Autoritat de Certificació de la Comunitat Valenciana

Manual de configuración de un controlador de dominio con certificados digitales emitidos por la ACCV .

Fecha: 28/11/06

Versión: 1.0

Estado: APROBADO

Nº de páginas: 13

OID: 1.3.6.1.4.1.8149.1.1.8.27

Clasificación: PÚBLICO

Archivo: Manual_logon.doc

Preparado por: ACCV

GENERALITAT VALENCIANA

Secretaria Autonòmica de Telecomunicacions i Societat de la Informació

Conselleria d'Infraestructures i Transport

Tabla de Contenido

1. Introducción

1.1. Objeto

Este procedimiento describe la configuración de un controlador de dominio para aceptar los certificados de incio de sesión en Windows emitidos por la Autoritat de Certificació de la Comunitat Valenciana.

1.2. Ámbito y deber de lectura

Es aconsejable que este procedimiento sea leído por todos los administradores de sistemas de aquellas organizaciones que vayan a utilizar certificados de logon emitidos por ACCV.

1.3. Clasificación

"La información contenida en este documento se ha clasificado como: PÚBLICO"

1.4. Archivado y publicación

- La ubicación de archivado: Repositorio documental de la ACCV.
- El medio de archivo: Formato electrónico
- La fecha de inicio de archivado: 19/12/06
- El periodo de conservación: Indefinido
- La persona responsable: Administradores de sistemas.
- Lugar de publicación: http://www.accv.es/descargas-manuales_c.htm y http://www.accv.es/descargas-manuales_v.htm.
- Responsable de la publicación: Responsable de Web.

1.5. Responsabilidades

1.5.1. Responsabilidad de la preparación, la revisión, la aprobación y el mantenimiento del procedimiento

Responsable de la preparación: ACCV.

Responsable de revisión: ACCV.

Responsable de aprobación: ACCV.

Responsable del mantenimiento del procedimiento: ACCV.

1.5.2. Responsabilidad general del cumplimiento del procedimiento

Administradores de sistemas de aquellas organizaciones que vayan a utilizar certificados de logon emitidos por ACCV.

1.5.3. Responsabilidades parciales

ACCV.

1.6. Referencias

http://support.microsoft.com/kb/295663/

http://support.microsoft.com/kb/281245

http://support.microsoft.com/kb/291010

1.7. Definiciones

ACCV: Autoritat de Certificació de la Comunitat Valenciana.

.msi: Microsoft Installer.

NTAuth

Ldp

1.8. Requisitos

CD Windows Server (2002 o 2003).

1.9. Listado de apéndices

No aplicable.

2. Desarrollo

En este manual se dan las las instrucciones para habilitar un proceso de inicio de sesión mediante tarjeta inteligente con una entidad emisora de certificados (CA) distinta de Microsoft.

Active Directory debe confiar en una entidad de certificación para autenticar a usuarios en función de los certificados de esa CA. Las estaciones de trabajo con tarjeta inteligente y los controladores de dominio se deben configurar con los certificados adecuados.

Los pasos a seguir para configurar un controlador de dominio para que acepte los certificados de logon emitidos por la Autoritat de Certificació de la Comunitat Valenciana (ACCV) son:

1. Conseguir las herramientas necesarias para configurar un controlador de dominio.
2. Importar los certificados de las CA en el sistema.
3. Hacer que el sistema reconozca los certificados.
4. Añadir el certificado de controlador de dominio.

2.1. Conseguir las herramientas necesarias para configurar un controlador de dominio.

El certificado de inicio de sesión en tarjeta inteligente debe emitirlo una CA que esté en el almacén *NTAuth*. Para hacer la configuración, el administrador del sistema necesita el *CD Windows Server (2000 o 2003)* para instalar las herramientas necesarias, *Support Tools*. Siga los pasos a continuación:

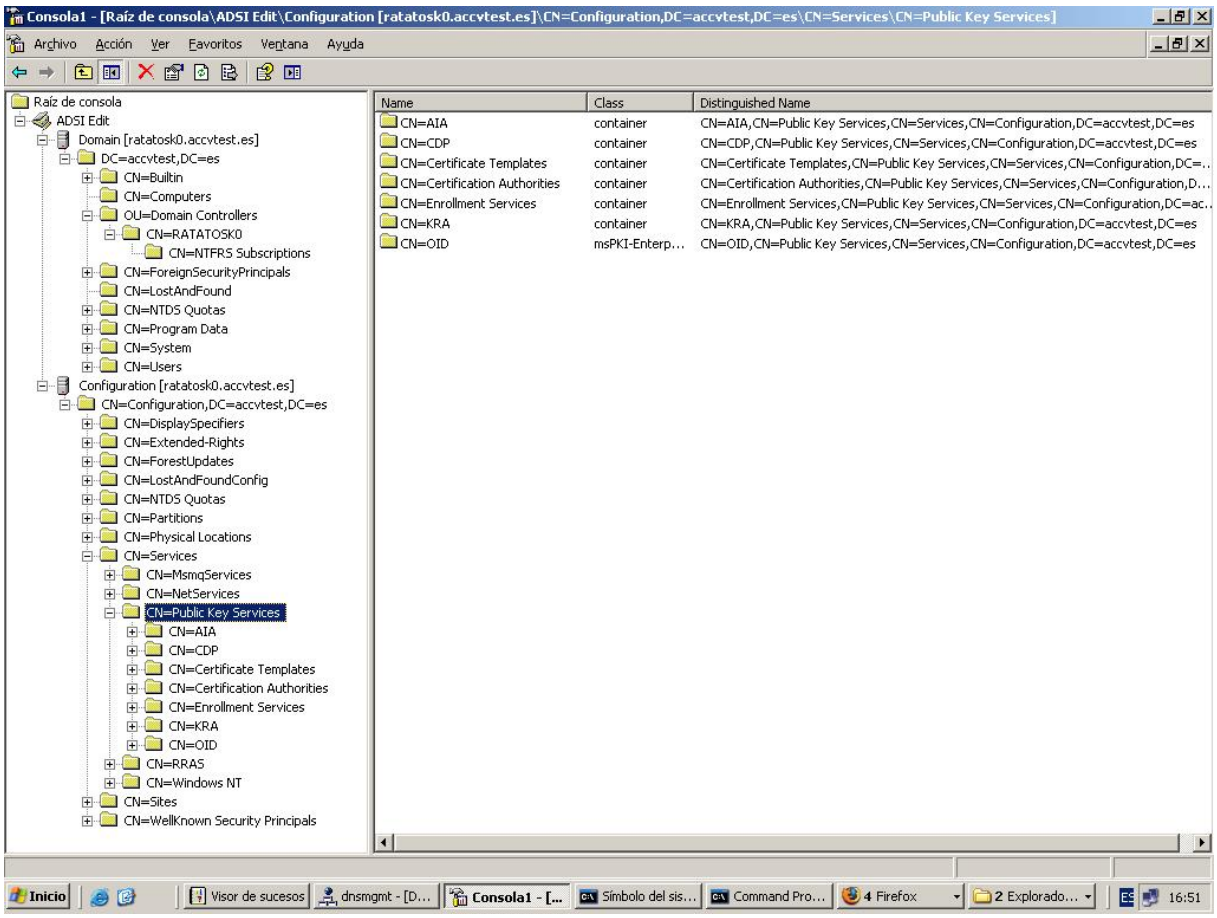
Explorar el CD y acceder a la ruta *D:\SUPPORT\TOOLS*

Ejecutar el fichero *SUPTOOLS.MSI.* Es una instalación típica, hacer clic en *Siguiente* hasta pinchar el botón *Finalizar*.

A continuación, desde la línea de comandos, ejecutar el comando *mmc.* Automáticamente, se lanzará una consola.

Ir al menú *Archivo/Agregar o quitar complemento.* Señalar *Adsiedit* en el cuadro de diálogo. En el campo *Connect to* apuntar el dominio en cuestión. Pulsar el botón *Aceptar* dos veces.

Para continuar observe la siguiente imagen:

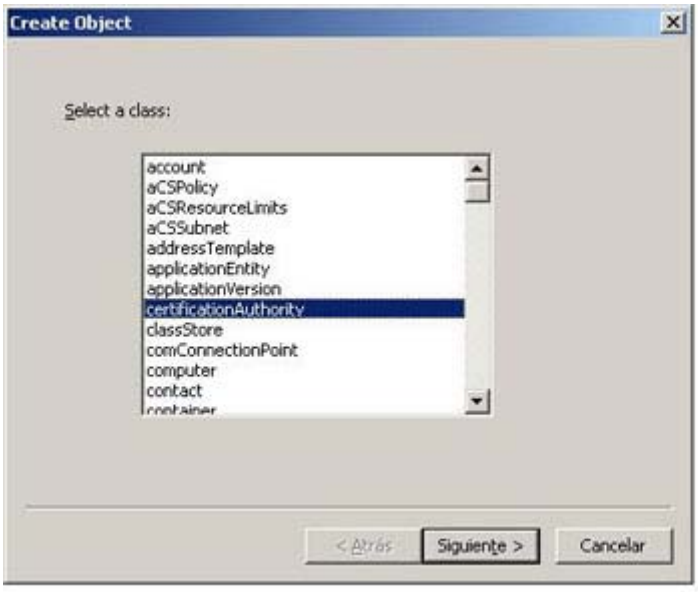


Se tiene que crear el objeto *NTAuth*, que no viene definido por defecto, a no ser que la Autoridad de Certificación sea la nativa de Microsoft.

El almacén *NTAuth* se encuentra dentro de la rama *Configuration* del bosque. Por ejemplo, he aquí una ubicación de ejemplo:

> *LDAP://server1.name.com/ CN=NTAuthCertificates, CN=Public Key Services, CN=Services, CN=Configuration, DC=name, DC=com*

En la rama *CN= Services / Public Key.* Al pulsar el botón derecho del ratón debe hacer clic en *New object*, seleccionar *certificationAuthority*, tal y conforme aparece en la imagen siguiente.



Al pulsar sobre el botón *Siguiente*, debe coincidir cada campo descrito con el valor a continuación:

Value: NTAuthCertificates. Pulsar *Siguiente*,

certificationAuthority → value: 0x0. Pulsar *Siguiente*,

authorityRevocationList → value: 0x0. Pulsar *Siguiente*,

certificateRevocationList → value: 0x0. Pulsar *Finalizar*.

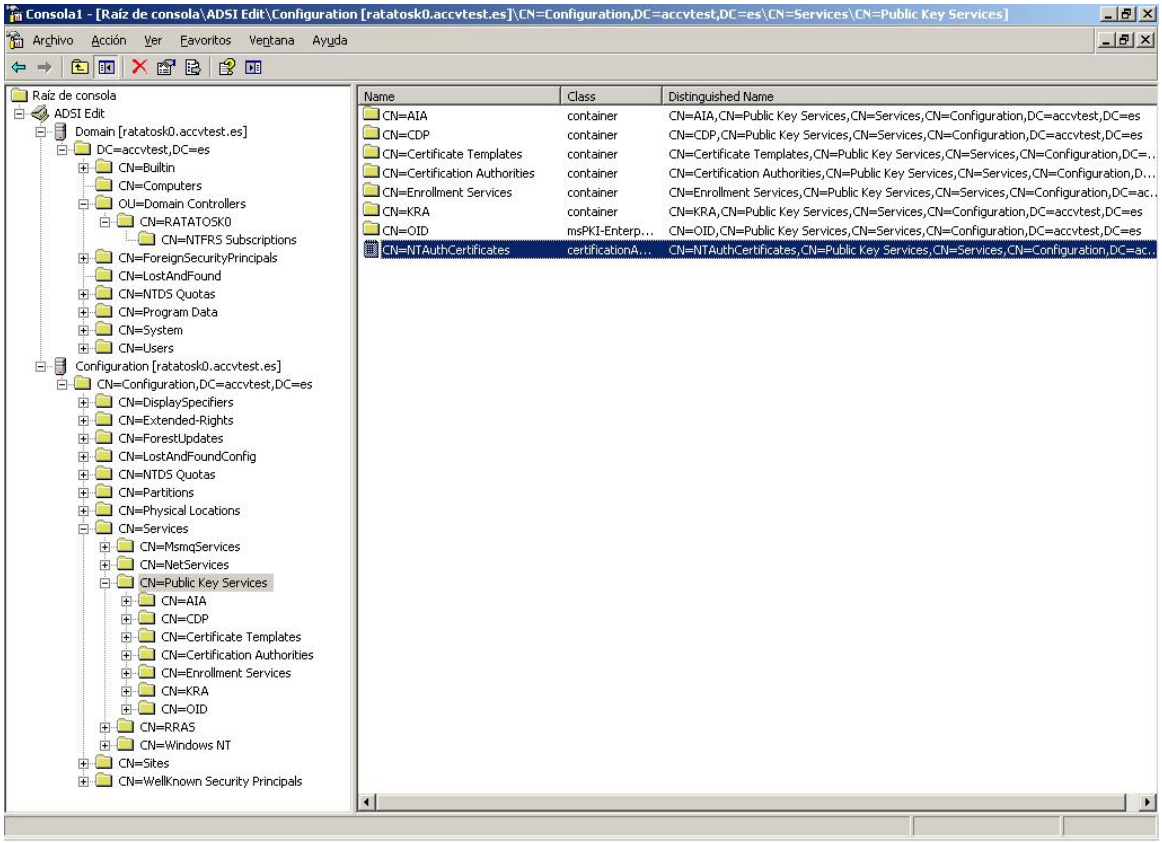
2.2. Importar los certificados de las CA en el sistema.

Descargar el *kit de recursos* desde *Microsoft Installer* con el fin que el complemento *PKIView* se añada como extensión del sistema.

Desde la consola, ir al menú *Archivo, Agregar o quitar complemento.*

Pinchar el botón *Agregar*. Señalar la opción *Enterprise PKI*, pulsar sobre el botón *Agregar*. A continuación pulsar los botones *Cerrar* y *Aceptar*.

Desde la raíz de la consola\ Enterprise PKI, pulsar el Menú *Manage AD Container* con el botón derecho. Pinchar la opción (en el repositorio *NTAuth*) tal y como indica la pantalla siguiente.

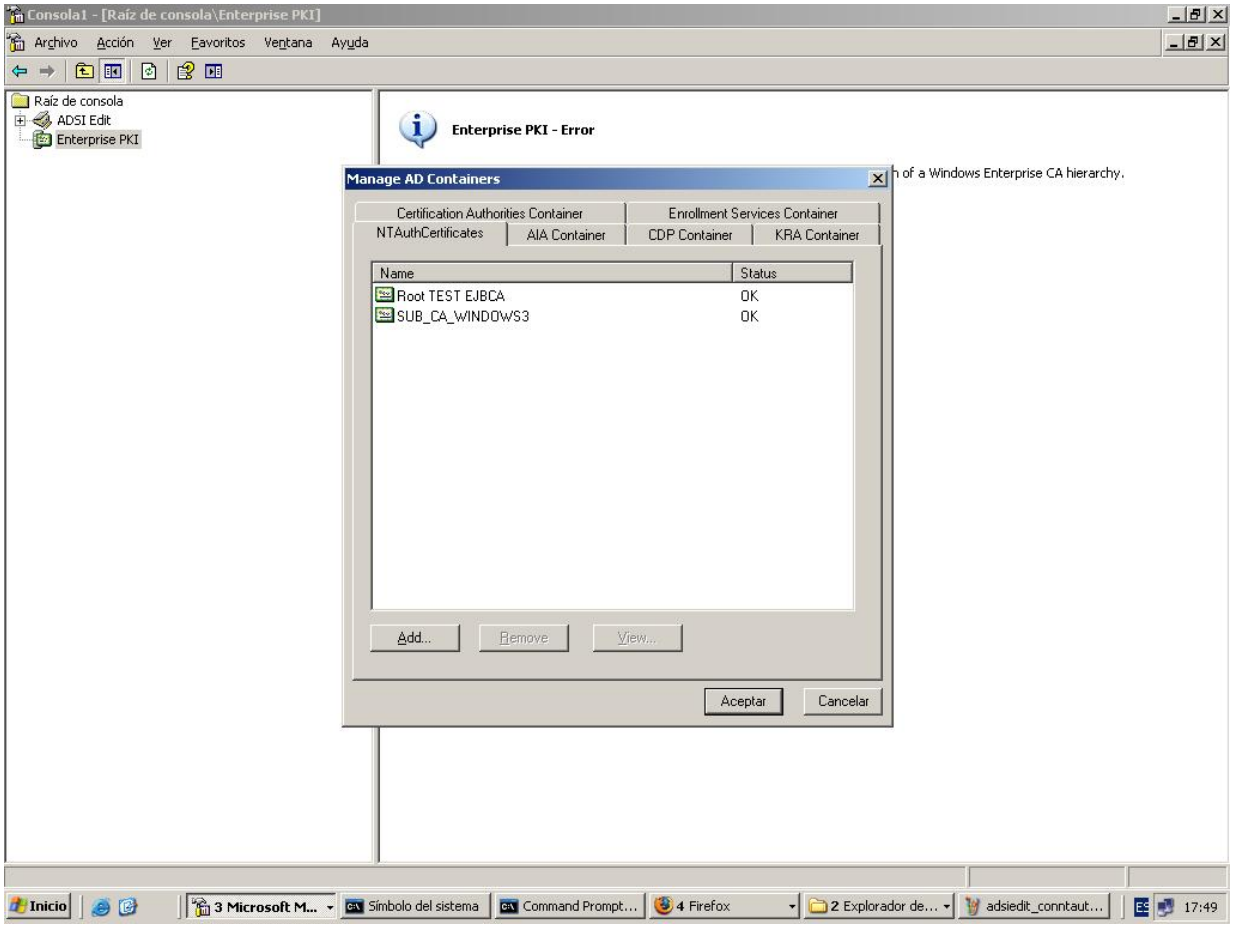


Descargar los certificados de la ACCV desde http://www.accv.es/solicitalogon_c.htm .

Instalar primero 

. Después, y de la misma manera, instalar el Certificado 

. Finalmente debe aparecer la pantalla siguiente:



2.3. Hacer que el sistema reconozca los certificados.

Desde la consola, ir al menú *Archivo, Agregar o quitar complemento.*

Pinchar el botón *Agregar*. Señalar la opción *Certificado*, indicar la *cuenta del equipo.* Pinchar el botón *Siguiente*, indicar *Local,* pinchar sobre los botones *Finalizar*, *Cerrar* y *Aceptar*.

Desde el punto de Entidades Emisoras raíz de Confianza, acceder a *Certificados* \ *todas las tareas*, pinchar sobre el botón *Importar*, *Examinar*, *Root CA.*

Desde el punto de Entidades Emisoras raíz de Confianza, acceder a *Certificados* \ *todas las tareas*, pinchar sobre el botón *Importar*, *Examinar*, *SUB_CA_WINDOWS3.*

Con los certificados de la ACCV registrados, el controlador de dominio ya puede reconocer todos los certificados de incio de sesión emitidos por dicha CA.

2.4. Añadir el certificado de controlador de dominio.

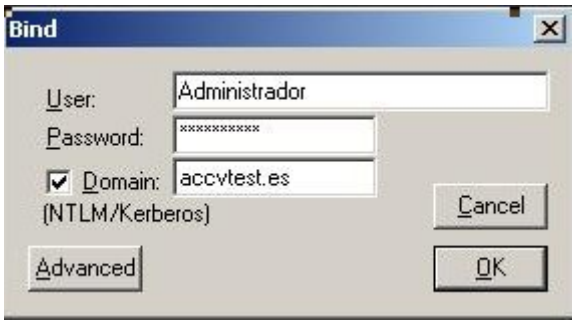
Son necesarios dos datos:

1. Nombre del Controlador. Se consigue en el campo *Descripción del equipo* de Mi PC\Propiedades del sistema\Nombre del equipo.

2. guid. Se consigue con la herramienta ldp.

Desde la consola, ir al menú *Connection*. Seleccionar *Server*: localhost.

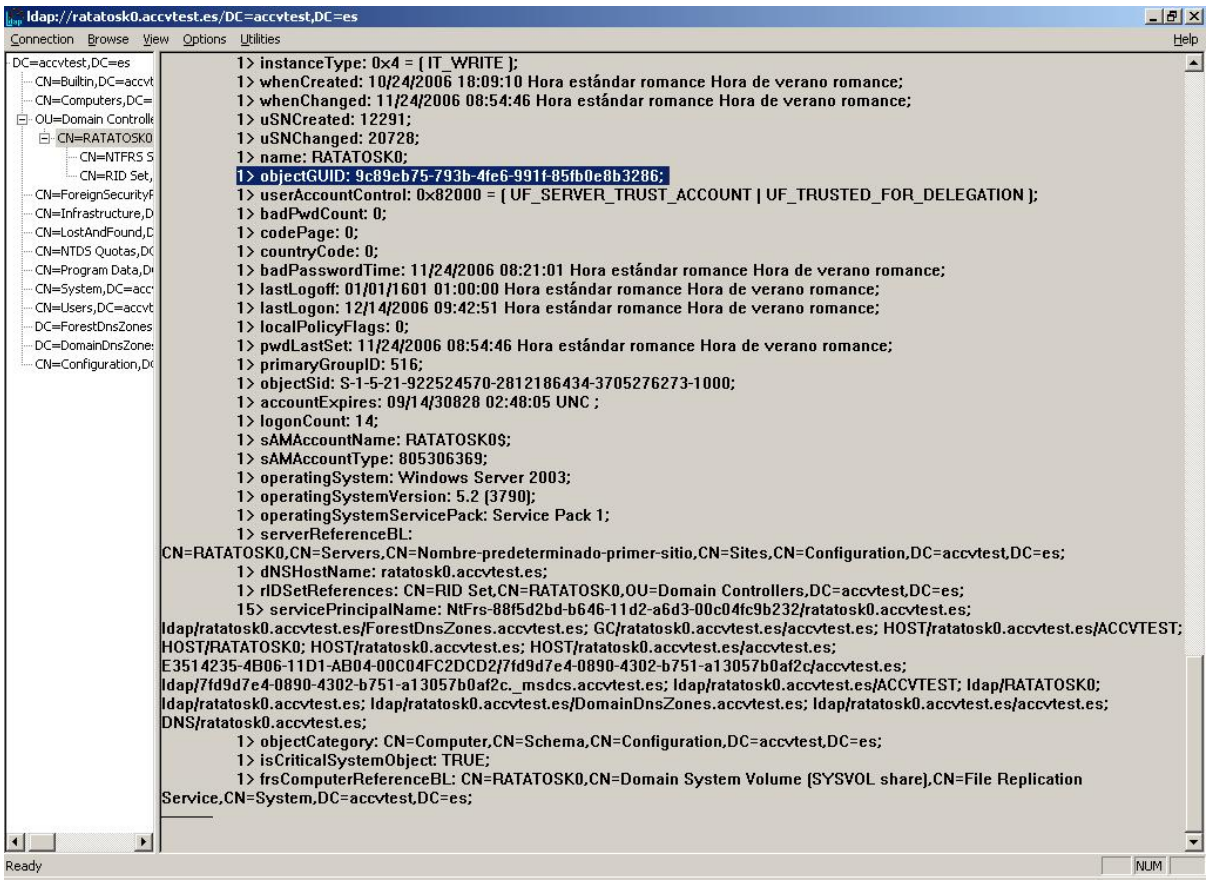
Nuevamente *Connection.* Seleccionar *Bind.* Indicar el *User* (siempre con privilegios de administrador). A continuación, pulsar sobre el botón *Connect.*



Ir a *View, tree, BaseDN DC= , DC= .* Pulsar el botón *ok.*

Ir a *DC*, apartado *OU*, seguir con *CN* (nuestro controlador de dominio).

Observar en la pantalla el dato correcto.



Con este dato (*objectGUID*) más el nombre del dominio se solicita el certificado .p12 a la ACCV.

Después de tener el certificado emitido por la ACCV obtendrá un .p12.

Ejecutar en la línea de comando, *mmc.* Desde la consola, ir al menú *Archivo, Agregar o quitar complemento.* Pinchar el botón *Agregar*. Señalar la opción *Certificado*, indicar la *cuenta del equipo.* Elegir la opción *equipo local,* a continuación pulsar el botón *Aceptar*.

La siguiente tarea es la importación típica de un certificado .p12. Desde la opción *Personal,* indicar *todas las tareas*, *Importar*. Pulsar *Siguiente* hasta acabar en el botón *Finalizar*. Automáticamente, el certificado se ha colocado en el almacén correcto.

Pulsar el botón *Cerrar*. Cerrar CDP.

Para comprobar que la operación ha sido satisfactoria, reinicie el sistema e inicie sesión con un certificado de logon del dominio. Se producirá una notificación en el visor de procesos con la información obtenida del acceso.

3. Apéndices

No aplicable