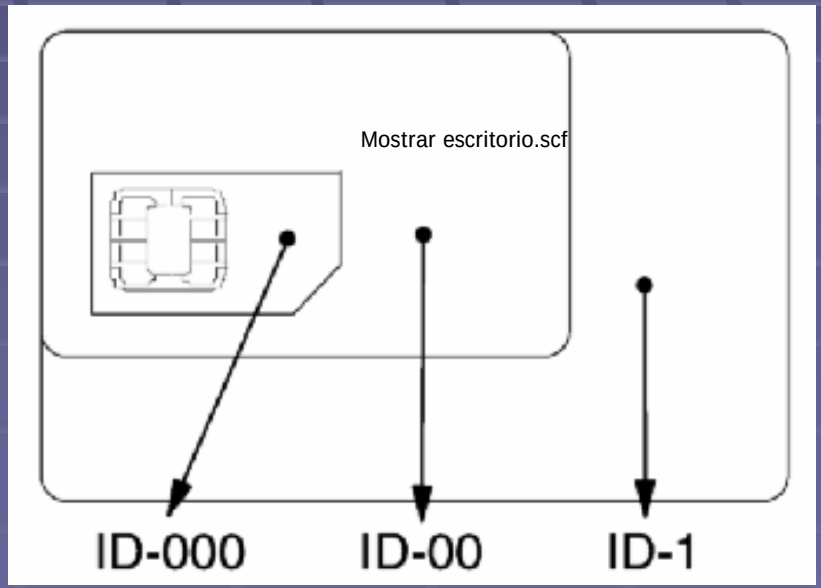
Tarjetas microprocesadores

- Ventajas:
  - Dispositivo seguro por definición
  - Capaces de procesar información (además de almacenarla)
  - Pueden ser programadas.
  - Multiaplicación (monedero electrónico, información bancaria, telefonía,etc)
- Desventajas:
  - Lenguajes de programación de tarjetas dependientes del hardware.
  - Programación de las tarjetas en ensamblador.
  - Aplicaciones desarrolladas por el proveedor de la tarjeta.

TARJETAS INTELIGENTES

Tamaños de tarjetas ISO 7816-1

- ID-1 (es el más habitual)
- ID-00
- ID-000 (GSM)



PROTOCOLOS DE AUTENTICACIÓN: KERBEROS

- Protocolo de seguridad
- Utiliza criptografía de claves simétricas para validar usuarios
- Evita el envío de contraseñas a través de la red.

Kerberos puede proporcionar tres servicios de seguridad:

- **Autenticación:** Probar que usted es quien dice ser.
- **Integridad:** Asegurar que los datos no son modificados en su tránsito.
- **Privacidad:** Asegurar que los datos no son leídos por personas ajenas.

PROTOCOLOS DE AUTENTICACIÓN: KERBEROS

VENTAJAS

- Autenticación segura: mezcla de números aleatorios y marcas de tiempo
- Eliminar la transmisión a través de la red de información de autenticación.
- Confidencialidad de datos: Flujo seguro mediante cifrado con claves de sesión

DESVENTAJAS

- Gran centralización del sistema, si el servidor Kerberos falla, no habrá autenticación y por tanto no se podrá prestar ningún servicio que requiera autenticación
- Casi toda la seguridad reside en el servidor de la base de datos, y si esta se ve amenazada, lo estará la red
- Necesarias aplicaciones “kerberizadas” en todos los participantes

ARQUITECTURA AAA

AUTENTICACION (Authentication)

- Comprobación de que el usuario es quien dice ser

AUTORIZACIÓN (Authorization)

- Verificación de las tareas autorizadas

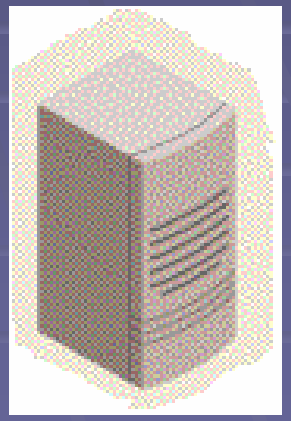
CONTABILIDAD (Accounting)

- Medición del consumo de recursos recursos

SIGN ON

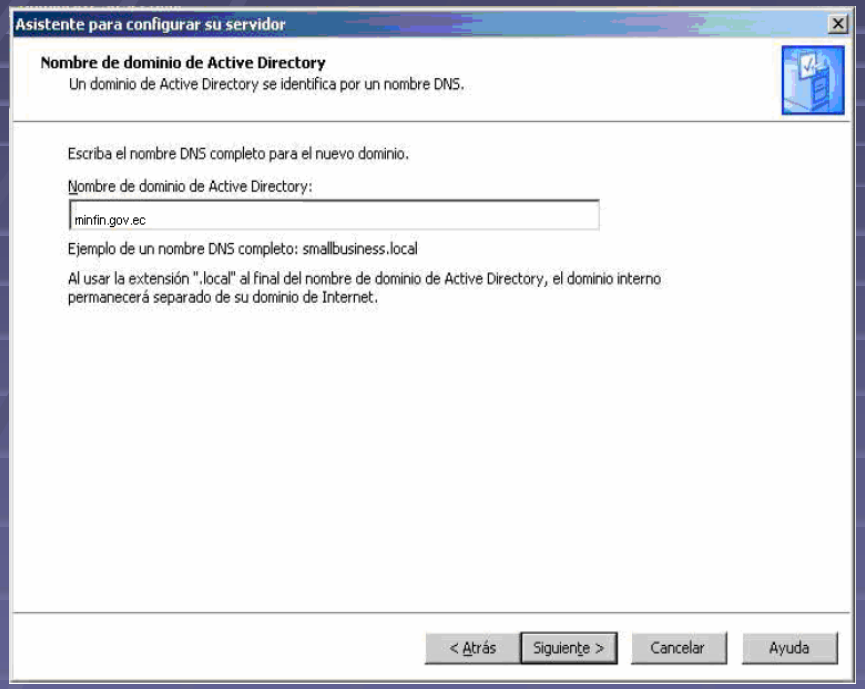
Agente certificador

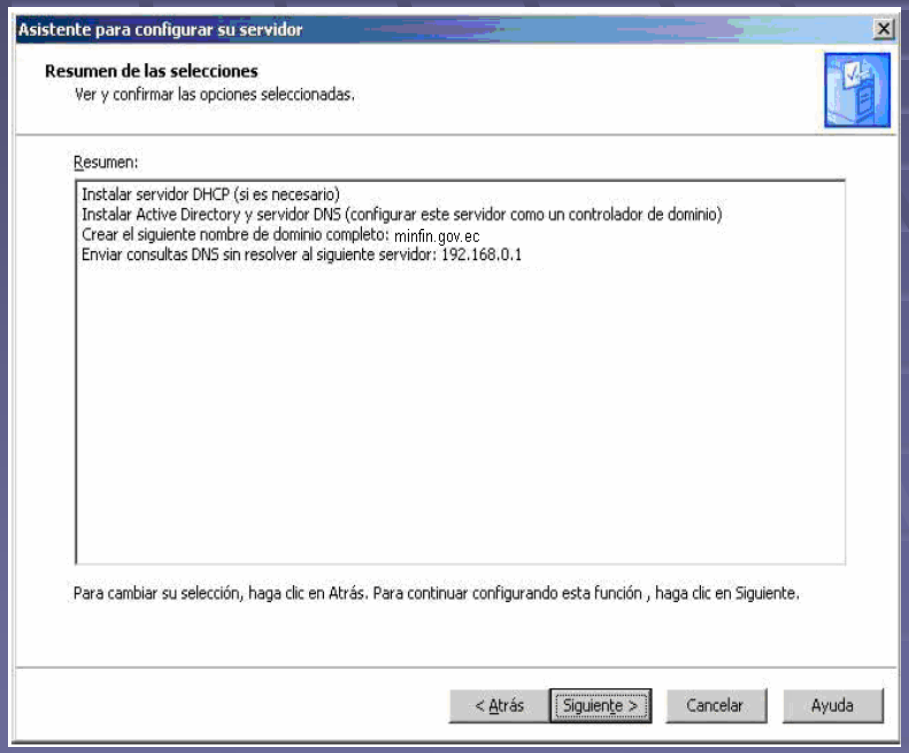
Cliente



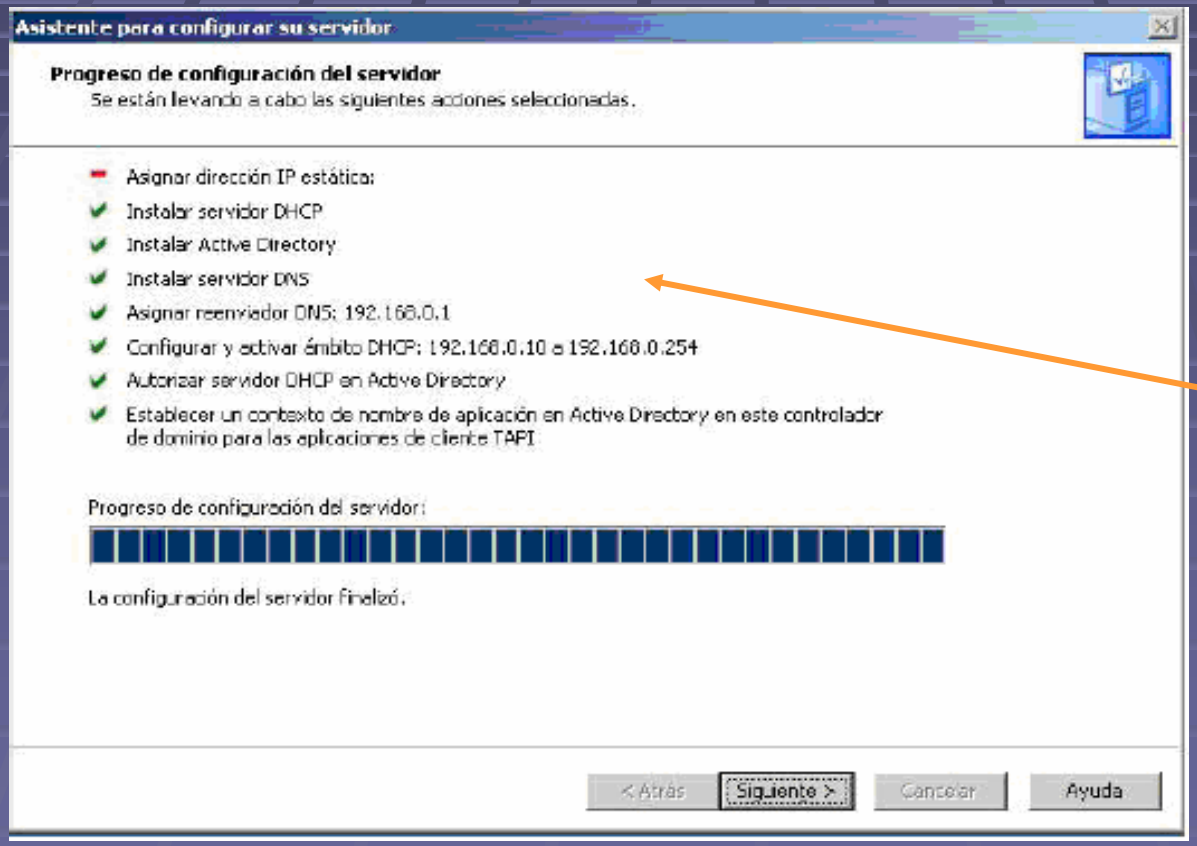
Servidor

INSTALACIÓN DE ACTIVE DIRECTORY - DHCP



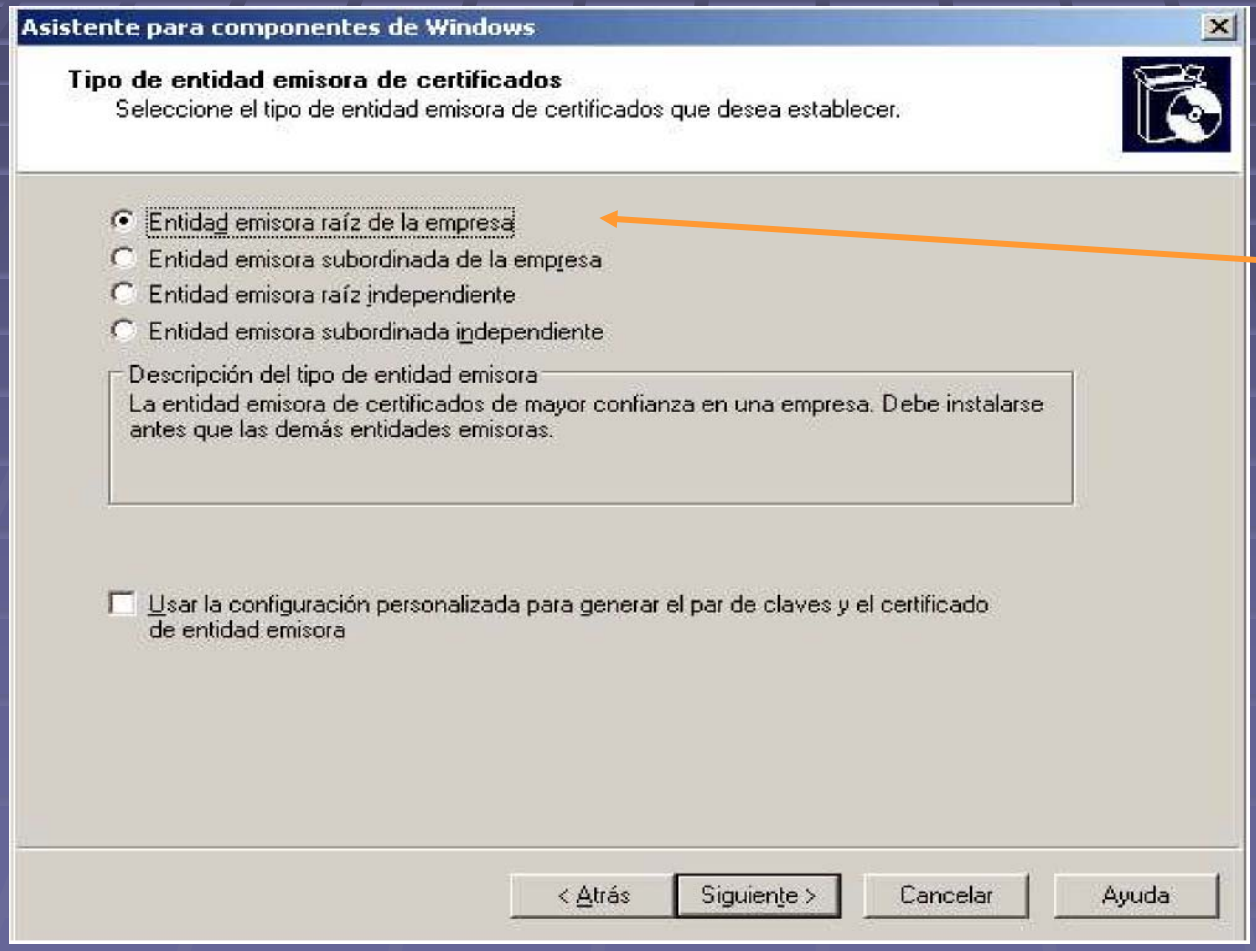


INSTALACIÓN DE ACTIVE DIRECTORY - DHCP



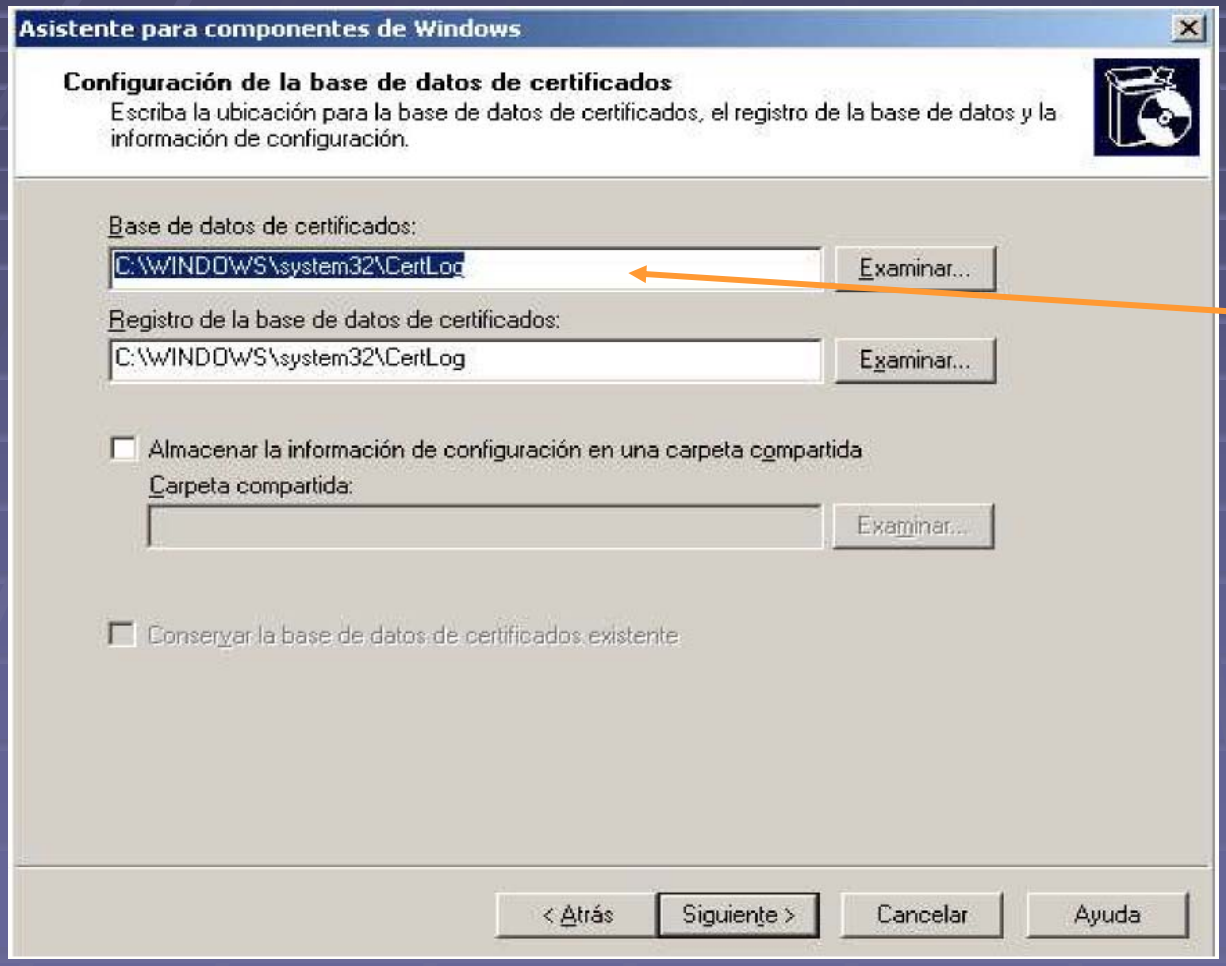
Finalización De la Instalación Active Directory DHCP, etc

INSTALACIÓN DE LA ENTIDAD EMISORA DE CERTIFICADOS



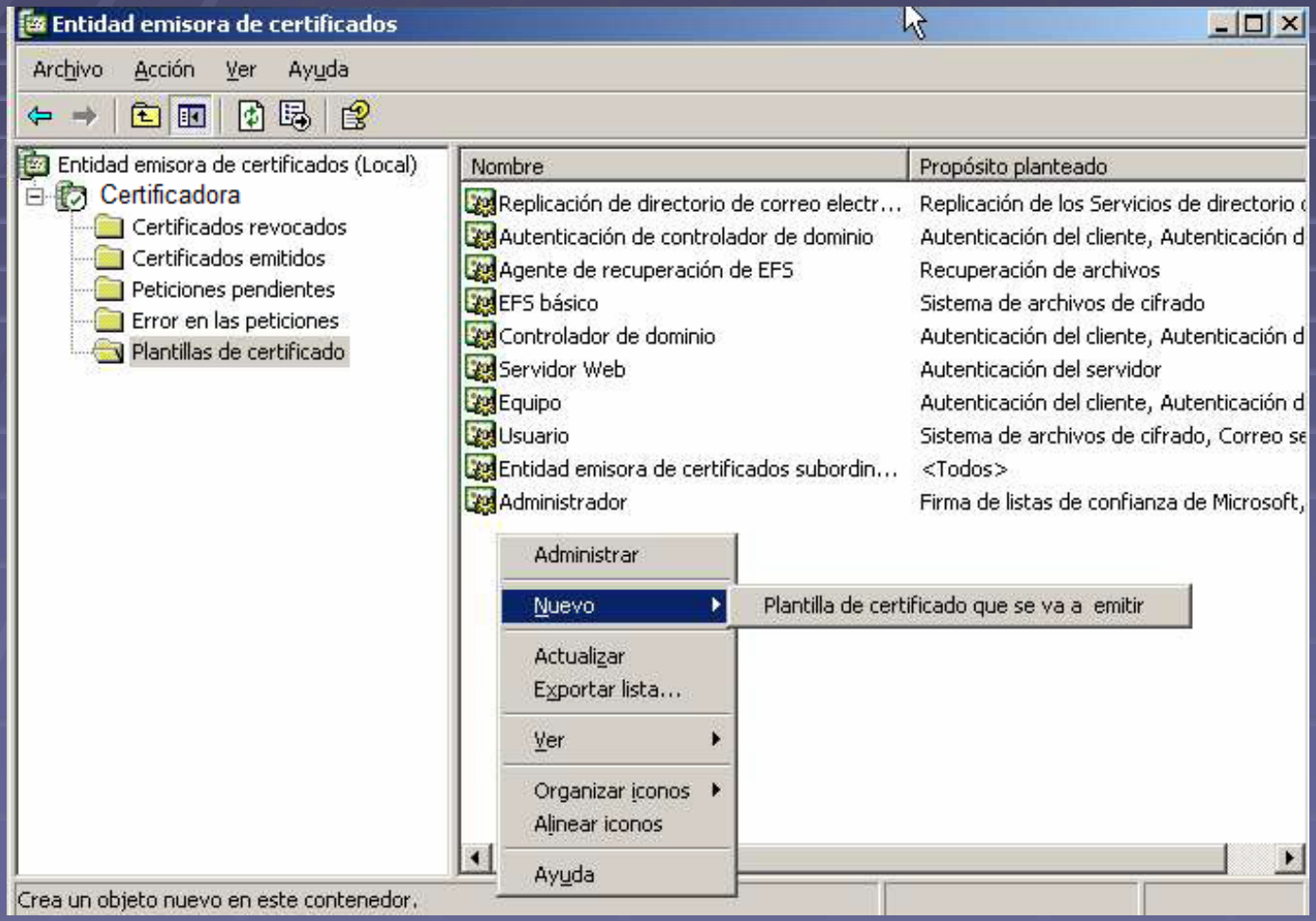
Entidad emisora raíz de la empresa

INSTALACIÓN DE LA ENTIDAD EMISORA DE CERTIFICADOS



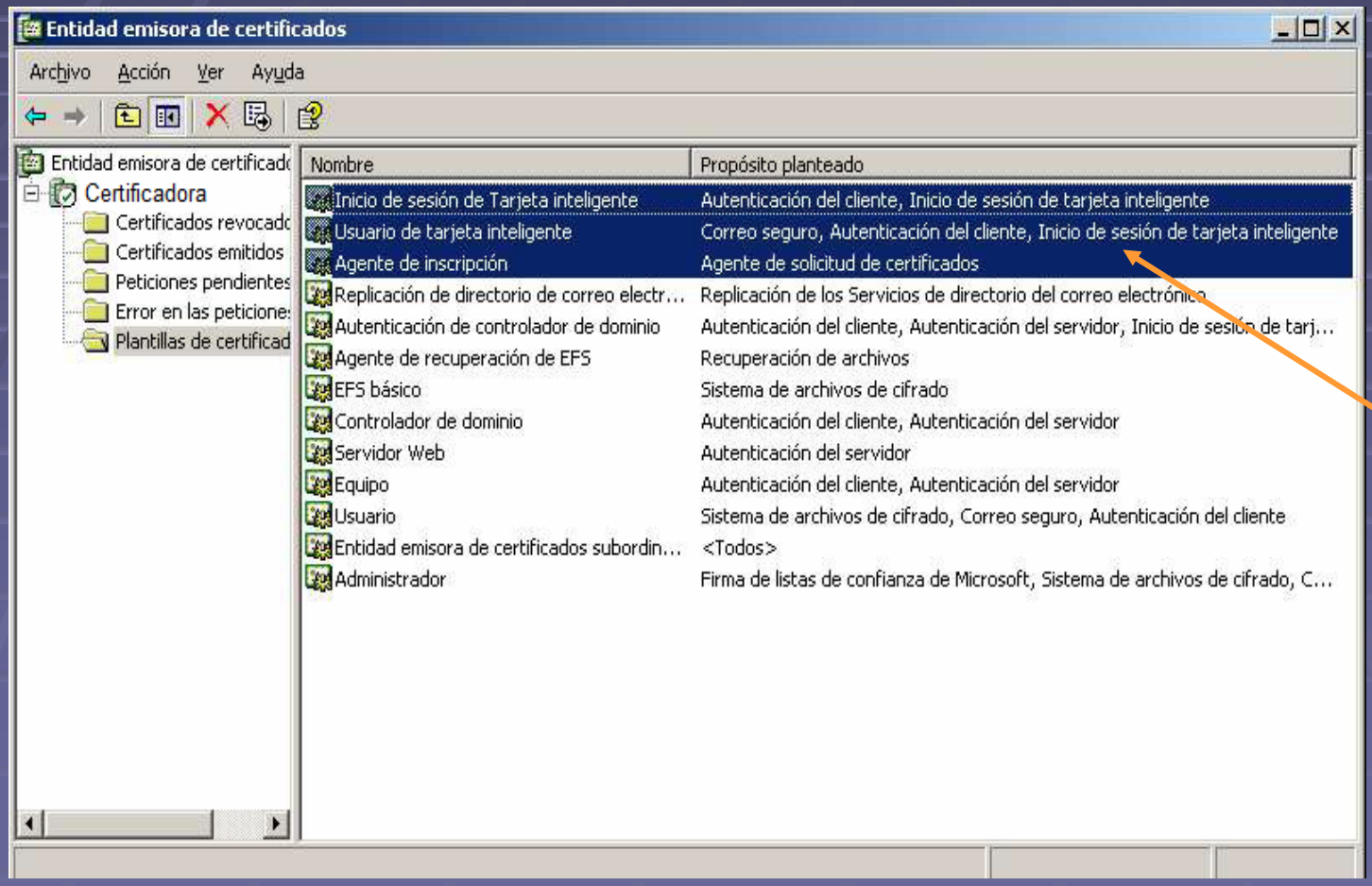
Almacenamiento de los certificados

CONFIGURACIÓN DE ENTIDAD EMISORA DE CERTIFICADOS



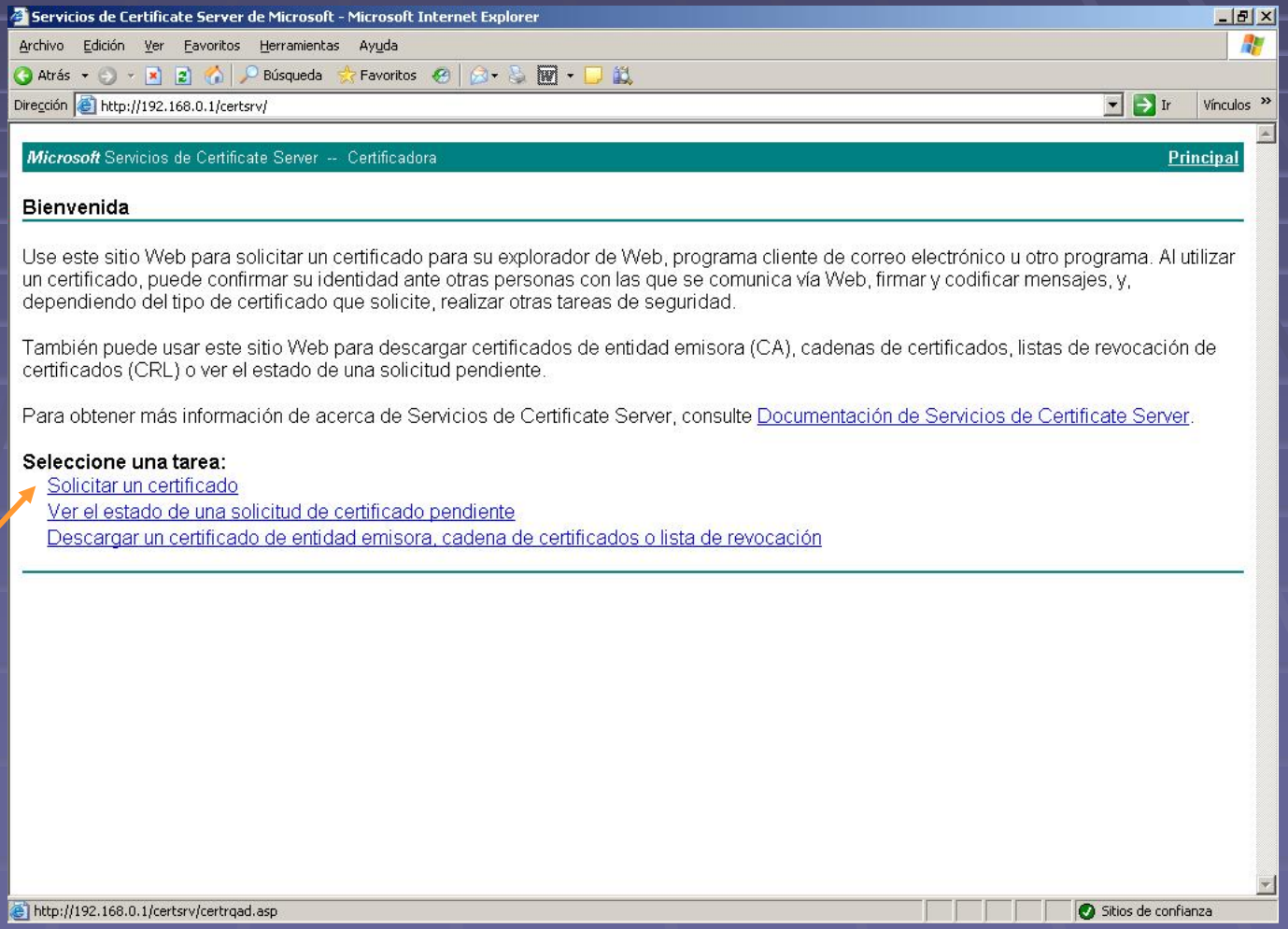
Seleccionar Plantillas

CONFIGURACIÓN DE ENTIDAD EMISORA DE CERTIFICADOS



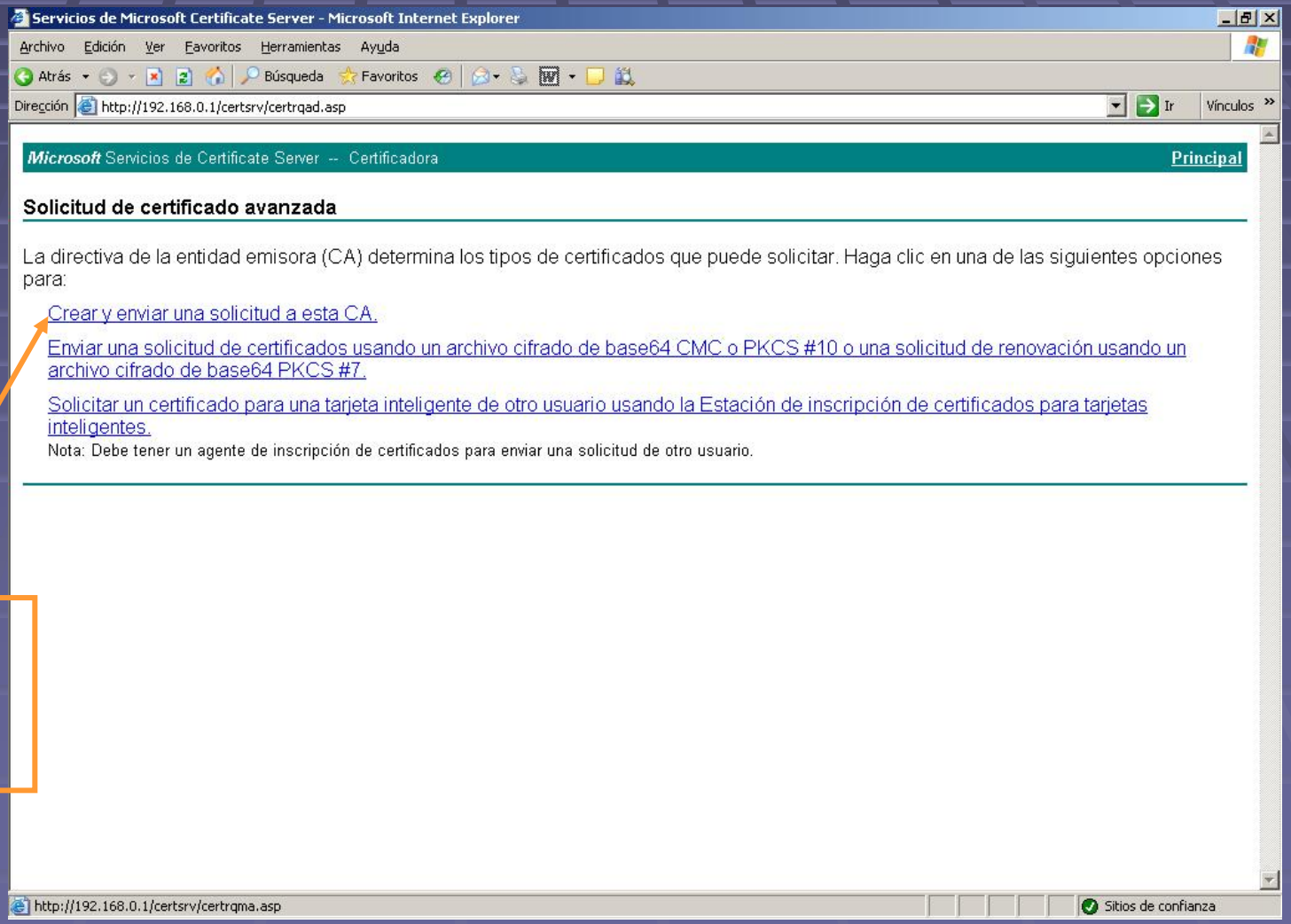
Seleccionar plantillas a ser emitidas

GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN



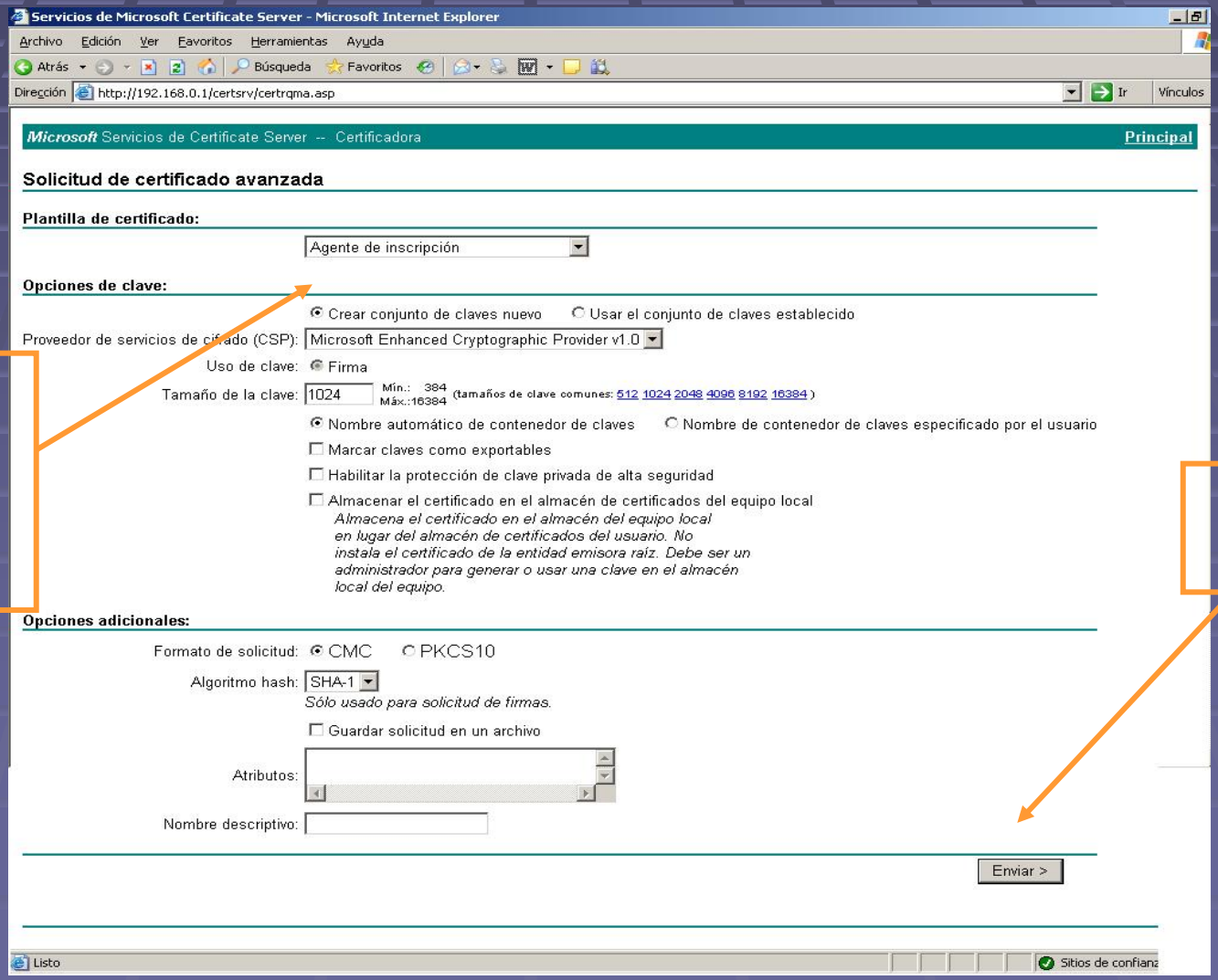
Solicitar un certificado

GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN



Crear y Enviar una Solicitud a esta CA

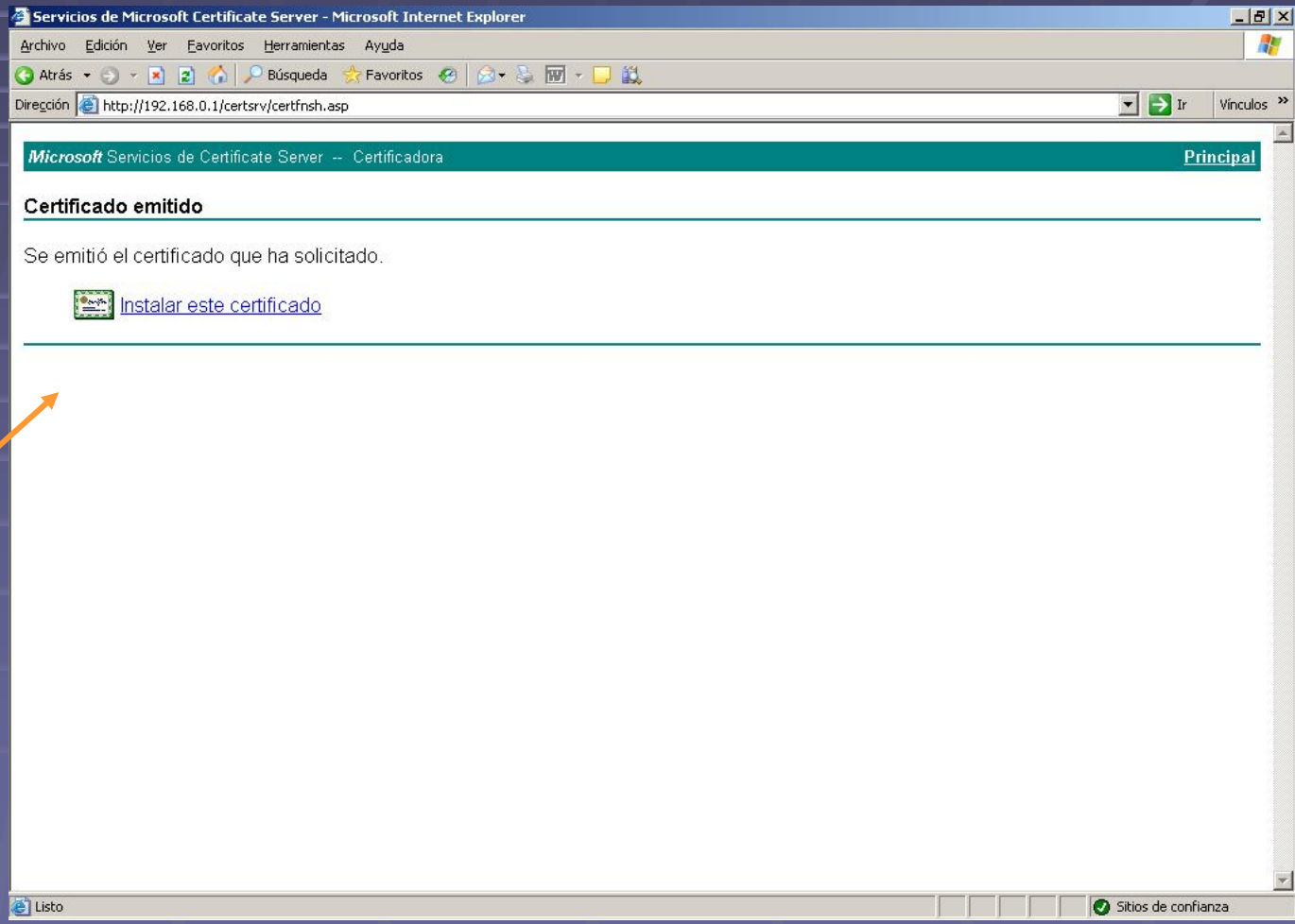
GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN



Seleccionar la Opción de Agente de Inscripción

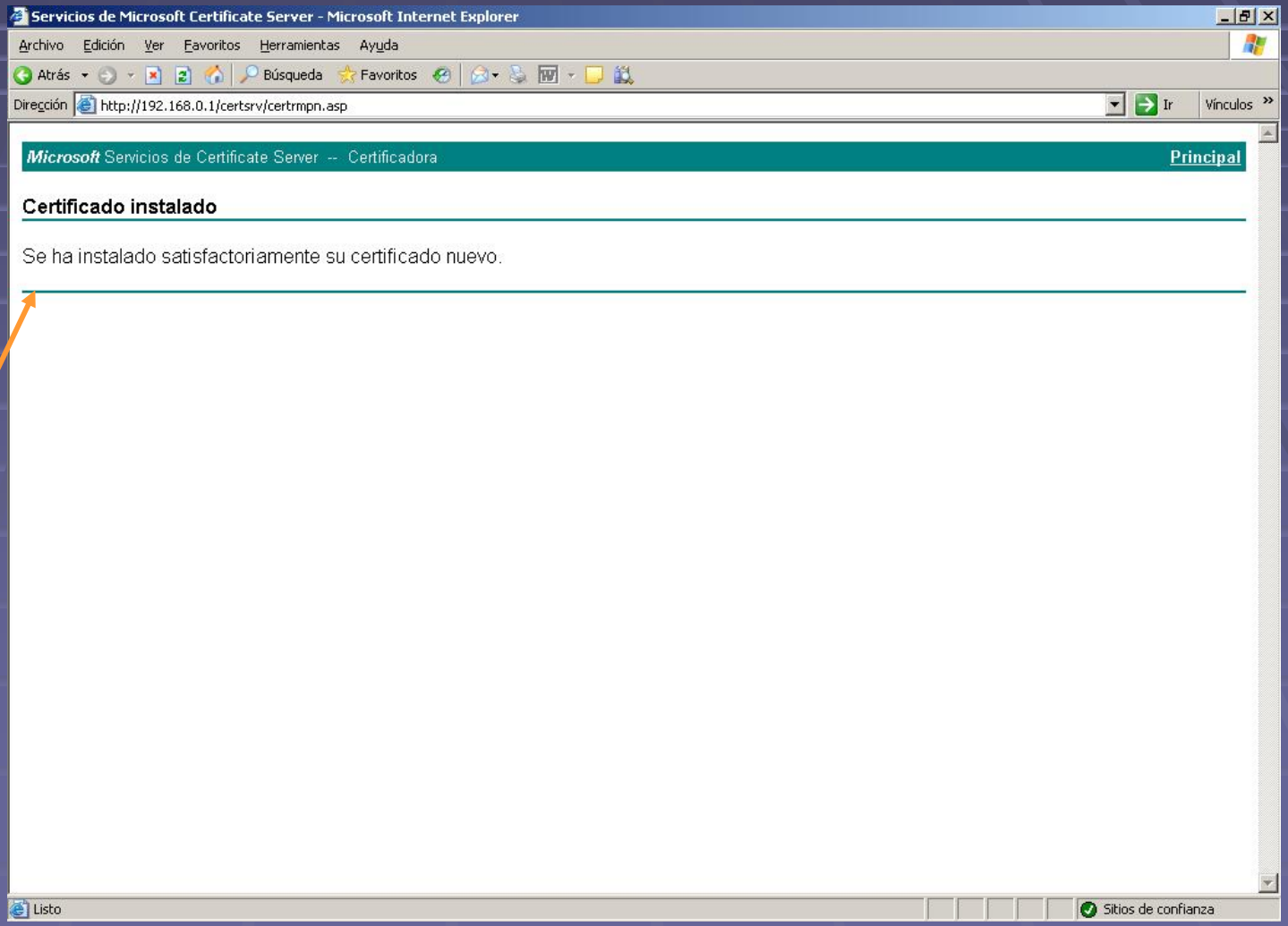
Enviar solicitud

GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN



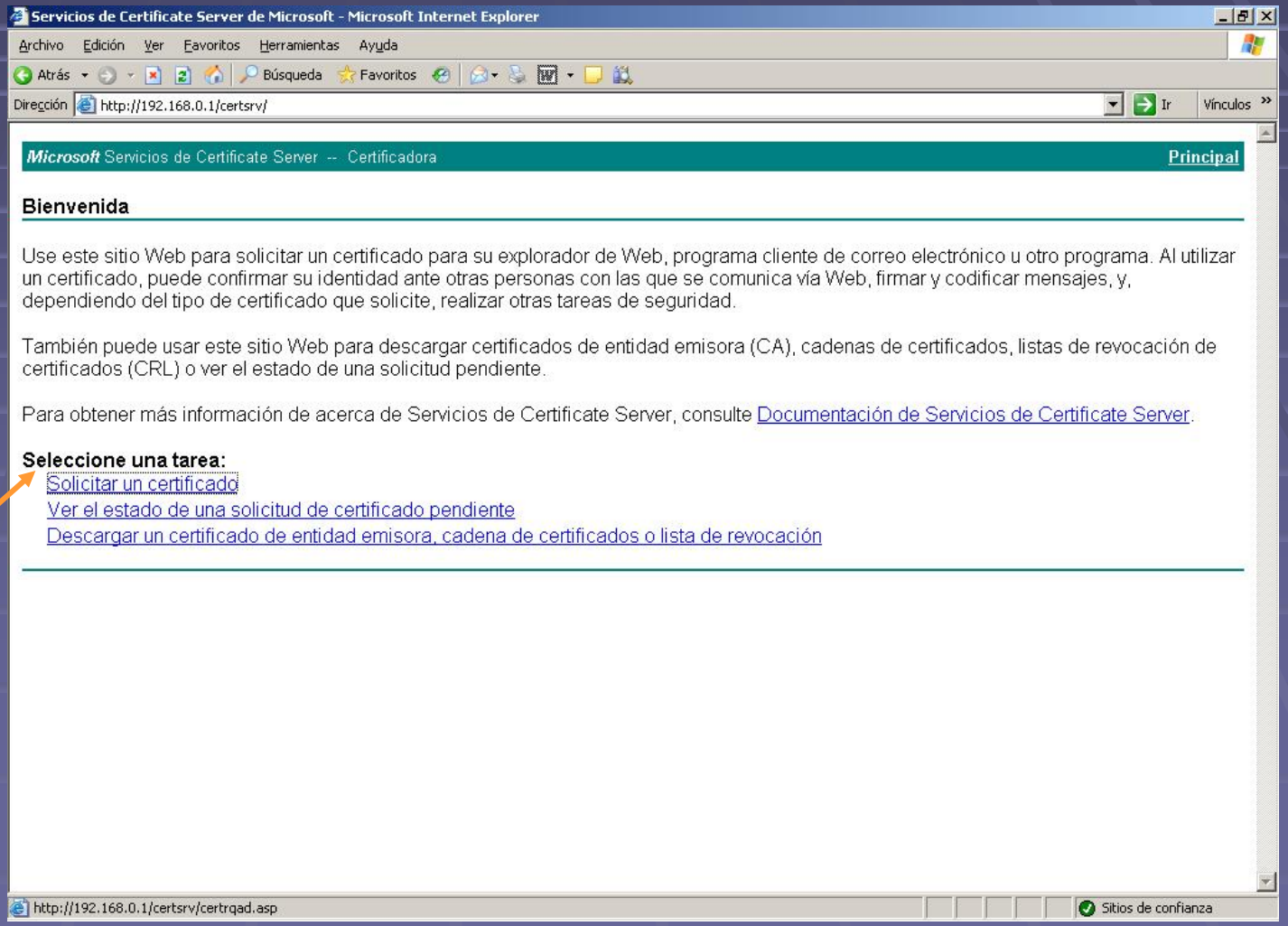
Instalar certificado

GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN



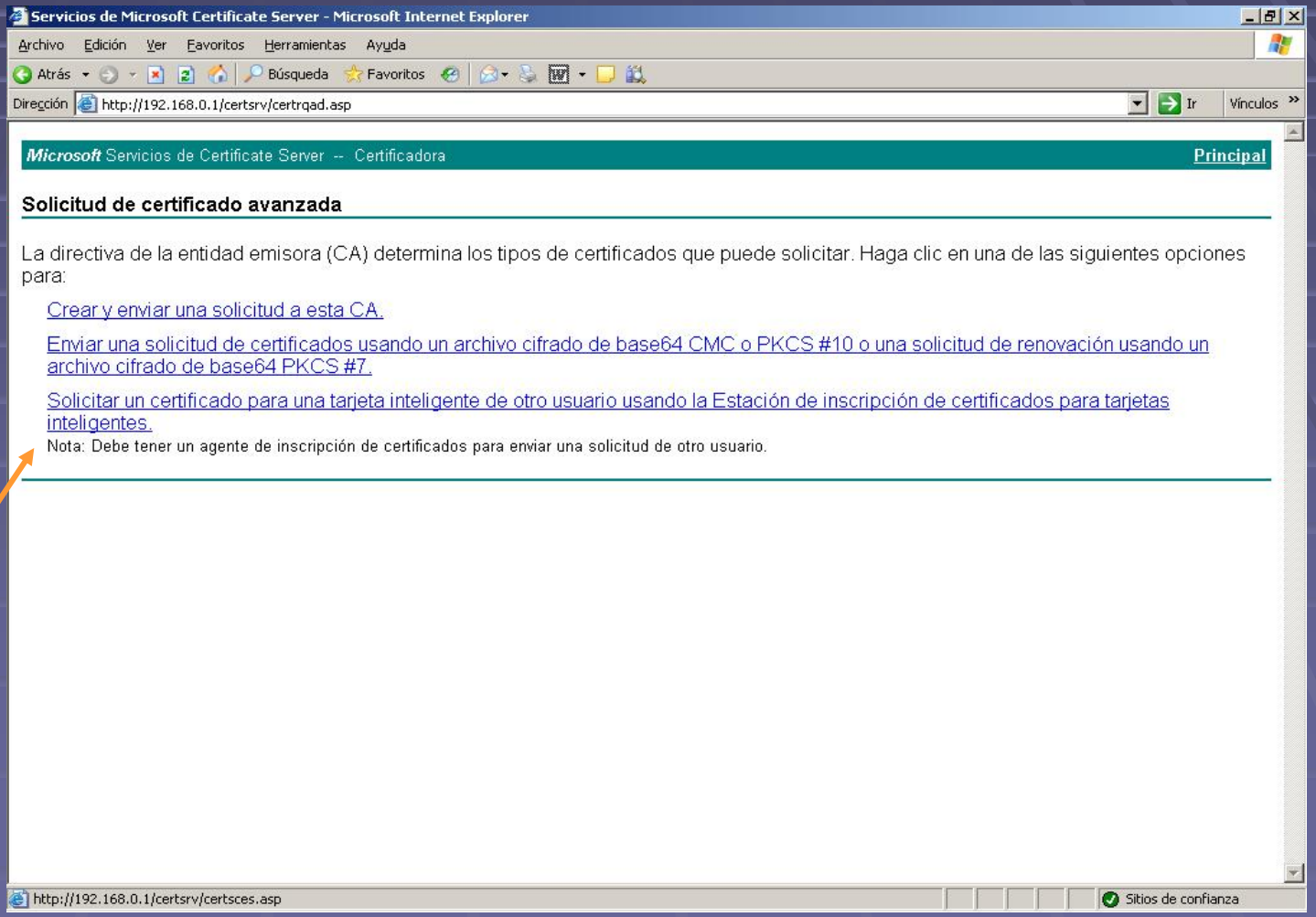
Finalización Configuración del Agente Certificador

GENERACIÓN DE CERTIFICADOS PARA USUARIOS



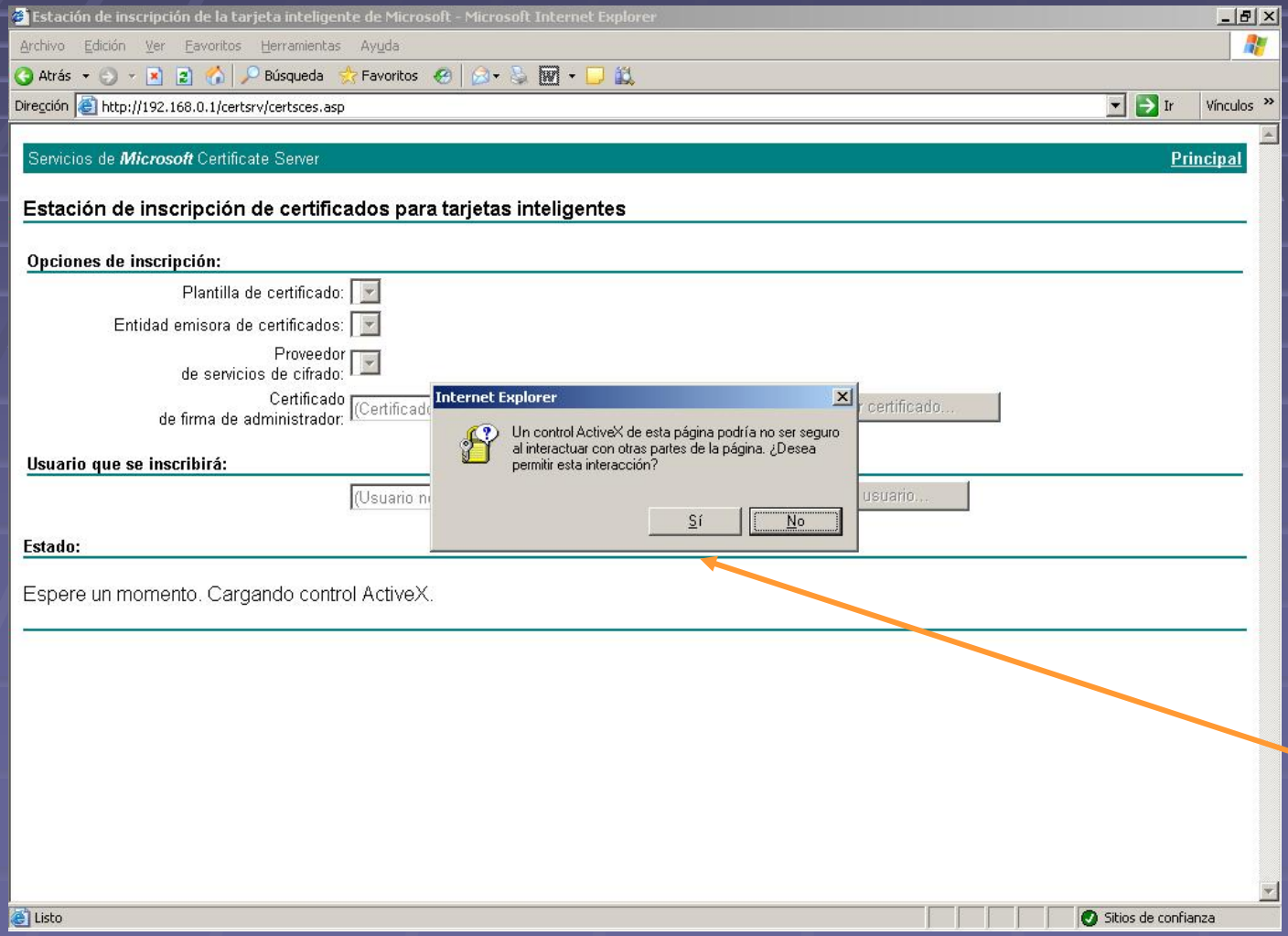
Solicitar un certificado para usuario

GENERACIÓN DE CERTIFICADOS PARA USUARIOS



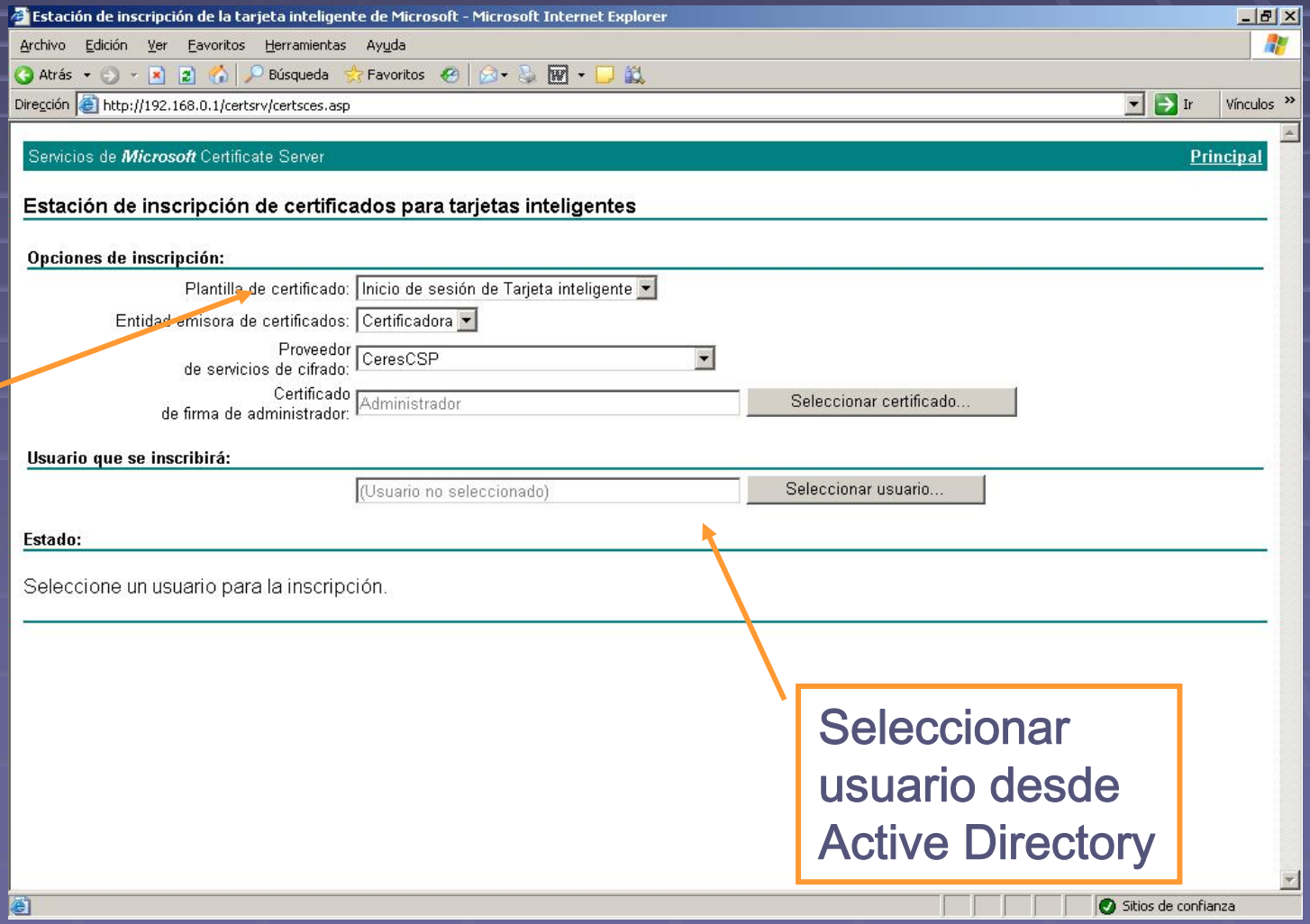
Solicitar un certificado para tarjeta inteligente

GENERACIÓN DE CERTIFICADOS PARA USUARIOS



Aceptar la solicitud

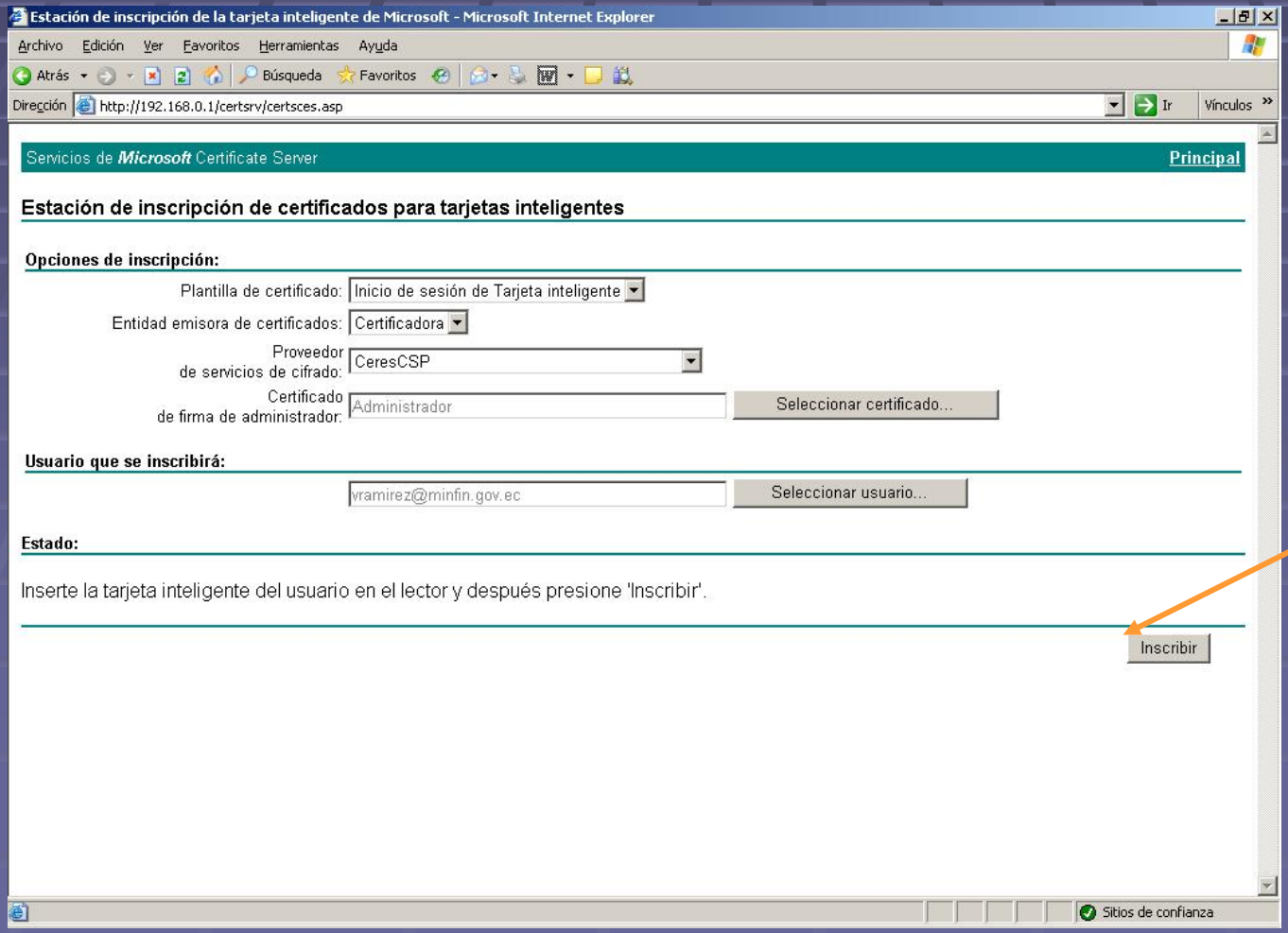
GENERACIÓN DE CERTIFICADOS PARA USUARIOS



Seleccionar la opción de…

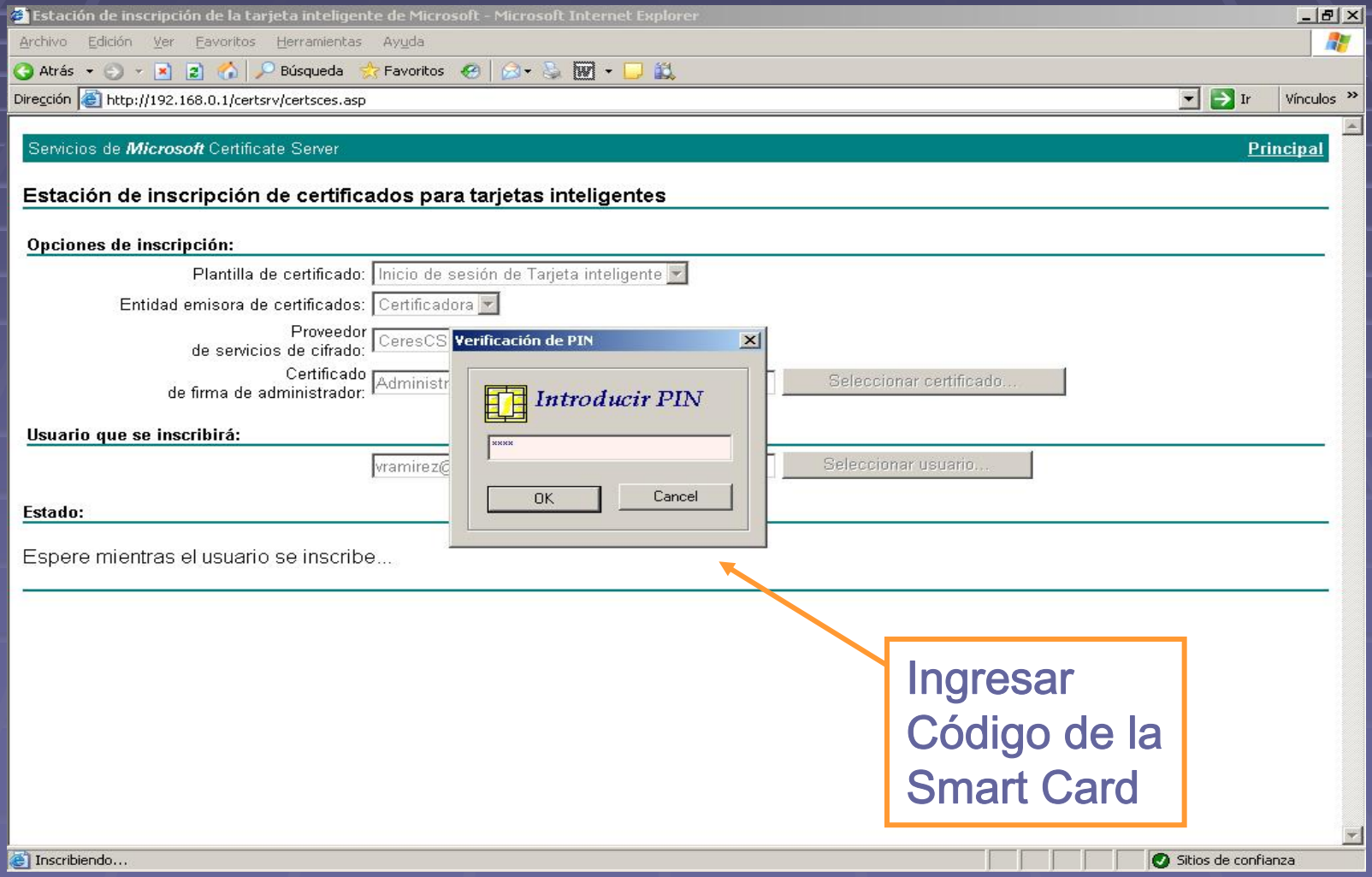
Seleccionar usuario desde Active Directory

GENERACIÓN DE CERTIFICADOS PARA USUARIOS

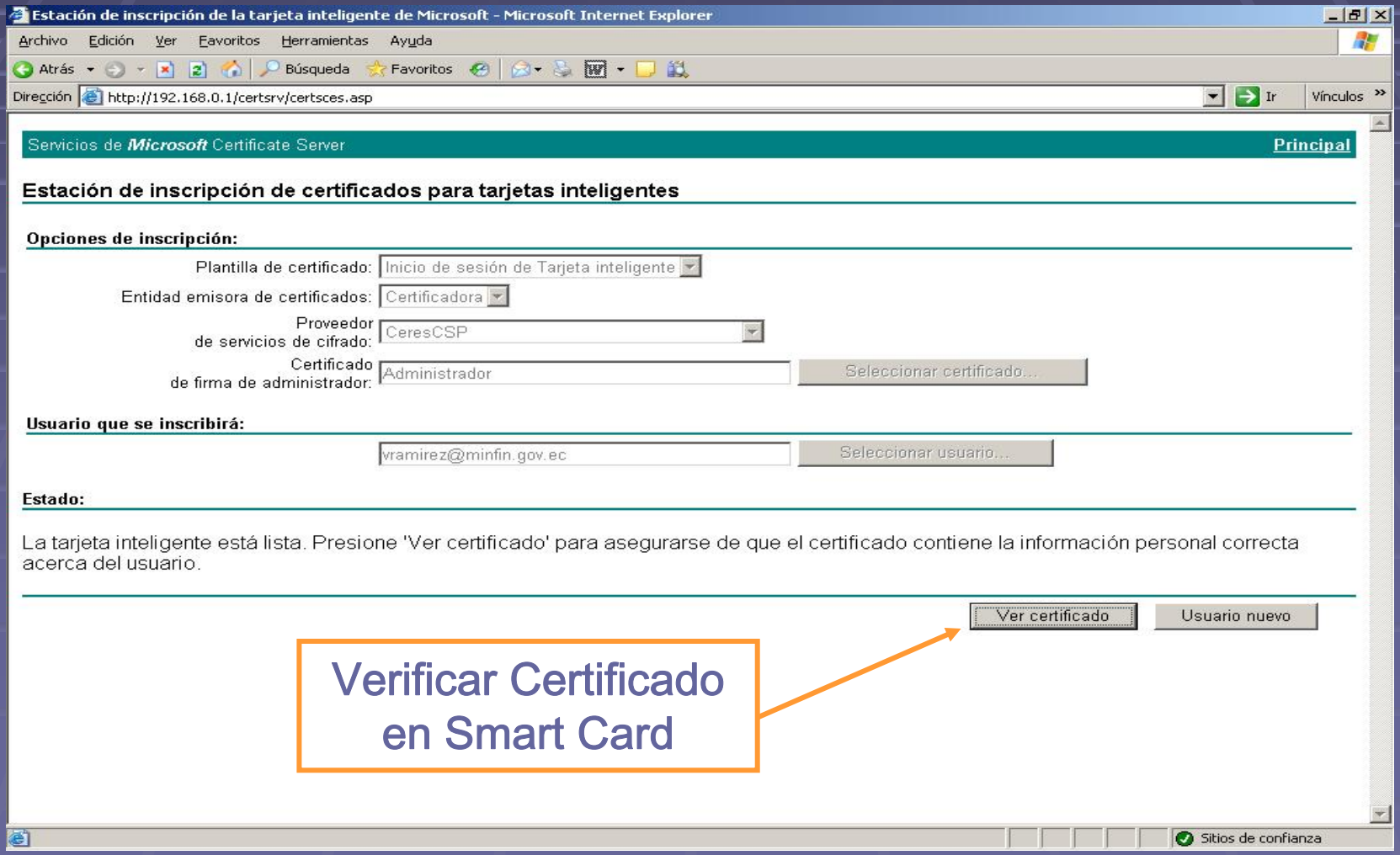


Inscribir la tarjeta

GENERACIÓN DE CERTIFICADOS PARA USUARIOS



GENERACIÓN DE CERTIFICADOS PARA USUARIOS



GENERACIÓN DE CERTIFICADOS PARA USUARIOS

Certificado en Smart Card

INICIO DE SESIÓN CON TARJETA INTELIGENTE

Cliente listo para log on con smart card

INICIO DE SESIÓN CON TARJETA INTELIGENTE

Ingresar Pin de Smart Card

GRACIAS