User Documentation for SmartPolicy

Version 1.2

Prepared by: "Vincent Le Toux"

Date: 07/02/2013

MySmartLogon

Table of Contents

Revision History

This section records the change history of this document.

Name	Date	Reason For Changes	Version
Vincent Le Toux	07/02/2013	Creation	1.0
Frédéric Bourgeois	23/02/2013	Update	1.1
Vincent Le Toux	03/07/2014	Smart Policy v2	1.2

Introduction

Smart Policy allows the configuration of existing certificates stored on smart cards issued by third party authorities (For example the US Department of Defense [CAC smart card] or European Government [EID Cards]). It does not install third party components. It just modifies the configuration of the active directory, the client computers and the domain controllers.

Security Notice

By using this tool you are accepting the following security risks:

- **A security breach of the third party certificate authority can lead to the generation of certificates which can be used to logon to your system**
- **This tool can be used to setup a credential for any account, including the administrator account**

System Specifications

The Operating systems supported to run SmartPolicy.exe are:

- Windows Vista and later
- Windows 2008 and later

Target domain controller operating systems are:

- Windows 2003 and later for UPN Mapping only
- Windows 2008 and later for UPN Mapping and Explicit mapping

Target domain member operating systems are :

- Windows XP and later for UPN Mapping only
- Windows Vista and later for UPN Mapping and Explicit mapping

Requirement

The ADCS (Active Directory Certificate Services) MUST be installed. It is needed to provide authentication certificate to the domain controllers.

Installation

Smart Policy is delivered as a standalone program. No procedure is needed before launching the tool.

But you ***MUST*** accept the license in order to proceed.

Mapping

Smart Policy can perform two kinds of mapping depending of the certificate:

- UPN mapping
- Explicit mapping

UPN mapping

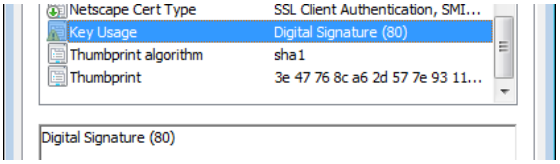
The UPN mapping is the traditional way of configuring smart card logon in an Active Directory. It is the only method working before Windows Vista.

To find the user account related to the certificate, Windows looks for the SAN attribute to identity the UPN of the Windows account.

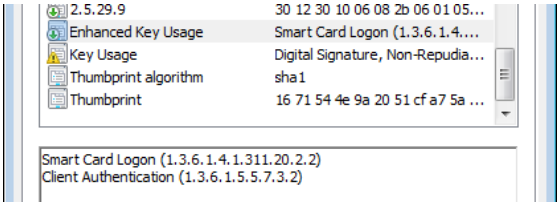
The requirements are:

- for the certificate
  - A **CRL Distribution Point (CDP)** location specified in the certificate (where CRL is the Certification Revocation List) which must be populated, online, and available. This requirement can removed using a GPO. For example:

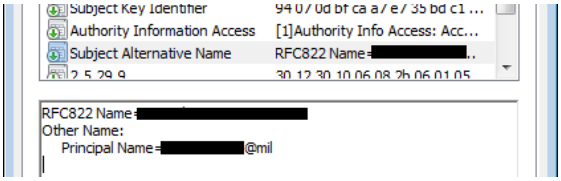
  - **Key Usage** = Digital Signature



  - **Basic Constraints** [Subject Type=End Entity, Path Length Constraint=None] (Optional)
  - **Enhanced Key Usage** =
    - Client Authentication (1.3.6.1.5.5.7.3.2)
      (The client authentication OID) is only required if a certificate is used for SSL authentication.)
    - Smart Card Logon (1.3.6.1.4.1.311.20.2.2)



- **Subject Alternative Name** = Other Name: Principal Name= (UPN).
  For example:
  UPN = user1@name.com
  The UPN OtherName OID is : "1.3.6.1.4.1.311.20.2.3" (it must be ASN1-encoded UTF8 string)



- **Subject** = Distinguished name of user. This field is a mandatory extension, but the population of this field is optional.

- For the user account
  - The UPN of the certificate must match the UPN of the account
  - The UPN must not be used on another account

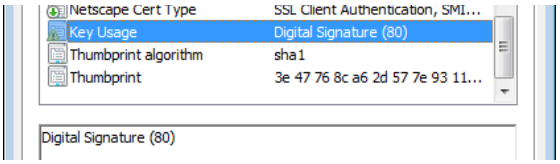
Explicit mapping

The Explicit mapping has been designed for certificates which don't have a UPN. To find the user account related to the certificate, Windows looks for the altSecurityIdentity attributes of all Windows accounts to see if this certificate has been registered to any account. The mapping can be done using the subject, the SHA1 hash or on the RFC822 name.

The requirements are not as strict as the UPN mapping but some requirements remain:

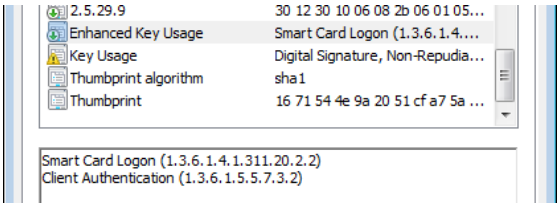
- A **CRL Distribution Point (CDP)** location specified in the certificate (where CRL is the Certification Revocation List) which must be populated, online, and available. This requirement can removed using a GPO. For example:

- **Key Usage** = Digital Signature



- **Enhanced Key Usage** =
  - **No EKU** or one of the following :

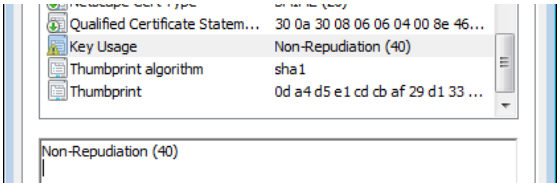
- Client Authentication (1.3.6.1.5.5.7.3.2)
  (The client authentication OID) is only required if a certificate is used for SSL authentication.)
- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)



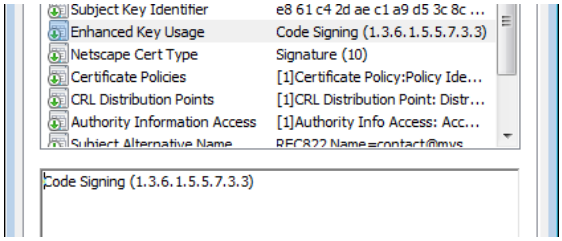
Certificates which can't be used with Smart Policy

Certificates:

- With a **Key Usage** different from "Digital Signature"



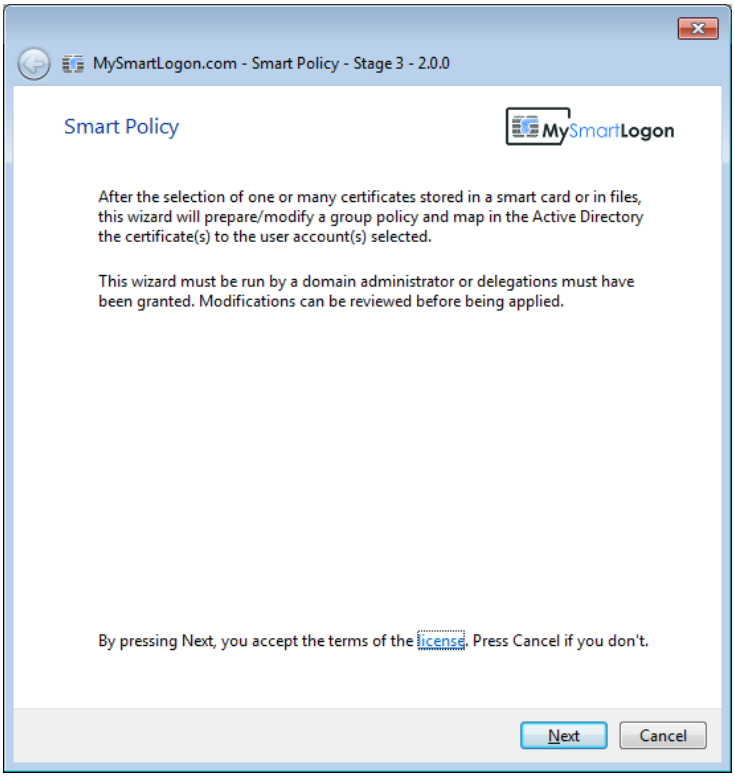
- With **Enhanced Key Usage** set and which doesn't contain :
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - nor Smart Card Logon (1.3.6.1.4.1.311.20.2.2)



User Interface

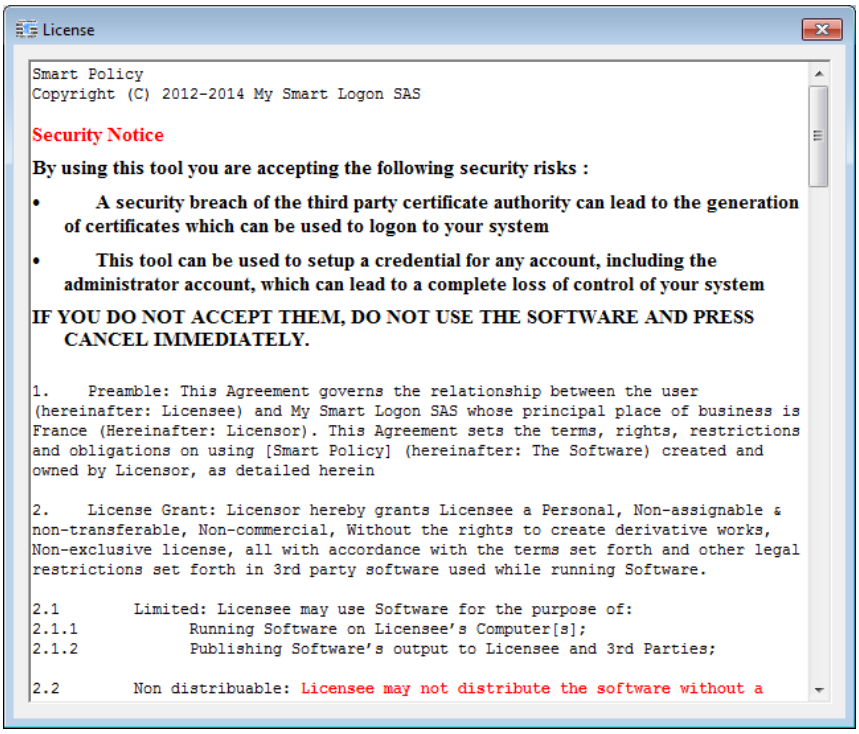
First dialog

The first dialog shown by Smart Policy presents the program. This screen captures the users' consent if he/she clicks on Next. It is called a "Click-wrap license agreement". The license can be viewed by clicking on the "license" link.

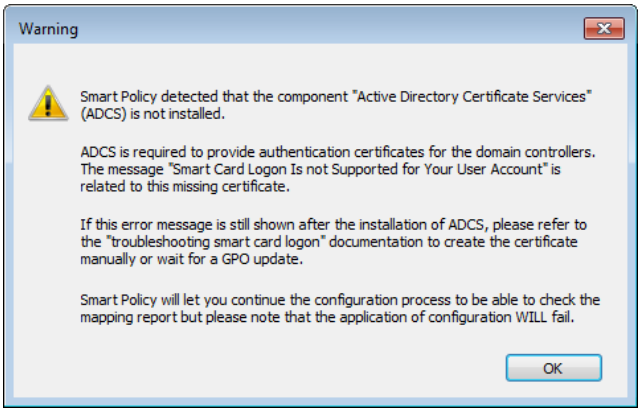


The license is shown with the security notice of this program.

If you don't accept the terms of the license, close the program by clicking on "Cancel" or press "Escape" on the keyboard.

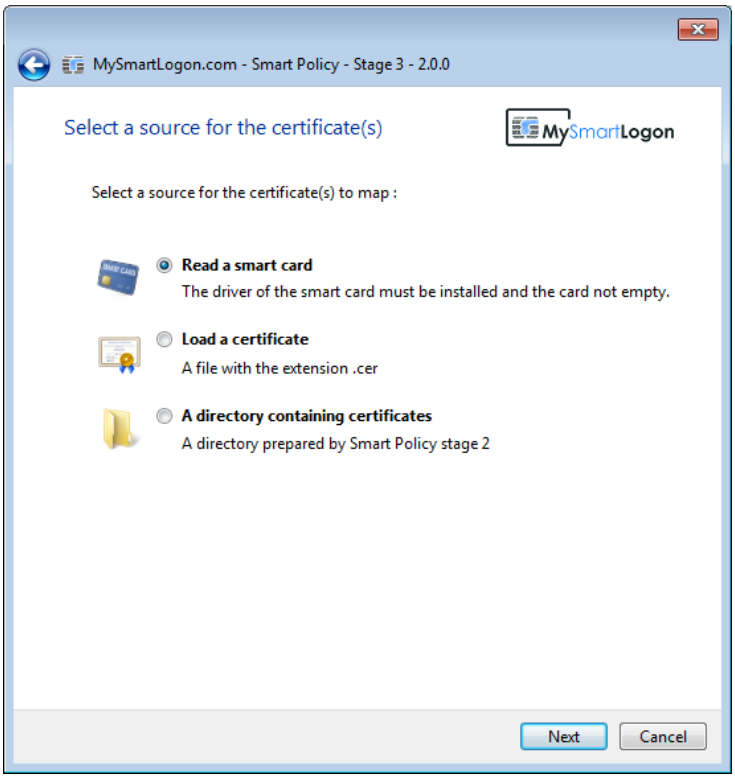


Smart Policy is then doing a check to detect if ADCS is installed. If not, the following message is shown:



Certificate's source dialog

This dialog allows the selection of a source for the certificate(s) to map.

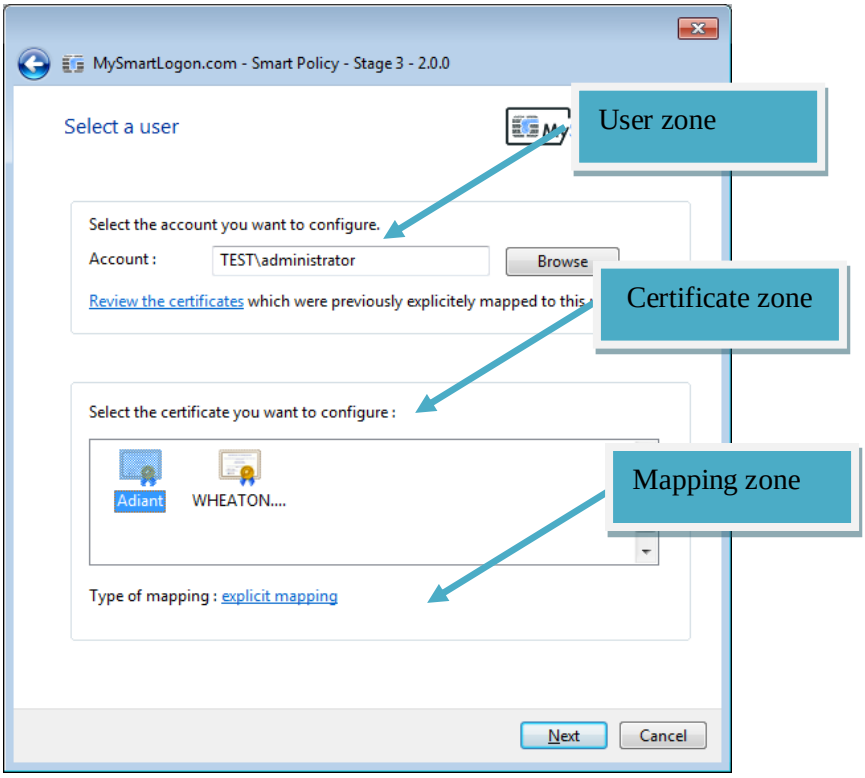


It can be a "smart card" having a CSP or a minidriver installed, a cer file in binary encoding or a directory prepared by Smart Policy stage 2.

If a smart card or a certificate file is selected, the user will be redirected to the next dialog.

Else the user will be redirected to the "mass mapping" dialog.

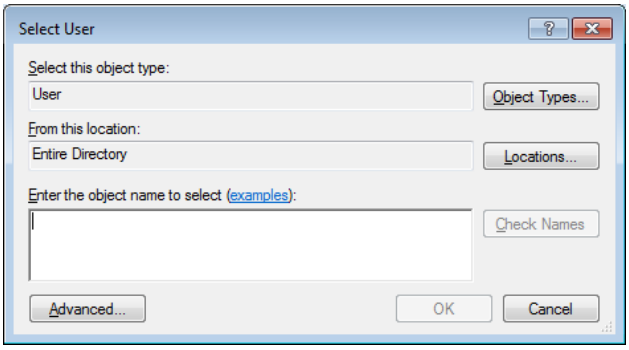
Smart card or certificate file dialog



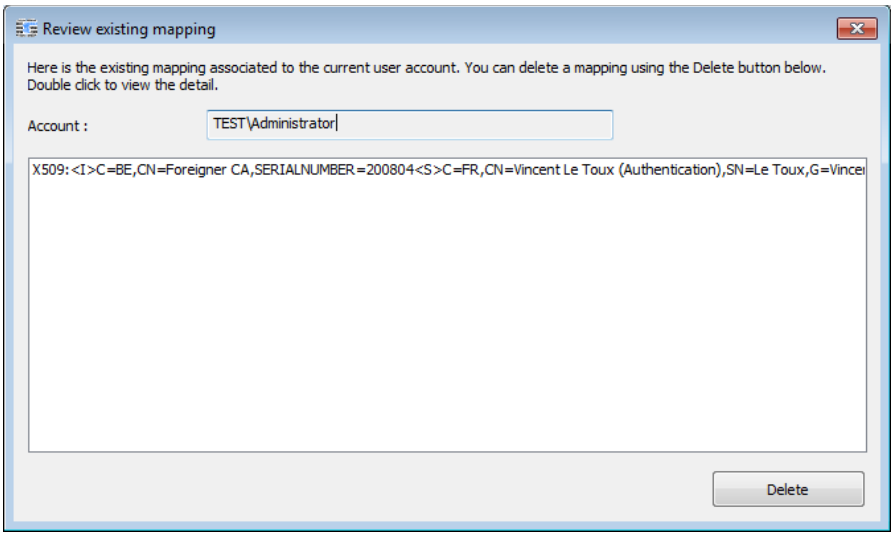
This dialog has 3 zones:

- the user zone

By default, the current user is automatically selected. Any user belonging to the domain can be selected by clicking on Browse.



If any explicit mappings exist for this user, they can be reviewed by clicking on the link "Review the certificates". The following dialog will be shown, where after selection, a mapping can be removed.



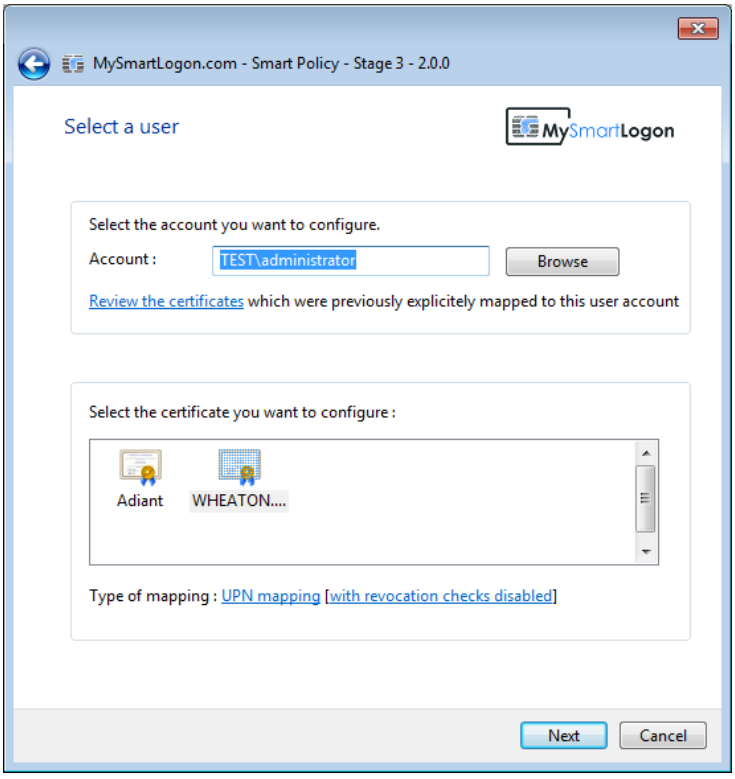
- the certificate zone

If a certificate file has been chosen, the certificate stored in the file will displayed. On a smart card, every certificate will be displayed.

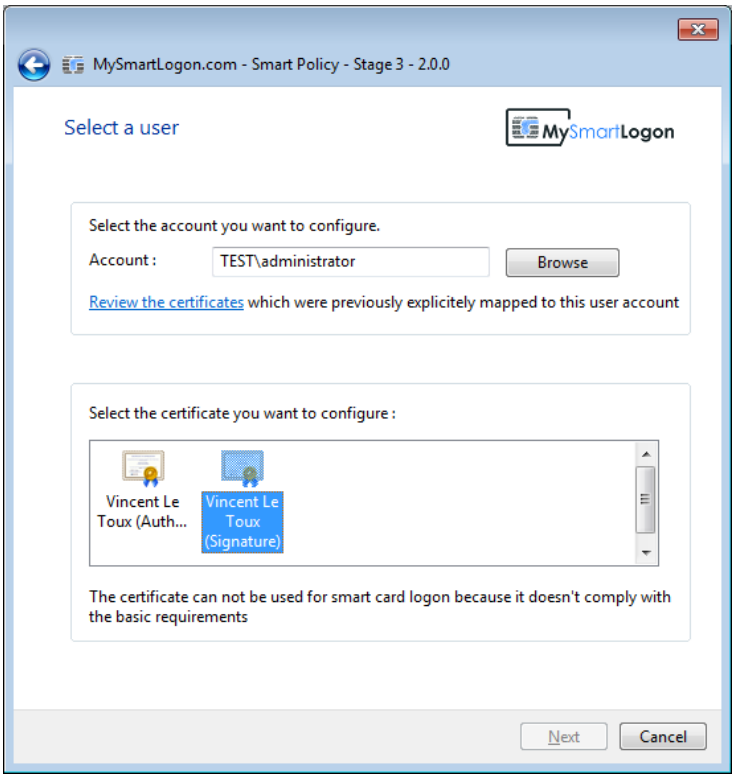
- the mapping zone

The mapping zone will display what mapping can be used, if the CRL checks have to be deactivated or any errors.

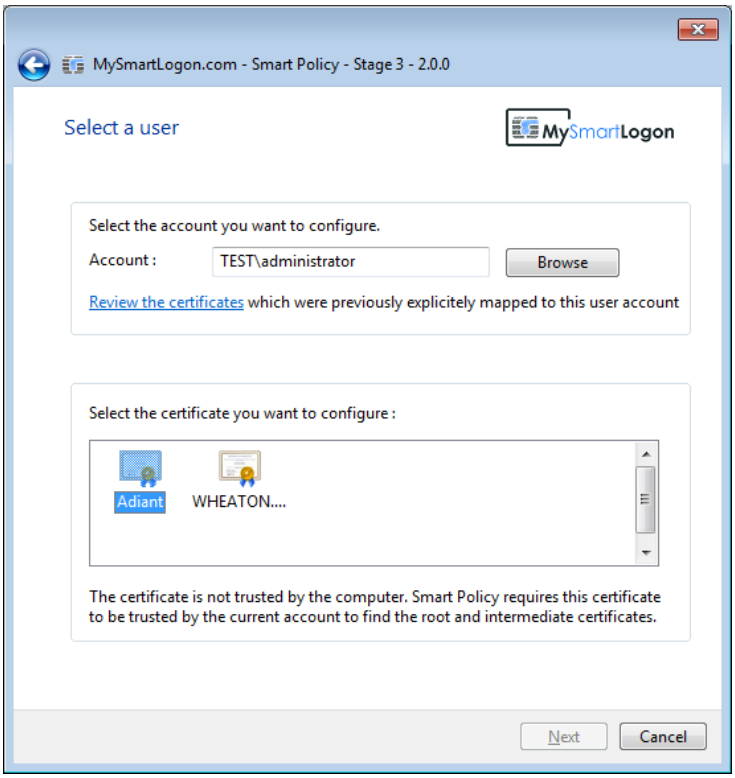
In the following example, the certificate chosen will be mapped using the UPN method with the certificate revocation checks disabled.



In the next example, smart policy detected that the certificate cannot be used for smart card logon, even if some security policies are disabled.

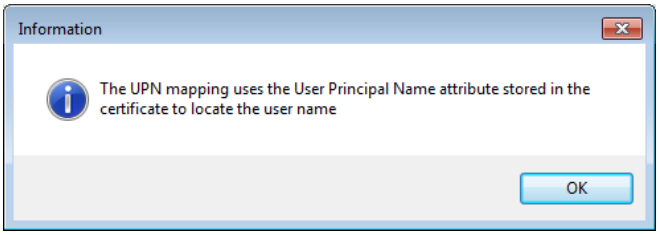


In the next example, Smart Policy couldn't build the certificate chain to determine the root and intermediate certificates. Make sure the certificate is trusted before continuing.

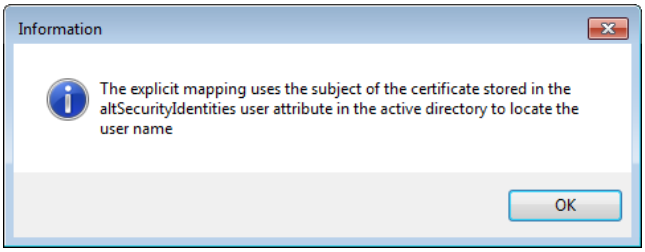


Here are the hints which can be displayed when the user click on the links:

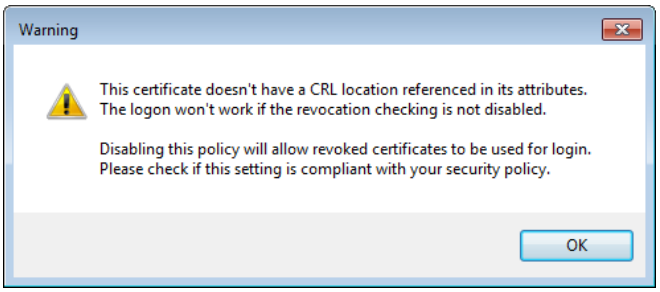
UPN mapping:



Explicit mapping:



With revocation checks disabled:



The next screen will be the CRL checking dialog

Mass mapping dialog

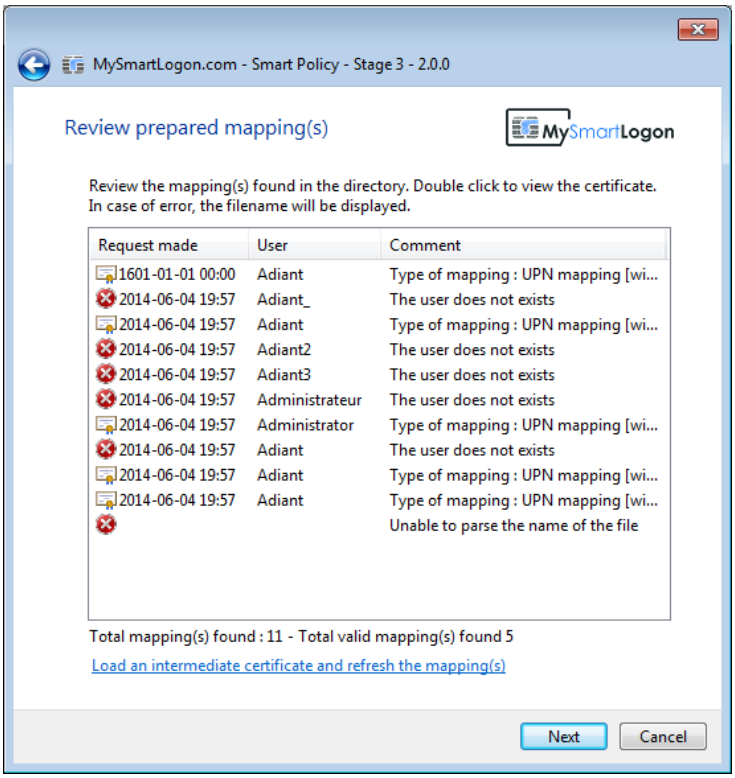
If a directory has been chosen in the source dialog, this dialog is shown.

For each certificate, Smart Policy extracts from its name the date of the mapping, the user concerned by the mapping, and a comment to display the type of mapping chosen or any error related.

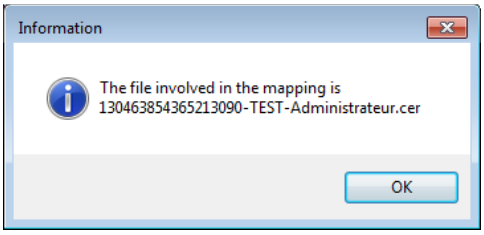
In the next example, every line having an error mark will be ignored. In this case, a double click shows the file involved to be able to better diagnostic the problem.

The directory has to be validated by a security officer before being selected: a rogue certificate can lead a security issue.

Smart Policy does not check for duplicate certificates.



The following dialog is shown if the file cannot be used by Smart Policy.



If some root or intermediate certificates are known but not registered on the Windows certificate store, they can be loaded and the screen refreshed to take account of them.

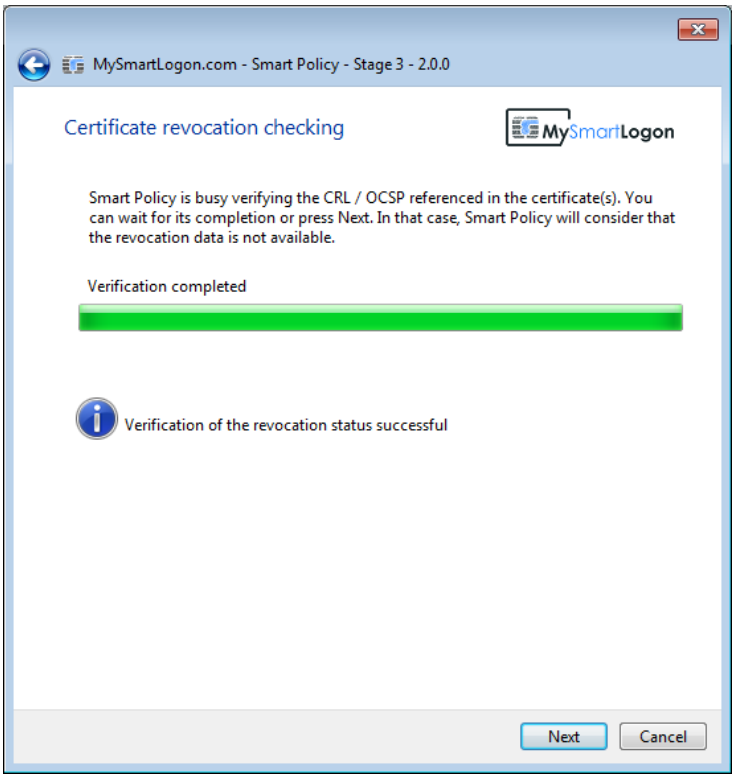
The next screen will be the CRL checking dialog

CRL checking dialog

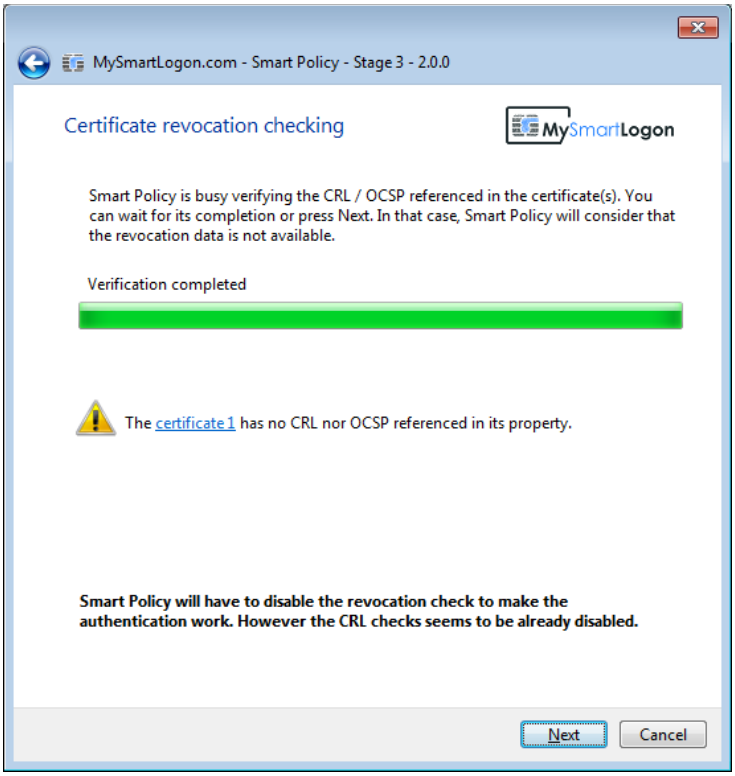
Before being mapped, Smart Policy checks if the certificates have a CRL Distribution Point (CDP) which is required by default, if the certificates have been revoked or if the CRL server is unavailable.

Smart Policy allows a timeout of 30 seconds per certificates. The verification can be interrupted at any time. If it is the case, Smart Policy will suggest that the CRL server can't be reach on the next dialogs.

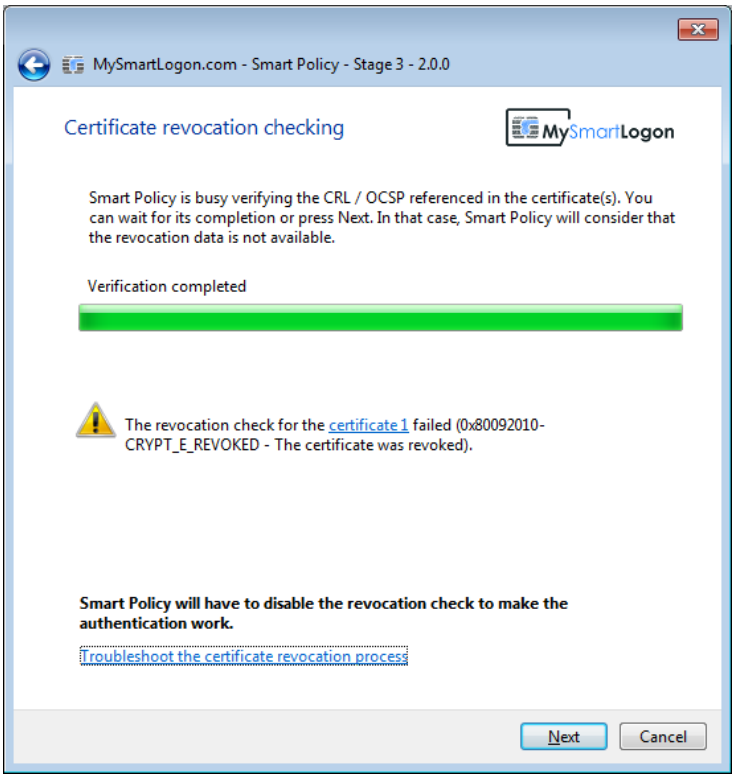
In the next screenshot a successful revocation check is shown.



If a certificate doesn't have a CDP property, the CRL checks must be disabled to be able to be used.



If the revocation check failed, the error is shown by the wizard. In the next example, a certificate was revoked.



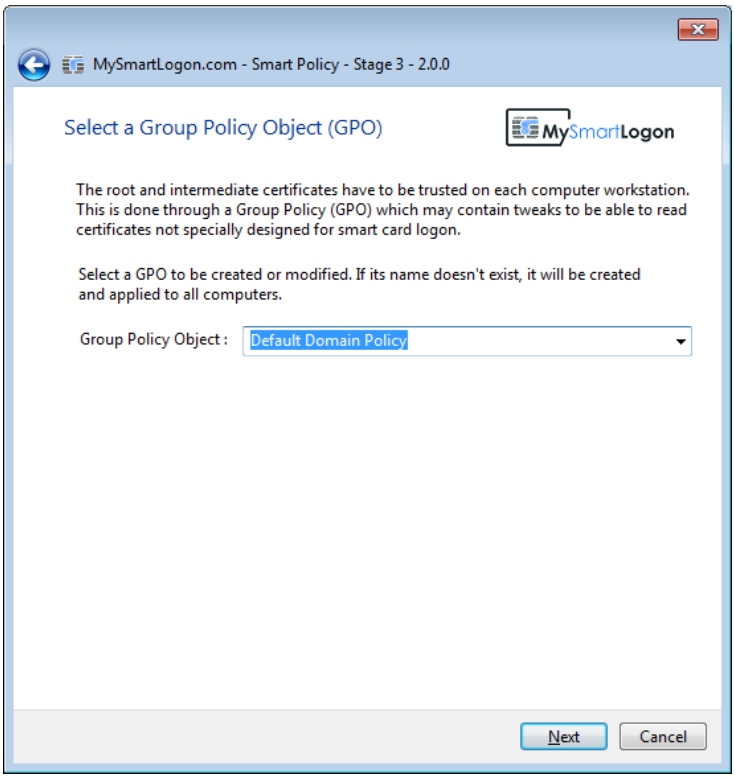
Note: The proxy parameter used by the user account and the SYSTEM account which performs the authentication is not the same. A successful CRL checking in this screen, even on the domain controller, doesn't mean that the authentication process will be able to connect to it.

Group Policy Object Dialog

Most of the tweaks needed for the smart card logon are located in a GPO. This dialog allows the user to select an existing GPO or to create a new one.

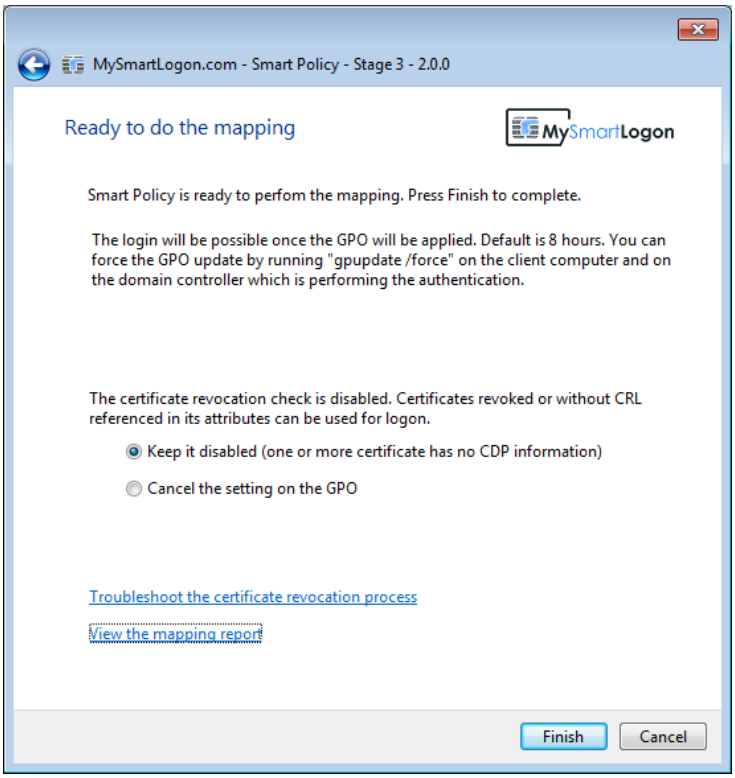
Note: if the keyboard is used to type the name of an existing GPO, the system will consider that it is a new one. If you need to select a GPO, pick its name in the listbox.

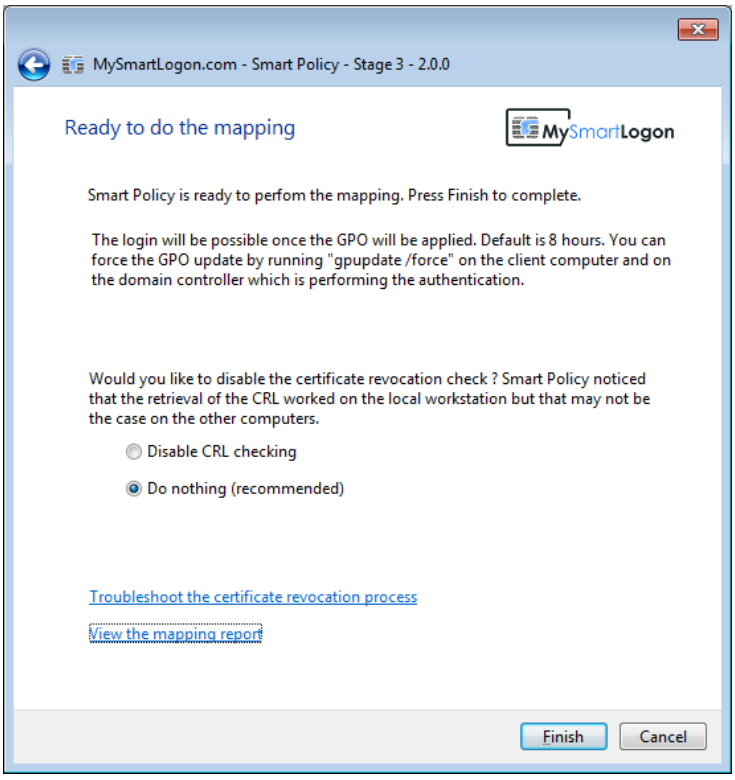
If a new GPO is created, it will be attached to all the computers of the domain. If you need to restrict the GPO to a subset of computers, create a new GPO and configure it according to your needs. Then select it.



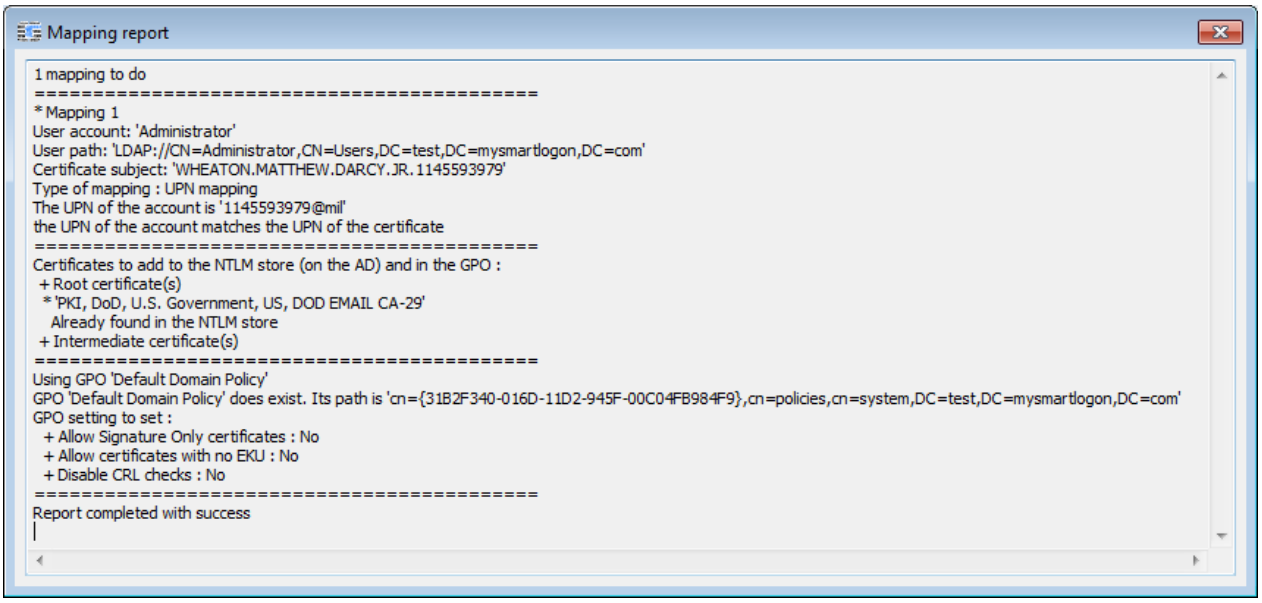
Final Dialog

The final screen allows the activation or the deactivation of the certificate revocation check. The text displayed will depend on the mapping, the existence of a CDP property or if the check has already been disabled.

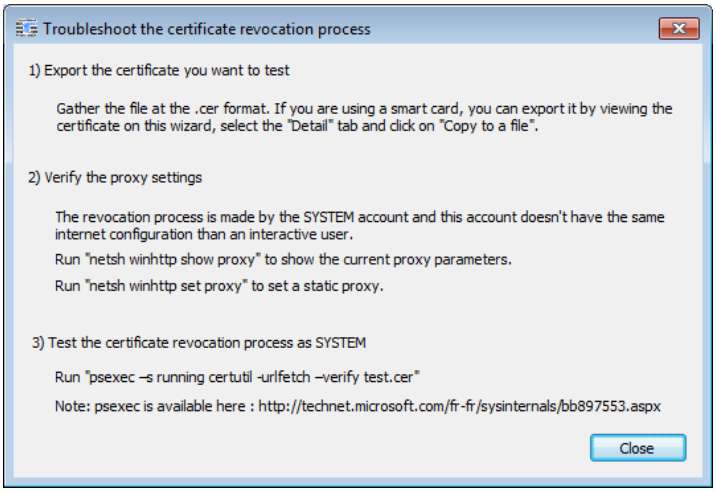




A mapping report can be shown to indicate what changes will be applied to the system.



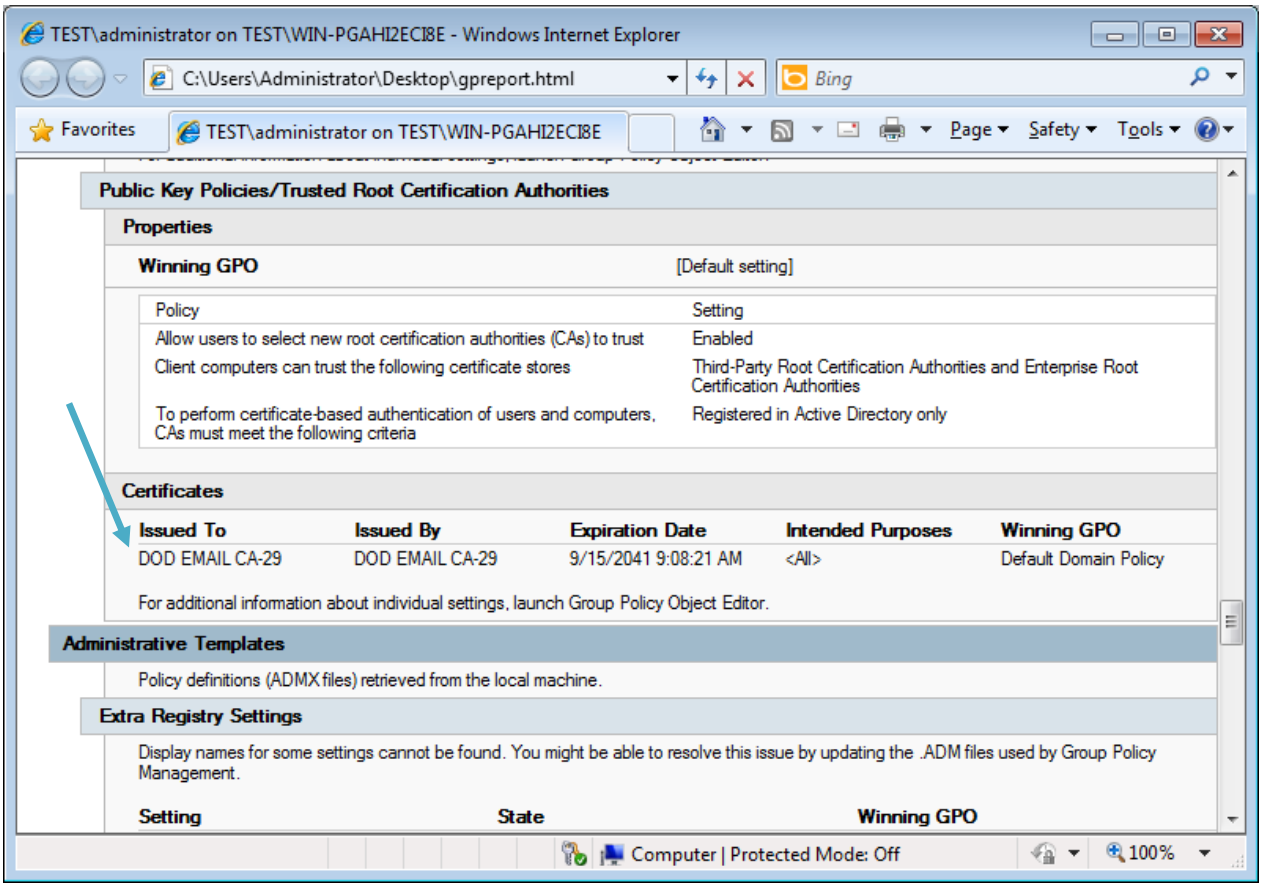
A reminder about the SYSTEM proxy configuration can be shown on demand ("Troubleshoot the certificate revocation process").



Annex - Check the GPO

The GPO modifications made by Smart Policy can be audited by issuing the command:

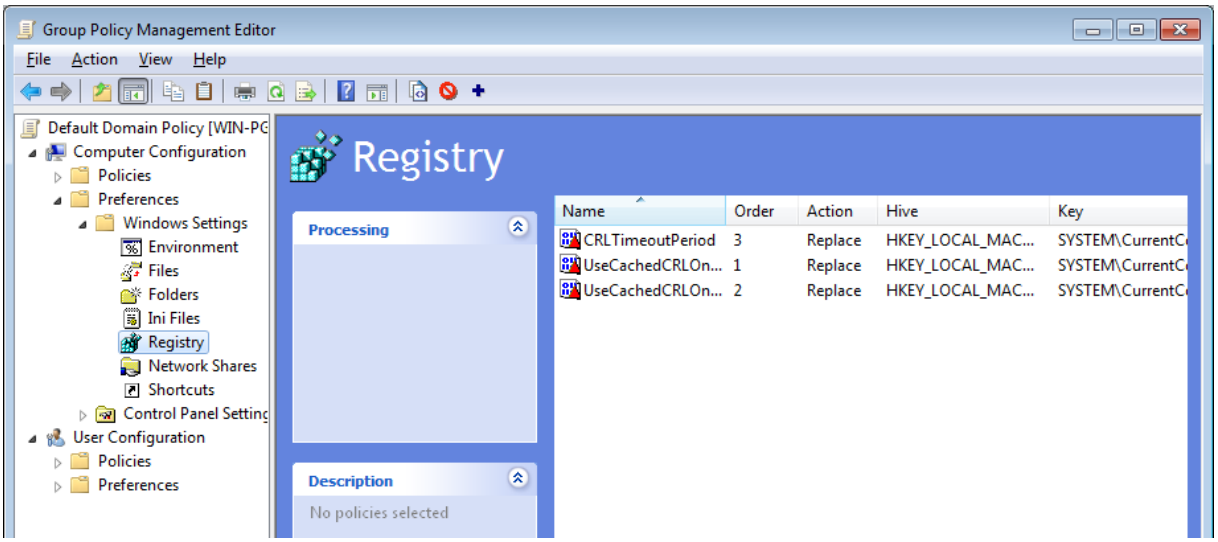
gpresult /h report.html



The settings located in the SYSTEM Hive are:

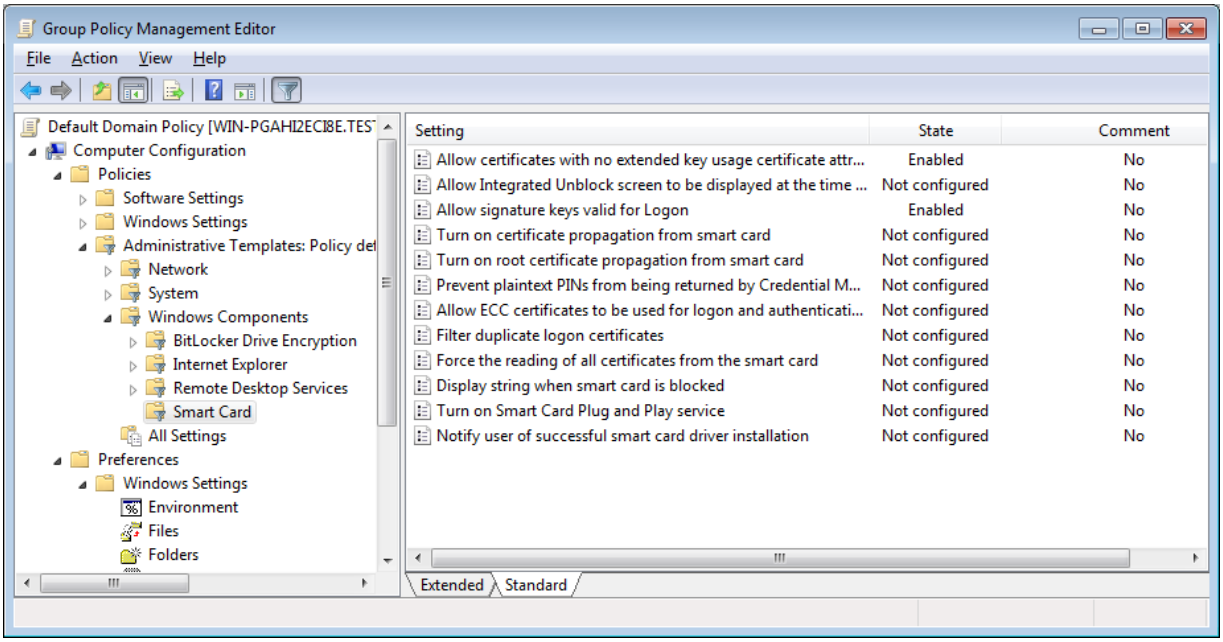
- Disable EKU checking
- Disable CRL checking

They can be audited by opening the Computer Configuration -> Preferences -> Windows Settings -> Registry as shown in the next screenshot.



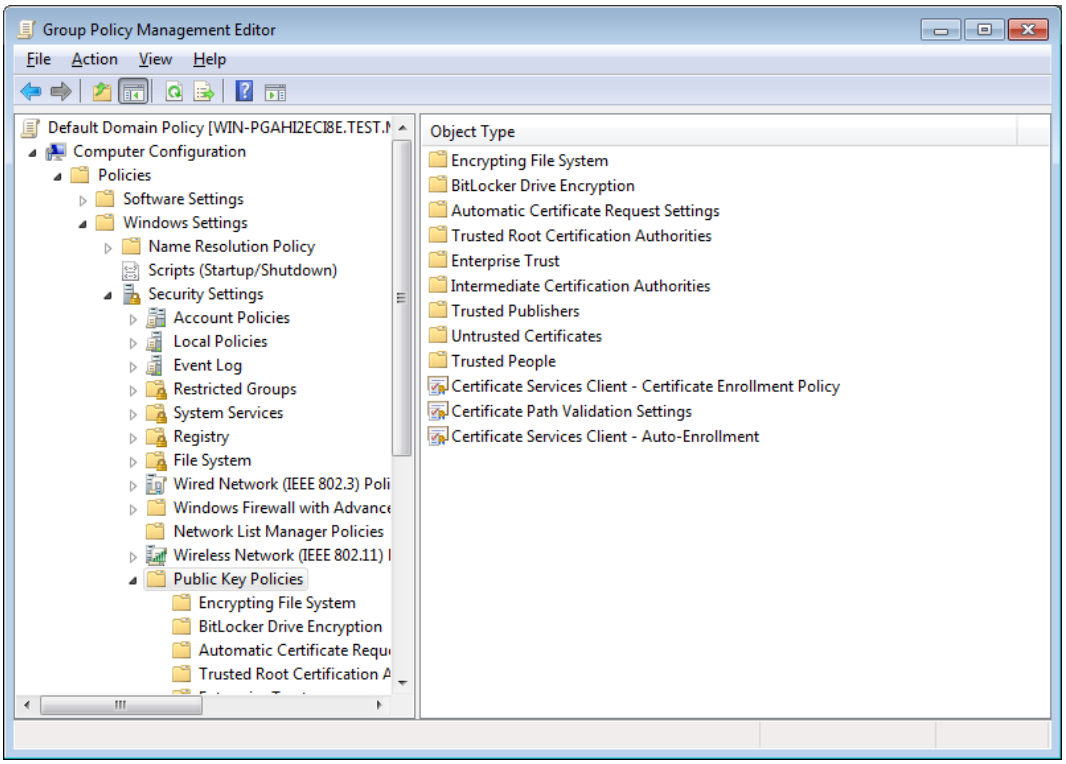
The settings located in the SOFTWARE Hive can be audited by opening the Computer Configuration->Policies->Administrative Templates -> Windows Components -> Smart Card:

- Disable EKU checking
- Allow smart card with signature only
- Read all certificates



The certificate appended can be audited in :

"Trusted root certification authorities" and "Intermediates Certification authorities" located in Computer Configuration -> Policies -> Windows Settings-> Public Key Policies

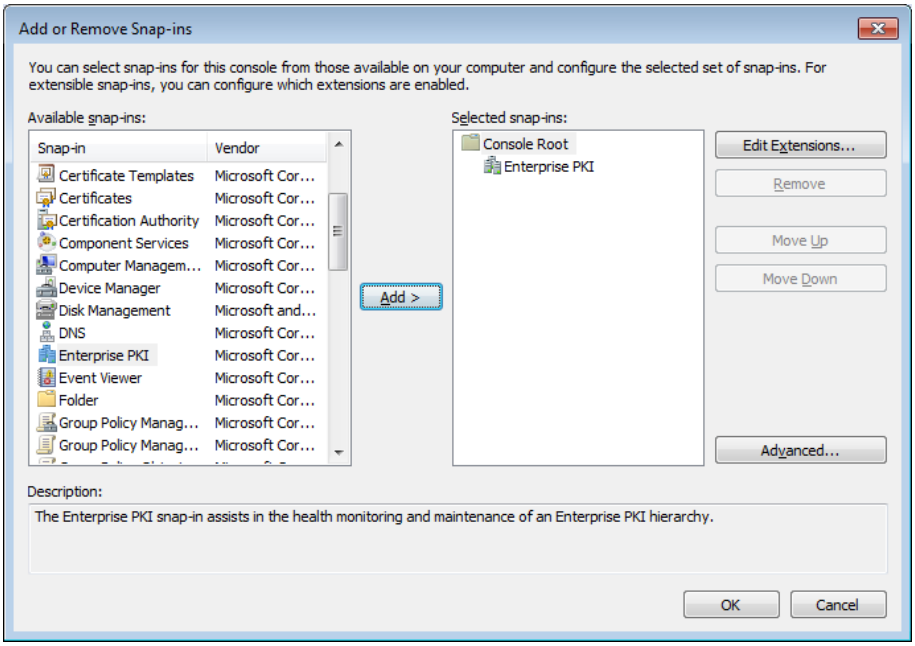

Group Policy Management Editor
File Action View Help
Default Domain Policy [WIN-PGAHI2ECI8E.TEST.
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Poli
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Requ
Trusted Root Certification A
Object Type
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment

Annex - Check the NTLM Store

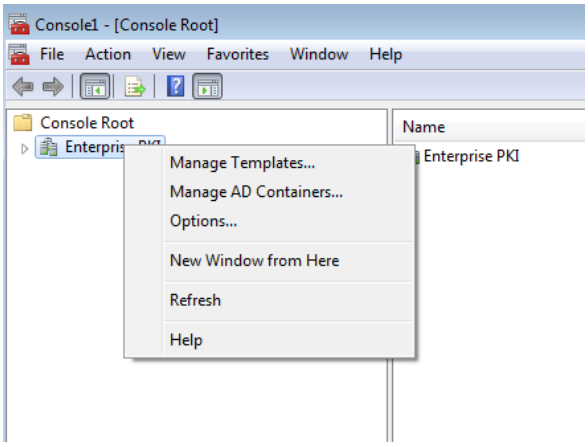
Method 1: Using the PKI Health Tool

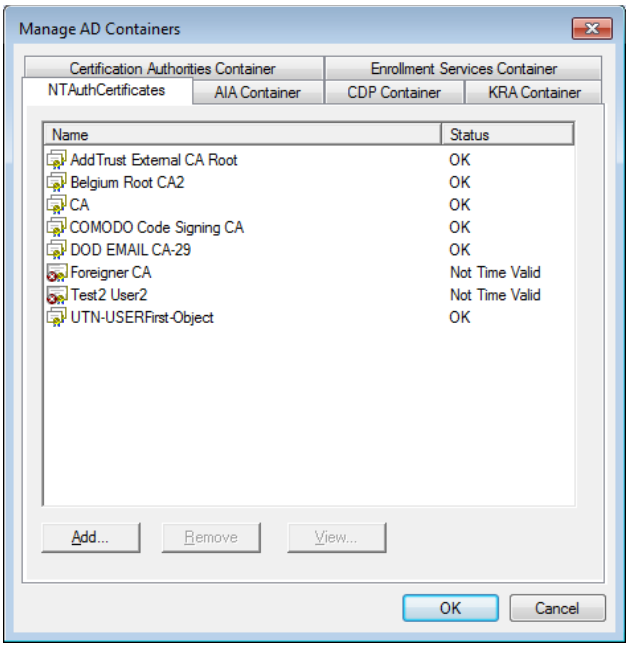
To check the certificates of the Enterprise NTAuth store, follow these steps:

1. Start Microsoft Management Console (Mmc.exe), and then add the PKI Health snap-in:
2. On the **Console** menu, click **Add/Remove Snap-in**.
3. Click the **Standalone** tab, and then click the **Add** button.
4. In the list of snap-ins, click **Enterprise PKI**.



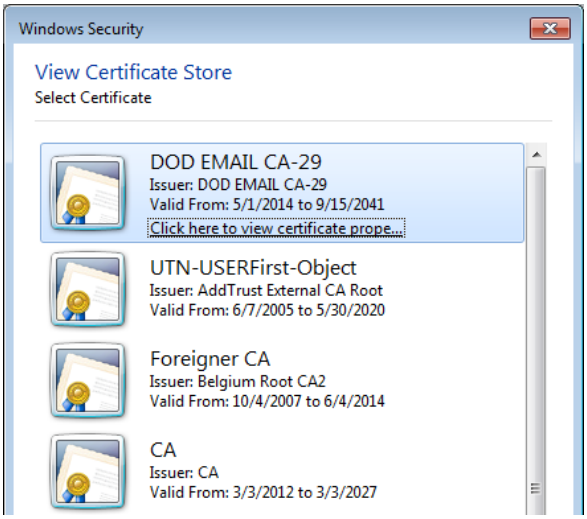
5. Click **Add**, and then click **Close**.
6. Click **OK**.
7. Right-click **Enterprise PKI**, and then click **Manage AD Containers**.





Method 2: Using Certutil.exe

Run the command `certutil -viewstore -enterprise NTAuth`

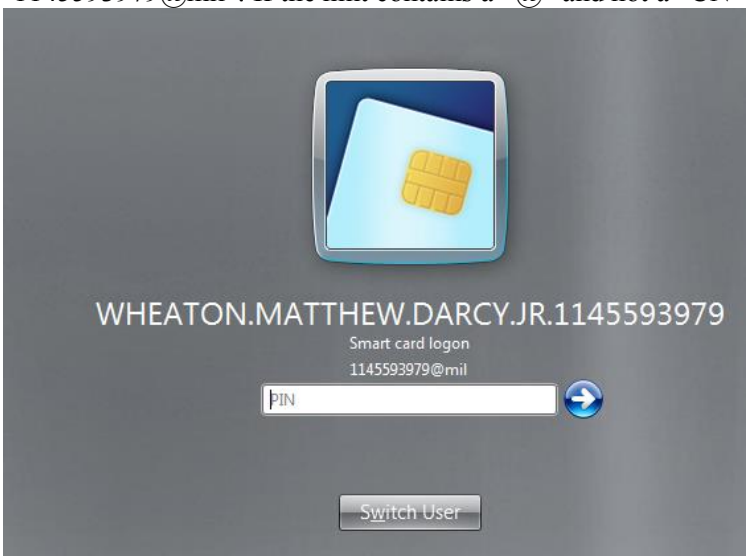


Annex - Audit the certificate mapping

Determine the type of mapping

There are two types of certificate mapping: UPN mapping and Explicit mapping

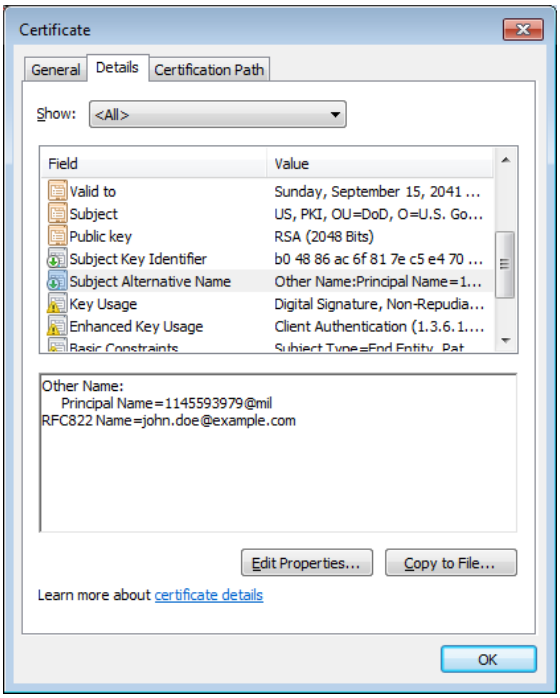
Look in the logon screen for the account hint written below “Smart card logon”. In this case the hint is “1145593979@mil”. If the hint contains a “@” and not a “CN=” string, it is a UPN mapping.



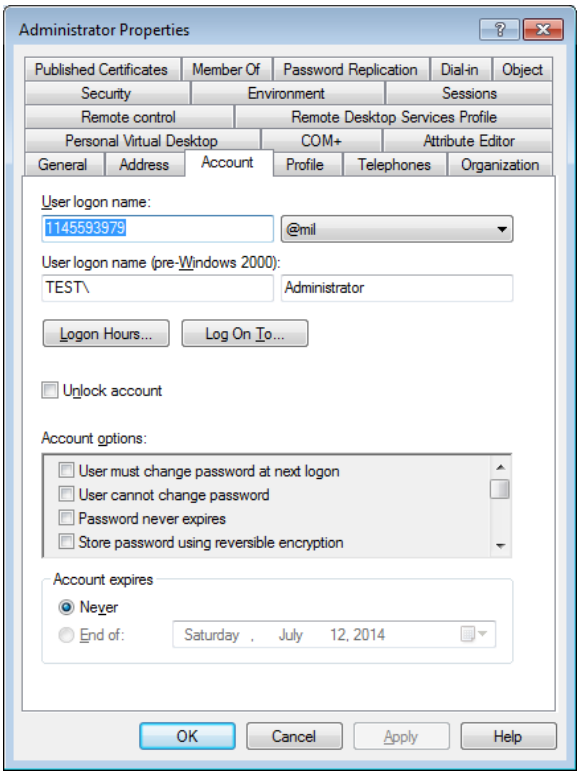
If the string contains a “CN=” or in general a “=”, it is an explicit mapping like showed in the example below.

Map a certificate to a user account using UPN mapping

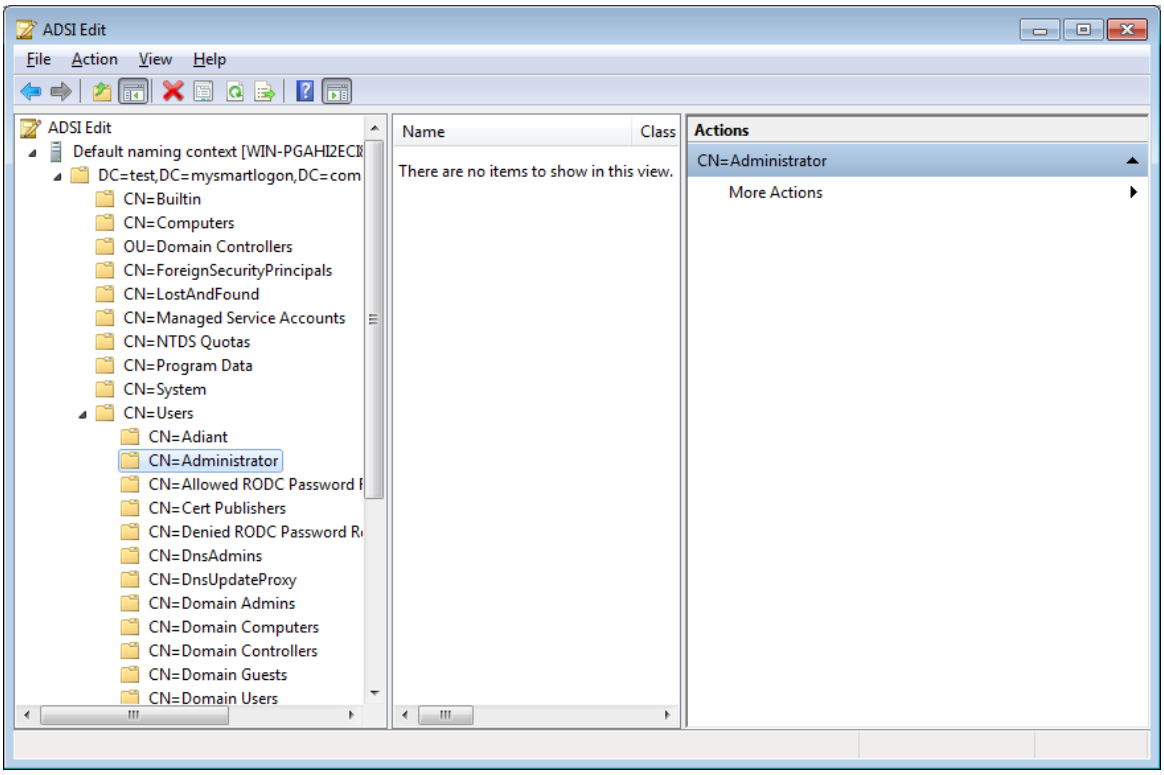
Open the certificate properties and the Details tab. Look for "Subject Alternative Name". At the bottom of the screen, search for "Principal Name". In this case, it is 1145593979@mil. There can be other definitions like RFC822 Name.



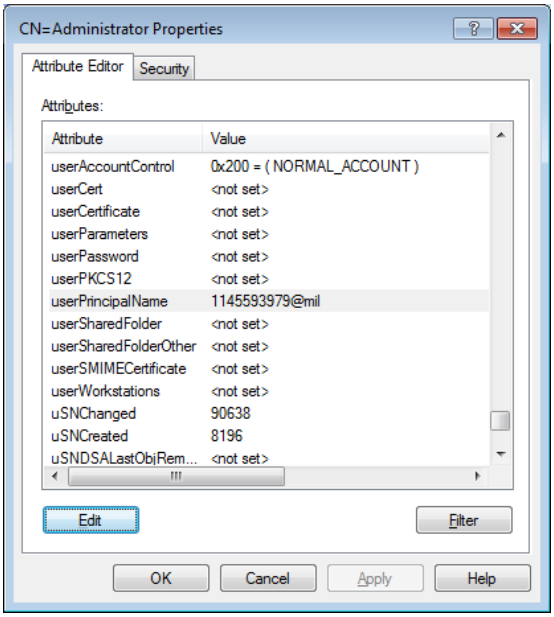
Open the properties of the user, and check that the User logon name matches the string returned previously.



If you need to change the string, you may not be able to change the suffix (@mil). Use ADSI Edit to open the properties of the user.



Change the attribute userPrincipalName to a value which matches the Principal Name set on the certificate.

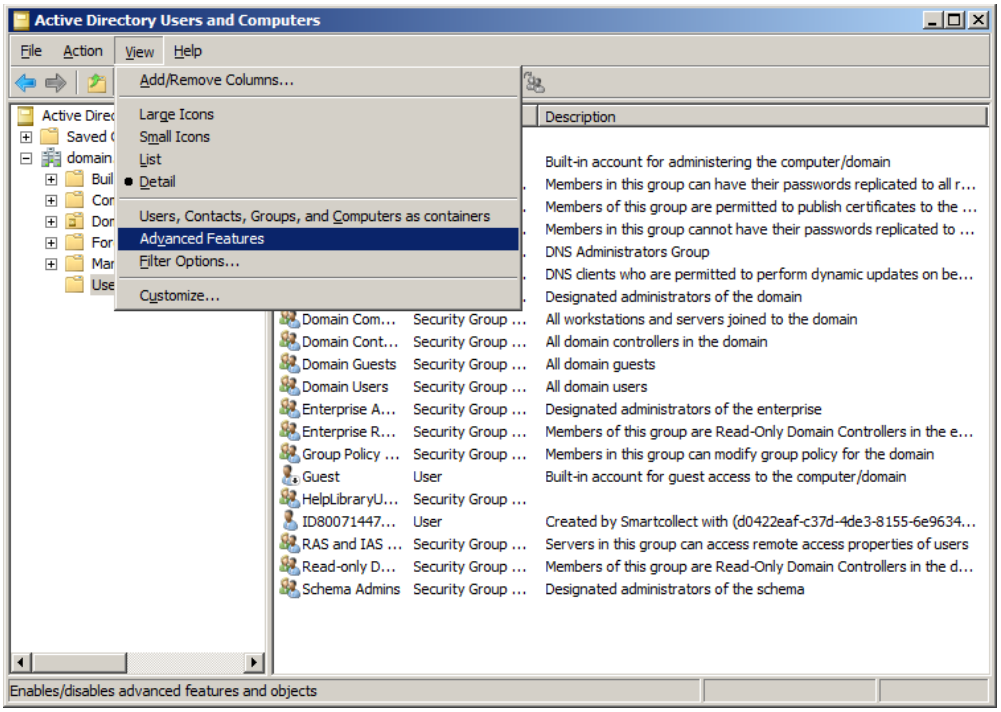


Map a certificate to a user account using explicit mapping

Reference: Explicit mapping in "MS-PKCA: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol Specification"[1]

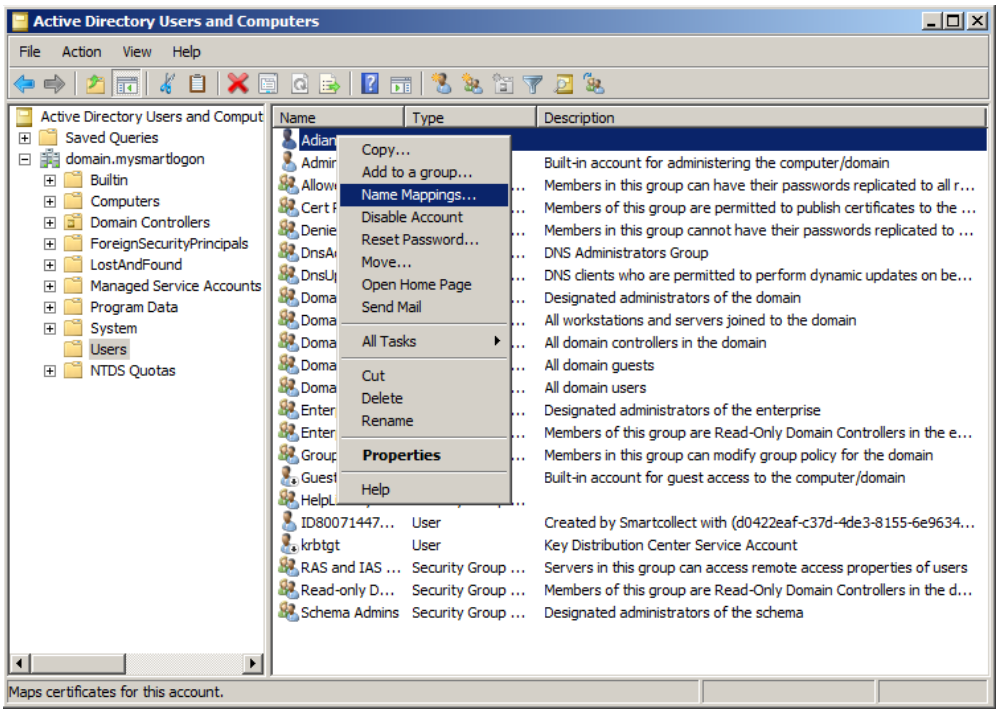
Open the console "Active Directory Users and Computers"

Select View -> Advanced features

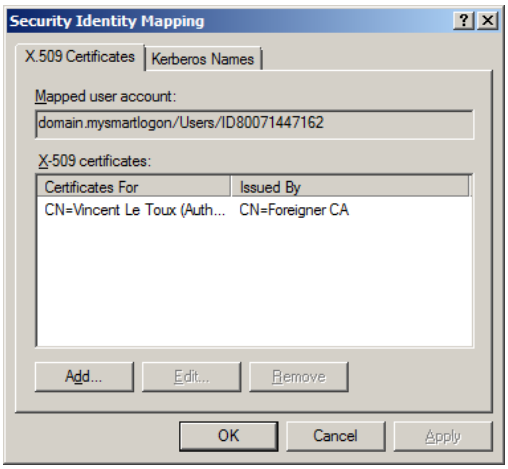


Select the account you want to map a smart card certificate to and then right click "Name mappings".

[1] http://msdn.microsoft.com/en-us/library/hh536384%28PROT.13%29.aspx



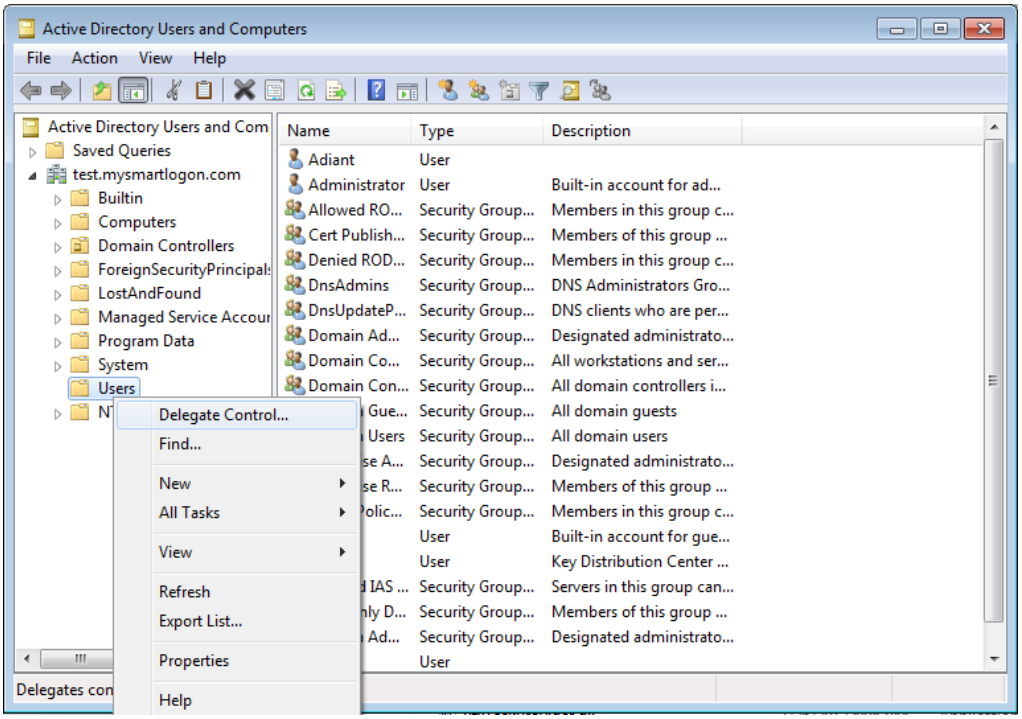
Select the smart card certificate previously exported and validate.



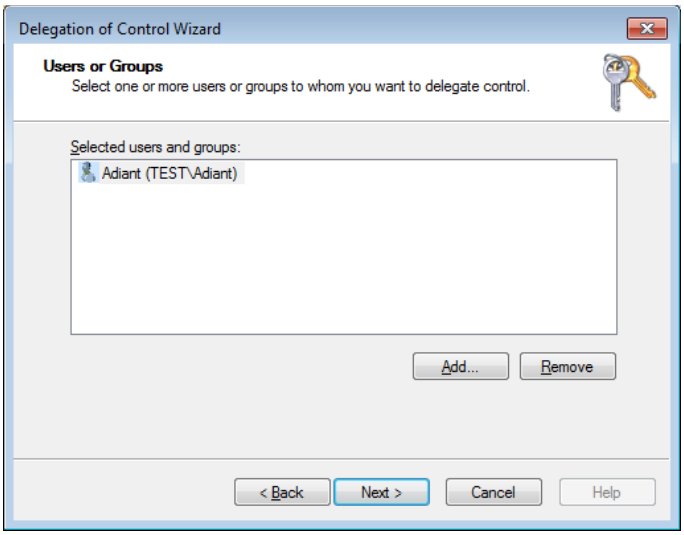
Annex - Configure a delegation policy

Delegating Authority for Editing the altSecurityIdentities and userPrincipalName attribute

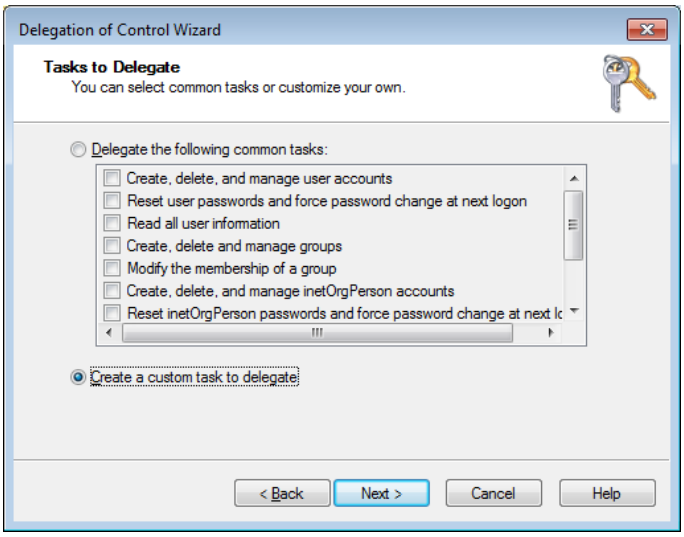
Right-click on the organizational unit you want to delegate and then click **Delegate Control**. It will launch the **Delegation of Control Wizard**.



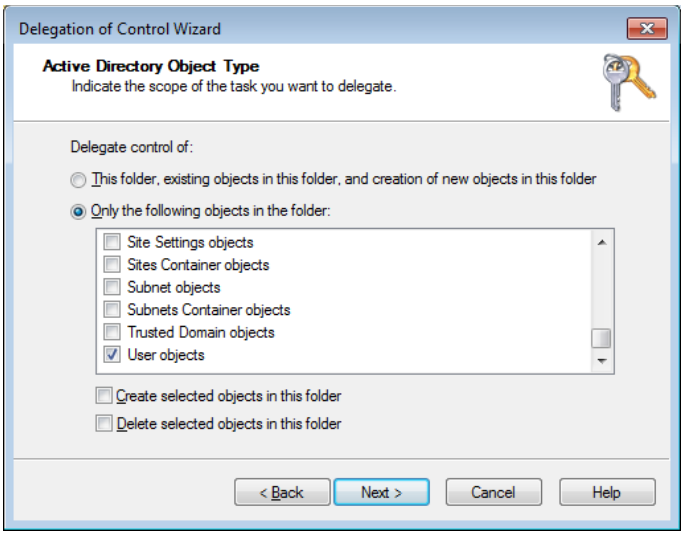
Select users or groups for delegation



Select **Create a custom task to delegate**

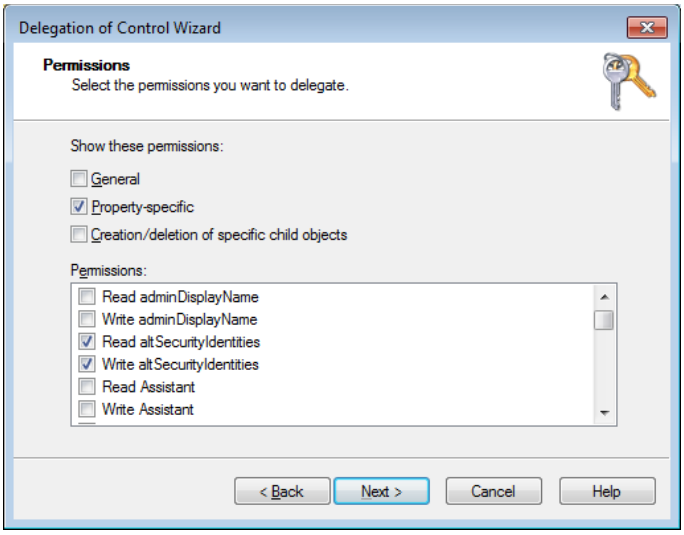


Select **Only the following objects in the folder**, then select **User objects**.

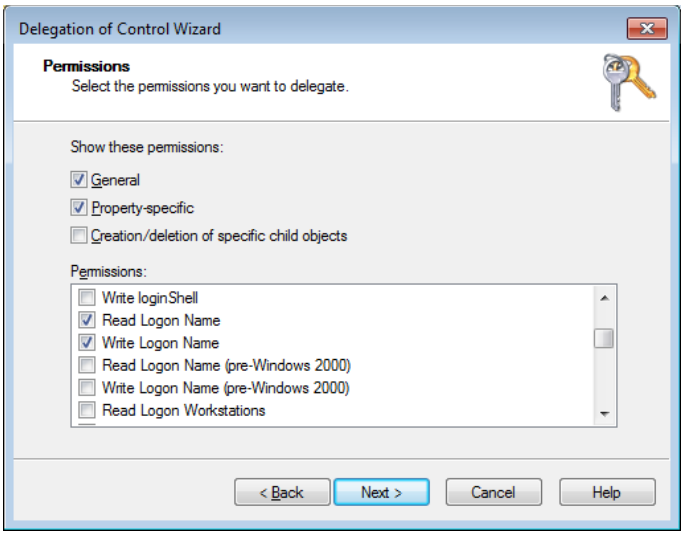


On the Permissions page, select **Property-specific**.

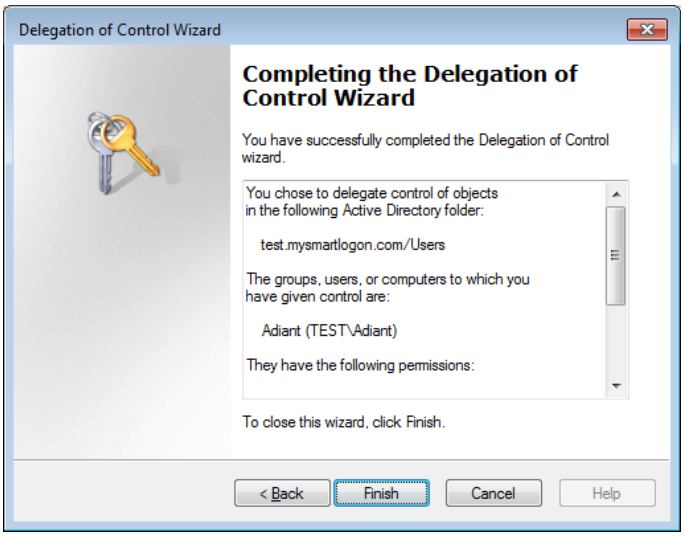
Then select read and write permissions for the following attribute *altSecurityIdentities*



For the UPN the name is "Logon Name".

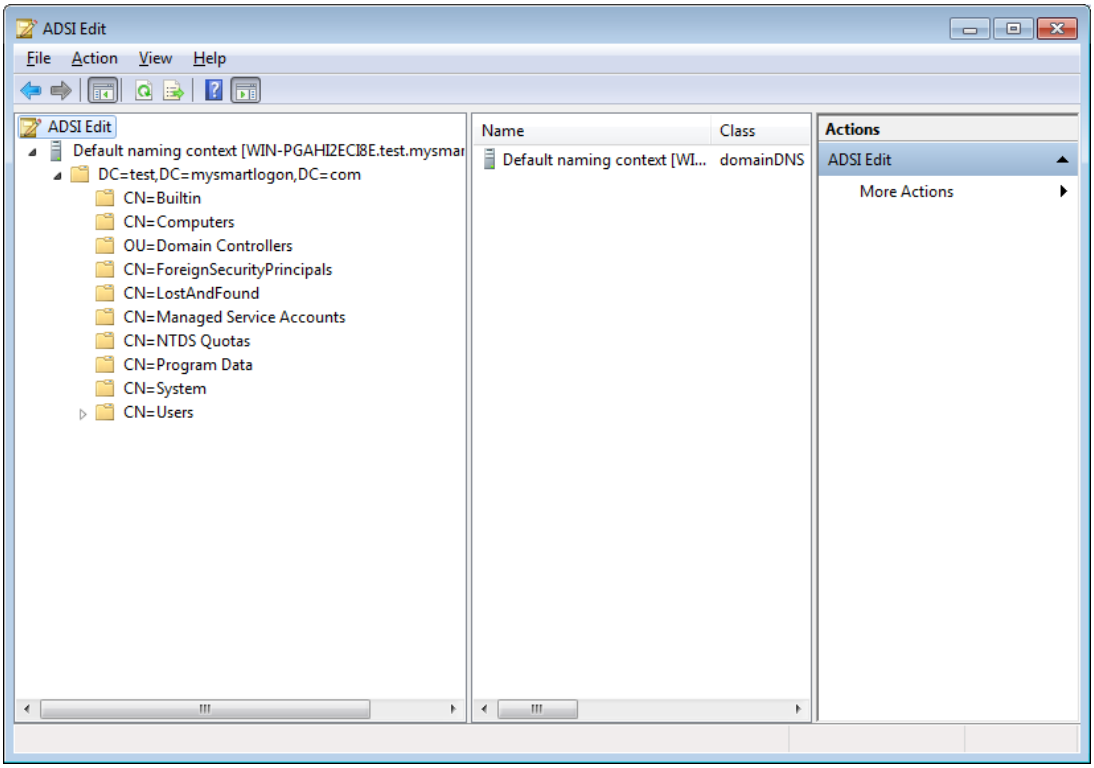


Click Next, and then click Finish.

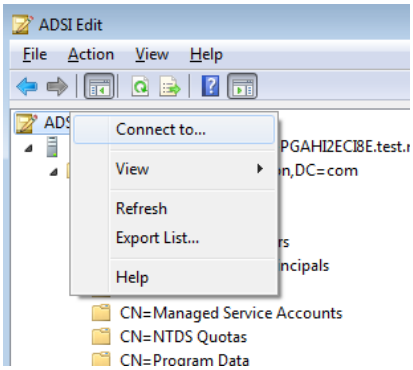


Delegate the NTLM certificate store

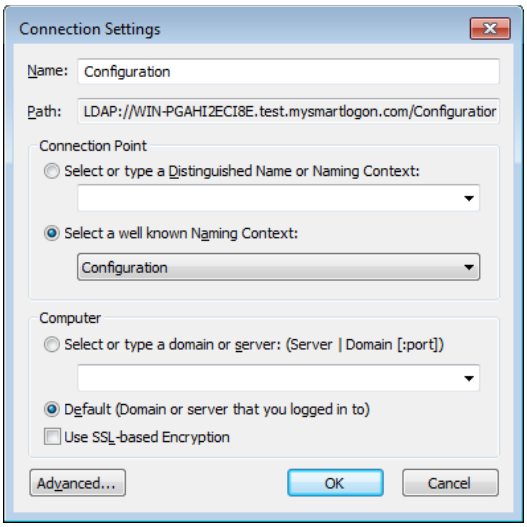
Launch ADSI Edit



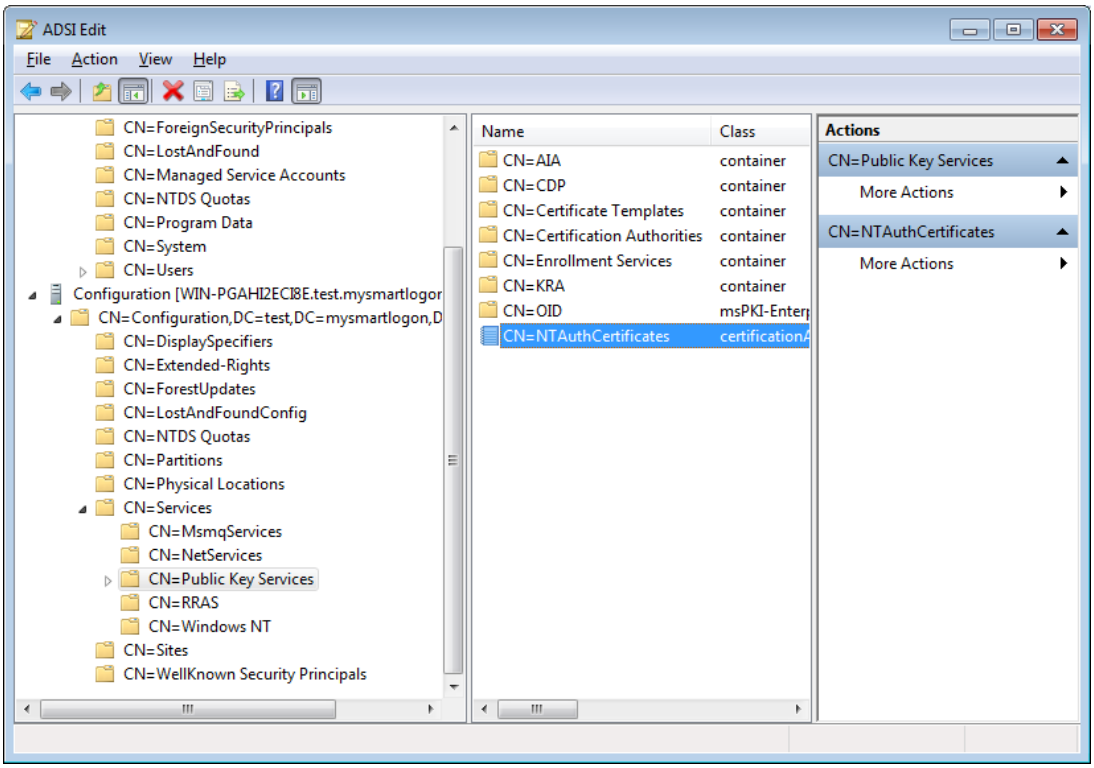
Select Connect to



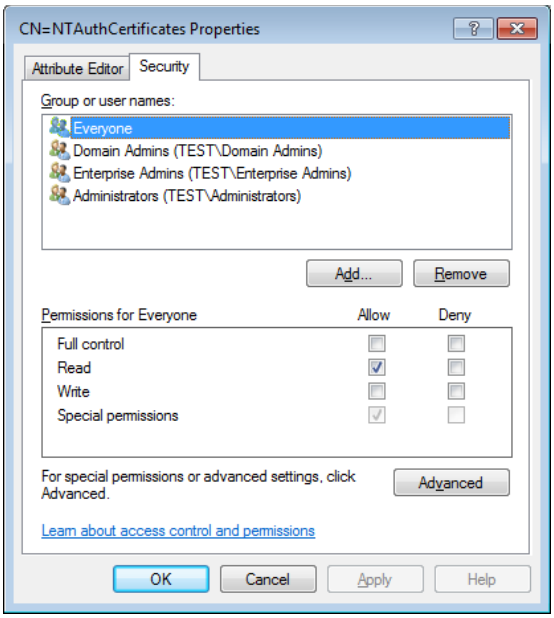
Choose the well known Naming Context "Configuration"



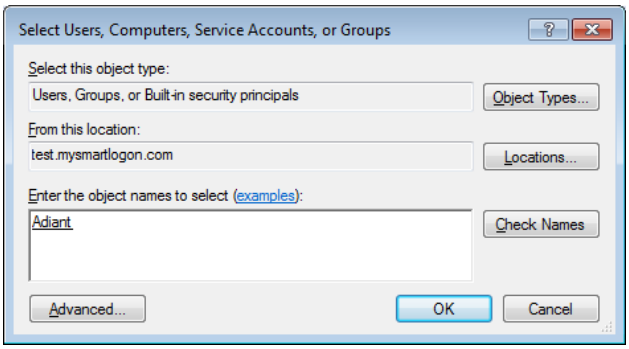
Select the NTAuthCertificates in Services->Public Key Services

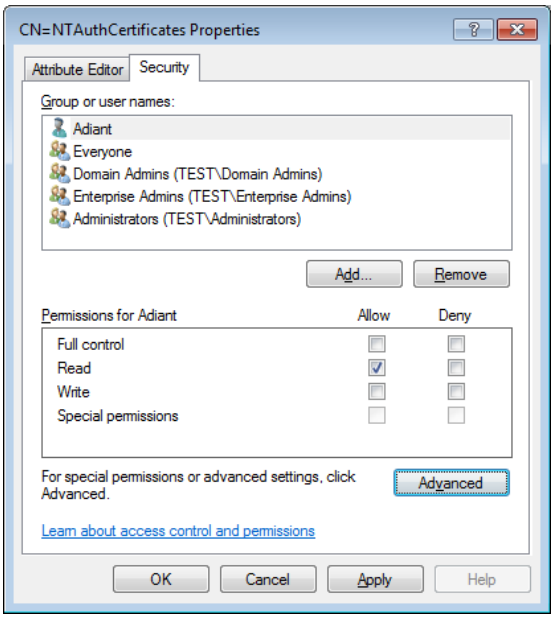


Right click on the item and select properties.

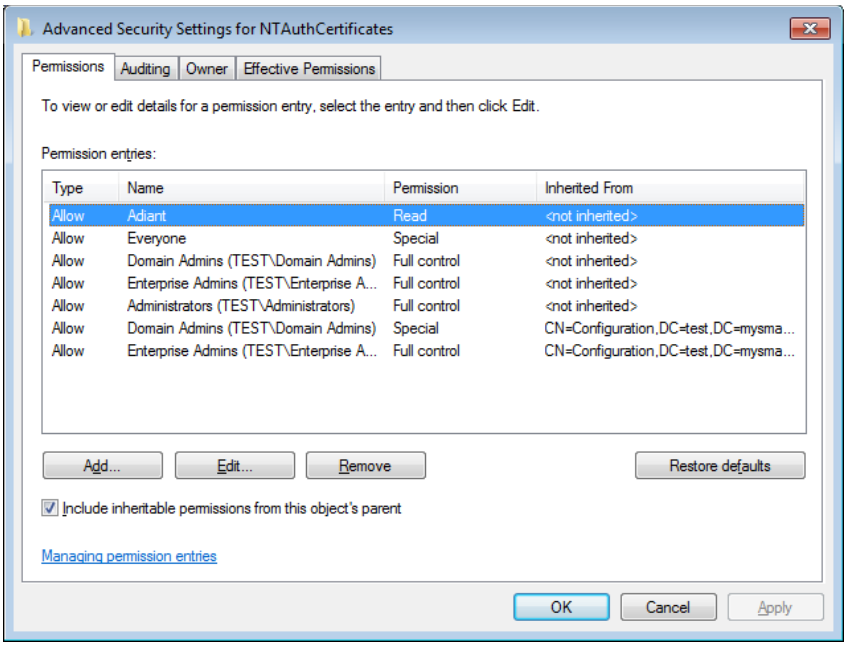


Add the user or the group



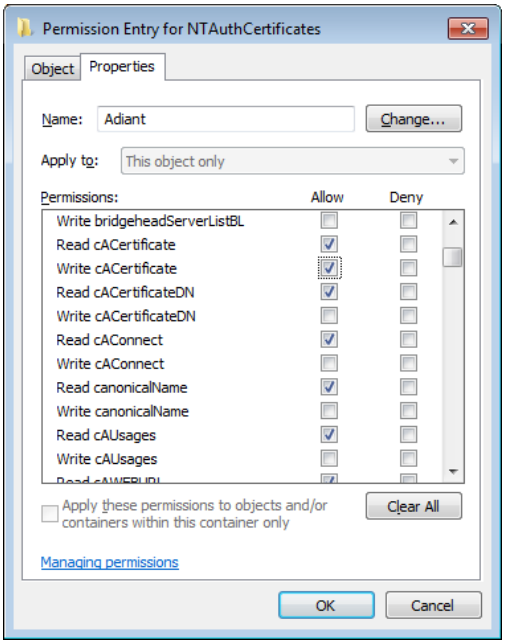


Then Click on Advanced



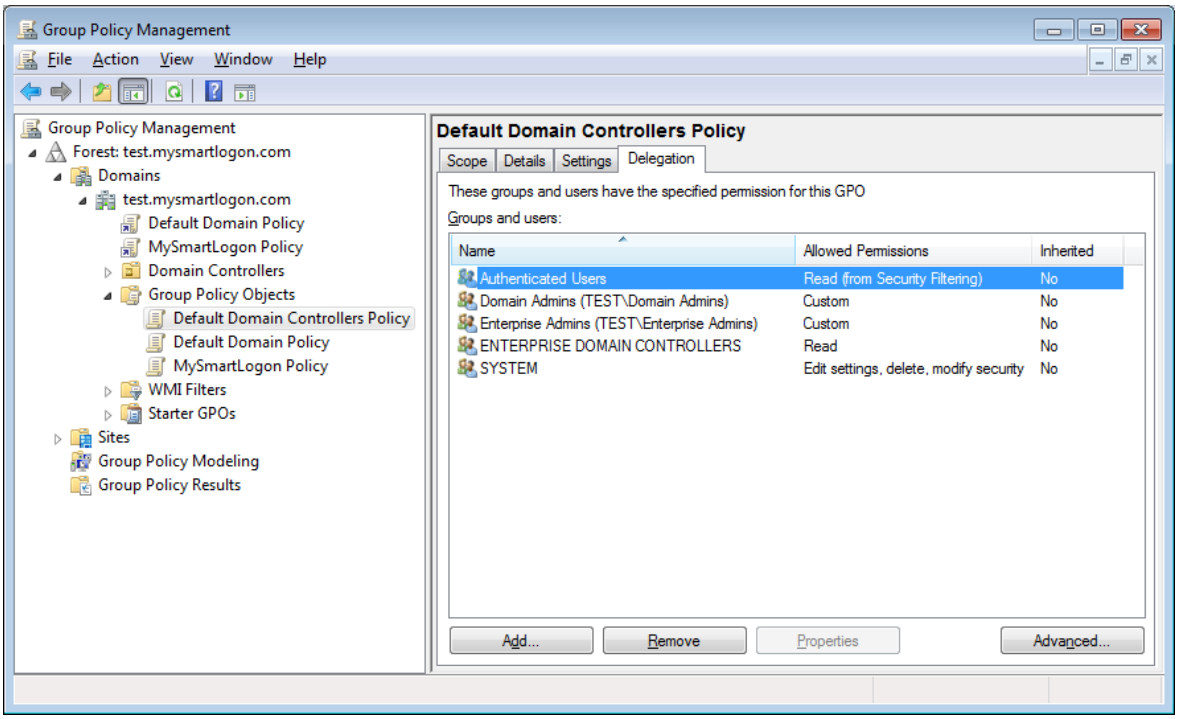
Select the user or the group and click on Edit

Add permissions "Write cACertificate"

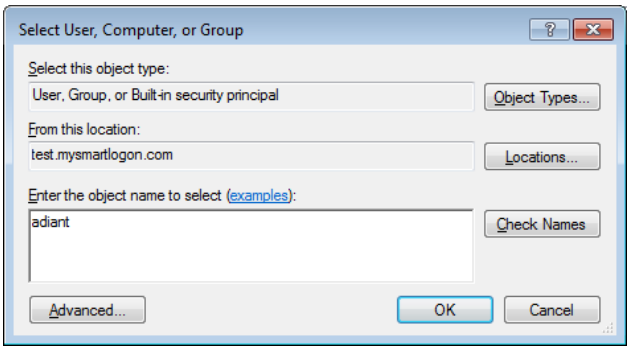


Delegate GPO

Select the GPO you want to delegate and open the tab Delegation.



Click on Add to select the user or the group.



Select the permission "Edit settings"