

# User Documentation for SmartPolicy

Version 1.2

Prepared by: "Vincent Le Toux"

Date: 07/02/2013



# **Table of Contents**

Table	of	Contents
	•••	•••••••

Introduction
System Specifications
Requirement
Installation
Mapping
UPN mapping
Explicit mapping6
Certificates which can't be used with Smart Policy7
User Interface
First dialog
Certificate's source dialog
Smart card or certificate file dialog11
mass mapping dialog14
CRL checking dialog
Group Policy Object Dialog17
Final Dialog
Annex - Check the GPO
Annex - Check the NTLM Store
Method 1: Using the PKI Health Tool
Method 2: Using Certutil.exe
Annex - Audit the certificate mapping
Determine the type of mapping
Map a certificate to a user account using UPN mapping
Map a certificate to a user account using Explicit mapping
Annex - Configure a delegation policy
Delegating Authority for Editing the altSecurityIdentities and userPrincipalName attribute31
Delegate the NTLM certificate store
Delegate GPO



#### **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:

Cel ulicate Policies	Effect and are concytrolicy tae	
CRL Distribution Points	[1]CRL Distribution Point: Distr	
Authority Information Δccess	[1]Authority Info Access: Acc	Ŧ
[1]CRL Distribution Point		

• **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 Key Identifier	94 07 0d bt ca a7 e7 35 bd c1 [1]Authority Info Access: Acc	
Subject Alternative Name	RFC822 Name=	
R 2 5 29 9	30 12 30 10 06 08 2h 06 01 05	Ŧ
/#812 5 29 9	30 12 30 10 06 08 2b 06 01 05	-
FC822 Name		
RFC822 Name = Other Name:		

- **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)

Key Usage	Digital Signature, Non-Repudia	
Thumbprint algorithm	sha 1	17
📺 Thumbprint	16 71 54 <del>4</del> e 9a 20 51 cf a7 5a	-

### **Certificates which can't be used with Smart Policy**

Certificates:

• With a Key Usage different from "Digital Signature"

Thumbprint algorithm	sha1	Ξ
Thumbprint	0d a4 d5 e1 cd cb af 29 d1 33	
manoprinc		•

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

	e8 61 c4 20 ae c1 a9 05 3c 8c	
Enhanced Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)	11
🗊 Netscape Cert Type	Signature (10)	
🗊 Certificate Policies	[1]Certificate Policy:Policy Ide	-
CRL Distribution Points	[1]CRL Distribution Point: Distr	
Authority Information Access	[1]Authority Info Access: Acc	
Subject Alternative Name	REC822 Name=contact@mvs	-



### **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.

🕞 🗊 MySmartLogon.com - Smart Policy - Stage 3 - 2.0.0	
Smart Policy	
After the selection of one or many certificates stored this wizard will prepare/modify a group policy and r the certificate(s) to the user account(s) selected.	d in a smart card or in files, nap in the Active Directory
This wizard must be run by a domain administrator been granted. Modifications can be reviewed before	or delegations must have e being applied.
By pressing Next, you accept the terms of the <u>licens</u>	g, Press Cancel if you don't.
	<u>N</u> ext Cancel

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.



Cicense				
Smart Po Copyrigh	licy t (C) 2012-2014 My Smart Logon SAS			
Security	Notice E			
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, which can lead to a complete loss of control of your system				
IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE AND PRESS CANCEL IMMEDIATELY.				
1. Pro (hereina) France () and oblic owned by	eamble: This Agreement governs the relationship between the user fter: Licensee) and My Smart Logon SAS whose principal place of business is Hereinafter: Licensor). This Agreement sets the terms, rights, restrictions gations on using [Smart Policy] (hereinafter: The Software) created and Licensor, as detailed herein			
2. Lio non-tran Non-exclu restrict	cense Grant: Licensor hereby grants Licensee a Personal, Non-assignable & sferable, Non-commercial, Without the rights to create derivative works, usive license, all with accordance with the terms set forth and other legal ions set forth in 3rd party software used while running Software.			
2.1 2.1.1 2.1.2	Limited: Licensee may use Software for the purpose of: Running Software on Licensee's Computer[s]; Publishing Software's output to Licensee and 3rd Parties;			
2.2	Non distribuable: Licensee may not distribute the software without a			

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.

🚱 🚺 MySmartLogon.com - Smart Policy - Stage 3 - 2.0.0
Select a source for the certificate(s)
Select a source for the certificate(s) to map :
<ul> <li>Read a smart card</li> <li>The driver of the smart card must be installed and the card not empty.</li> </ul>
Load a certificate A file with the extension .cer
A directory containing certificates A directory prepared by Smart Policy stage 2
Next Cancel

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

🚱 🇊 MySmartLogo	on.com - Smart Policy - Stage 3 - 2.	0.0	
Select a user			Jser zone
Select the acco Account :	ount you want to configure.	Browse	,
<u>Review the cer</u>	tificates which were previously exp	licitely mapped to this	Certificate zone
Select the cert	ificate you want to configure : 📕		
Adiant	WHEATON		Mapping zone
Type of mapp	ing : <u>explicit mapping</u>		*
		Next	Cancel

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.

Select this object type:	
User	Object Type
From this location:	
Entire Directory	Locations.
Entire Directory Enter the object name to select ( <u>examples</u> ):	Locations.
Entire Directory Enter the object name to select ( <u>examples</u> ):	Locations.
Entire Directory Enter the object name to select ( <u>examples</u> ):	Locations.

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.

Select the account you want to configure.         Account :       ItEST\administrator         Review the certificates which were previously explicitely mapped to this user account         Select the certificate you want to configure :         Image: Configure in the certificate with the configure in the certificate with the configure in the certificate with the certificate in the certificate with the configure in the certificate with the certificate in t	j MySmartLogon. elect a user	com - Smart Policy - Si	tage 3 - 2.0.0		Logon
Select the certificate you want to configure : Adiant WHEATON	Select the account Account :	nt you want to configu TEST\administrator icates which were previ	re. iously explicitely m	Browse apped to this user	account
Type of mapping : <u>UPN mapping [with revocation checks disabled]</u>	Select the certific	ate you want to config	jure :		
	Type of mapping	: UPN mapping (with	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.

Select the account you want to configure.         Account :       TEST\administrator         Review the certificates which were previously explicitely         Select the certificate you want to configure :	Browse mapped to this user account
Select the certificate you want to configure :	
Vincent Le Toux (Auth Vincent Le Toux (Signature)	E
The certificate can not be used for smart card logon bec the basic requirements	ause it doesn't comply with

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.

	×
🚱 🗊 MySmartLogon.com - Smart Policy - Stage 3 - 2.0.0	
Select a user	1
Select the account you want to configure. Account : TEST\administrator Browse Review the certificates which were previously explicitely mapped to this user accourt	nt
Select the certificate you want to configure :	
Adiant WHEATON	
The certificate is not trusted by the computer. Smart Policy requires this certificate to be trusted by the current account to find the root and intermediate certificates.	
Next Can	cel



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

UPN mapping:



#### Explicit mapping:



With revocation checks disabled:

Warning		
<b>A</b>	This certificate doesn't have a CRL location referenced in its attributes. The logon won't work if the revocation checking is not disabled. Disabling this policy will allow revoked certificates to be used for login. Please check if this setting is compliant with your security policy.	
	OK	

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.

## 

			×
🕒 G	MySmartLogon.com -	Smart Policy - Sta	ge 3 - 2.0.0
Re	view prepared ma Review the mapping(s) In case of error, the file	apping(s) ) found in the direc name will be displ	tory. Double click to view the certificate.
	Request made	User	Comment
	1601-01-01 00:00         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57         2014-06-04 19:57	Adiant Adiant Adiant Adiant Adiant2 Adiant3 Administrateur Administrator Adiant Adiant Adiant	Type of mapping : UPN mapping [wi The user does not exists Type of mapping : UPN mapping [wi The user does not exists The user does not exists The user does not exists Type of mapping : UPN mapping [wi The user does not exists Type of mapping : UPN mapping [wi Type of mapping : UPN mapping [wi Unable to parse the name of the file
	Total mapping(s) foun	d : 11 - Total valid certificate and refre	mapping(s) found 5 esh the mapping(s) Next Cancel

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.

### MySmartLogon



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.

## MySmartLogon



**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.

Cancel

<u>N</u>ext

# 

🚱 🗊 MySma	artLogon.com - Smart Policy - Stag	ye 3 - 2.0.0
Ready to	do the mapping	
Smart P	olicy is ready to perfom the mapp	ng. Press Finish to complete.
The log force th the dor	in will be possible once the GPO v e GPO update by running "gpupd nain controller which is performin	vill be applied. Default is 8 hours. You can ate /force" on the client computer and on g the authentication.
The cer reference ©	tificate revocation check is disable ced in its attributes can be used for Keep it disabled (one or more cer Cancel the setting on the GPO	d. Certificates revoked or without CRL logon. ificate has no CDP information)
<u>Trouble</u> View th	shoot the certificate revocation pr	ocess
		Finish Cancel
🚱 🚺 MySma	artLogon.com - Smart Policy - Stag	je 3 - 2.0.0
G 🕼 MySma Ready to	artLogon.com - Smart Policy - Stag do the mapping	je 3 - 2.0.0
G 🗊 MySma Ready to Smart P	artLogon.com - Smart Policy - Stag do the mapping olicy is ready to perfom the mapp	ye 3 - 2.0.0
C III MySma Ready to Smart P The log force th the dor	artLogon.com - Smart Policy - Stag do the mapping olicy is ready to perfom the mapp in will be possible once the GPO v the GPO update by running "gpupd main controller which is performin	re 3 - 2.0.0
C I MySma Ready to Smart P The log force th the dor Would y that the the case	artLogon.com - Smart Policy - Stay o do the mapping olicy is ready to perfom the mapp in will be possible once the GPO v re GPO update by running "gpupd main controller which is performin you like to disable the certificate re retrieval of the CRL worked on the on the other computers.	re 3 - 2.0.0
C IN MySma Ready to Smart P The log force th the dor Would y that the the case	artLogon.com - Smart Policy - Stag o do the mapping olicy is ready to perfom the mapp in will be possible once the GPO v te GPO update by running "gpupd main controller which is performin you like to disable the certificate re retrieval of the CRL worked on the on the other computers. Disable CRL checking	re 3 - 2.0.0
C MySmar Ready to Smart P The log force th the dor Would that the the case Trouble <u>View th</u>	artLogon.com - Smart Policy - Stay of do the mapping olicy is ready to perfom the mapp in will be possible once the GPO v te GPO update by running "gpupd main controller which is performin you like to disable the certificate re retrieval of the CRL worked on the con the other computers. Disable CRL checking Do nothing (recommended) shoot the certificate revocation pr e mapping report	Line 2 - 2.0.0

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



#### Mapping report



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

Troubleshoot the certificate revocation process
1) Export the certificate you want to test
Gather the file at the .cer format. If you are using a smart card, you can export it by viewing the certificate on this wizard, select the "Detail" tab and click on "Copy to a file".
2) Verify the proxy settings
The revocation process is made by the SYSTEM account and this account doesn't have the same internet configuration than an interactive user.
Run "netsh winhttp show proxy" to show the current proxy parameters.
Run "netsh winhttp set proxy" to set a static proxy.
3) Test the certificate revocation process as SYSTEM
Run "psexec –s running certutil -urlfetch –verify test.cer"
Note: psexec is available here : http://technet.microsoft.com/fr-fr/sysinternals/bb897553.aspx
Close



## **Annex - Check the GPO**

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

#### gpresult /h report.html

🏉 TEST\a	dministrator on TEST\WI	N-PGAHI2ECI8E - Windows	Internet Explorer				• •
00	C:\Users\Admini	strator\Desktop\gpreport.	html 👻	😽 🗙 📴 Bing			+ م
🚖 Favor	ites 🏾 🏉 TEST\adminis	trator on TEST\WIN-PGAH	II2ECI8E	🟠 🔹 🗟 🔹 🖃	🖶 🔻 <u>P</u> ag	e ▼ <u>S</u> afety ▼ T <u>o</u>	ols 🔻 🔞 🔻
P	Public Key Policies/Trus	ted Root Certification Au	thorities				<b>^</b>
	Properties						
	Winning GPO		[[	efault setting]			
	Policy			Setting			
	Allow users to select n	ew root certification authoritie	s (CAs) to trust	Enabled			
	Client computers can t	rust the following certificate st	ores	Third-Party Root Certific Certification Authorities	cation Authoritie	s and Enterprise Roo	t
	To perform certificate- CAs must meet the foll	based authentication of users owing criteria	and computers,	Registered in Active Di	rectory only		
	Certificates						
	Issued To	Issued By	Expiration Date	te Intended	Purposes	Winning GPO	
	DOD EMAIL CA-29	DOD EMAIL CA-29	9/15/2041 9:08	:21 AM <all></all>		Default Domain Po	blicy
	For additional information	about individual settings, lau	nch Group Policy Ob	ject Editor.			
Admir	nistrative Templates						
	Policy definitions (ADMX	files) retrieved from the local r	machine.				
E	Extra Registry Settings						
	Display names for some : Management.	settings cannot be found. You	ı might be able to res	olve this issue by updat	ing the .ADM file	es used by Group Pol	icy
	Setting	State	e		Winning GPO		-
			🐞 🌉 Compu	ter   Protected Mode	: Off	🛛 🖓 🔻 🔍 1	.00% 👻 🔐

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

Group Policy Management Editor			- • •
<u>File Action View H</u> elp			
🗢 🔿 🔁 🗊 🔒 🛛 🖬 🕅			
<ul> <li>Default Domain Policy [WIN-PGAHI2ECI8E.TES]</li> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Administrative Templates: Policy def</li> <li>Network</li> <li>System</li> <li>Network</li> <li>System</li> <li>BitLocker Drive Encryption</li> <li>Remote Desktop Services</li> <li>Smart Card</li> <li>All Settings</li> <li>Preferences</li> <li>Windows Settings</li> <li>Environment</li> </ul>	Setting         Image: Allow certificates with no extended key usage certificate attr         Image: Allow Integrated Unblock screen to be displayed at the time         Image: Allow signature keys valid for Logon         Image: Turn on certificate propagation from smart card         Image: Turn on certificate propagation from smart card         Image: Turn on cot certificate propagation from smart card         Image: Turn on cot certificate propagation from smart card         Image: Turn on cot certificates to be used for logon and authenticati         Image: Filter duplicate logon certificates         Image: Force the reading of all certificates from the smart card         Image: Display string when smart card is blocked         Image: Turn on Smart Card Plug and Play service         Image: Notify user of successful smart card driver installation	State Enabled Not configured Enabled Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured	Comment No No No No No No No No No No No
Files     Folders     T	< Ⅲ Extended ) Standard /		•

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	
<u>File Action View H</u> elp	
🗢 🤿 🔁 📰 🖸 🕞 🛛 🖬	
<ul> <li>Default Domain Policy [WIN-PGAHI2ECI8E.TEST.*</li> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Event Log</li> <li>Restricted Groups</li> <li>System Services</li> <li>File System</li> <li>Nirde Network (IEEE 802.3) Poli</li> <li>Wirels Network (IEEE 802.11)</li> <li>Public Key Policies</li> <li>Restricted Fries</li> <li>Wirels Network (IEEE 802.11)</li> <li>Public Key Policies</li> <li>Encrypting File System</li> <li>BitLocker Drive Encryption</li> <li>Automatic Certificate Requise</li> <li>Trusted Root Certification A</li> </ul>	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.

iap-in	Vendor	*	]	Console Root	Edit Extensions
Certificate Templates Certificates	Microsoft Cor Microsoft Cor			Enterprise PKI	Remove
Certification Authority	Microsoft Cor Microsoft Cor	Ш			Move Up
Device Manager	Microsoft Cor Microsoft Cor Microsoft and		<u>A</u> dd >		Move Down
DNS	Microsoft Cor				
Event Viewer	Microsoft Cor				
Group Policy Manag	Microsoft Cor				
Group Policy Manag	Microsoft Cor	Ŧ			Ad <u>v</u> anced
cription:					

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





Manage AD Containers			<b>—</b> ×
Certification Authorit	ies Container	Enrollment S	Services Container
NTAuthCertificates	AIA Container	CDP Container	KRA Container
Name AddTrust External C Belgium Root CA2 CA COMODO Code Sig DOD EMAIL CA-29 Foreigner CA Test2 User2	A Root ning CA ect		Status OK OK OK OK Not Time Valid Not Time Valid OK
<u>A</u> dd	emove V	íew	
			OK Cancel

#### 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.

Certificate	<b>—</b>			
General Details Certification Path				
Show: <ali></ali>				
Field	Value			
Valid to Subject Public key Subject Key Identifier Subject Alternative Name Execution Subject Alternative Name Enhanced Key Usage Enhanced Key Usage Resir Constraints Other Name: Principal Name = 1145593979@m RFC822 Name = john.doe@example	Sunday, September 15, 2041 US, PKI, OU=DoD, O=U.S. Go RSA (2048 Bits) b0 48 86 ac 6f 81 7e c5 e4 70 Other Name:Principal Name=1 Digital Signature, Non-Repudia Client Authentication (1.3.6.1 Subject Type=End Entity Pat			
Edit Properties Copy to File				
	ОК			

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

Administrator Properties	5			? 💌		
Published Certificates	Member Of	Password	Replication	Dial-in Object		
Security	Env	ironment		Sessions		
Remote control		Remote	Desktop Serv	rices Profile		
Personal Virtual De	sktop	COM+	- /	Attribute Editor		
General Address	Account	Profile	Telephones	s Organization		
User logon name:						
1145593979		@mil		-		
Liser locon name (pre-)	Vindowa 2000	). ).				
TEST\	<u>v</u> indows 2000	,. Administra	tor			
Logon Hours (	Log On To Unlock account Account gptions:					
User must change User cannot char Password never e Store password u	User must change password at next logon User cannot change password Password never expires Store password using reversible encryption					
Account expires						
○ End of:	Saturday ,	July 12	, 2014			
		]				
C	К	Cancel	Apply	Help		



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.

📝 ADSI Edit			
<u>File Action View H</u> elp			
🗢 🔿 🞽 🗊 🗙 🖹 🤷 🛃 🚺			
ADSI Edit	Name	Class	Actions
Default naming context [WIN-PGAHI2ECI	These are in items to show in this		CN=Administrator
DC=test,DC=mysmartlogon,DC=com	There are no items to show in this	view.	More Actions
CN=Builtin			
Oll=Domain Controllers			
CN-EnreignSecurityPrincipals			
CN=LostAndFound			
CN=Managed Service Accounts			
CN=NTDS Quotas			
CN=Program Data			
CN=System			
⊿ 🚞 CN=Users			
CN=Adiant			
CN=Administrator			
CN=Allowed RODC Password F			
CN=Cert Publishers			
CN=Denied RODC Password R			
CN=DrsAdmins			
CN-Domain Admins			
CN=Domain Computers			
CN=Domain Controllers			
CN=Domain Guests			
CN=Domain Users			
	<	+	

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

CN=Administrator Propert	ies	? 💌
Attribute Editor Security		
Attri <u>b</u> utes:		
Attribute	Value	*
userAccountControl userCert userCertficate userParameters userPAcsword userPKCS12 userPrincipalName userSharedFolder userSharedFolderOther userSharedFolderOther userSMIMECertificate userWorkstations uSNChanged uSNCreated uSNDSALastObjRem	0x200 = ( NORMAL_ACCOUNT ) <not set=""> <not set=""> <not< td=""><td></td></not<></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	
· · · · · · · · · · · · · · · · · · ·		•
Edit		<u>F</u> ilter
ОК	Cancel Apply	Help



#### 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"<sup>1</sup>

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".

<sup>&</sup>lt;sup>1</sup> http://msdn.microsoft.com/en-us/library/hh536384%28PROT.13%29.aspx



Active Directory Users and Com	puters				
File Action View Help					
🗢 🔿 🖄 📅 🖌 🗓  🕻	1 🖸 😹 🛛 🖬 🗏 😹 🖆 🎙	7 🖸 🕱			
Active Directory Users and Comput	Name       Type         Adair       Copy         Addiar       Disable Account         Reset Password       Move         Doma       All Tasks         Doma       All Tasks         Doma       Cut         Doma       Cut         Benter       Rename         Benter       Rename         Group       Properties         Guest       Help         Help       User         RAS and IAS       Security Group         Schema Admins       Security Group	Description           Built-in account for administering the computer/domain           Members in this group can have their passwords replicated to all r           Members of this group are permitted to publish certificates to the           Members in this group cannot have their passwords replicated to           DNS clients who are permitted to perform dynamic updates on be           Designated administrators of the domain           All workstations and servers joined to the domain           All domain controllers in the domain           All domain guests           All domain users           Designated administrators of the enterprise           Members of this group are Read-Only Domain Controllers in the e           Members in this group can modify group policy for the domain           Built-in account for guest access to the computer/domain           Created by Smartcollect with (d0422eaf-c37d-4de3-8155-6e9634           Key Distribution Center Service Account           Servers in this group can access remote access properties of users           Members of this group are Read-Only Domain Controllers in the d           Designated administrators of the schema			
Maps certificates for this account.					

Select the smart card certificate previously exported and validate.

Security Identity Mappin	g	<u>? ×</u>			
X.509 Certificates Kerber	X.509 Certificates Kerberos Names				
Mapped user account:					
domain.mysmartlogon/Us	sers/ID80071447162				
X-509 certificates:					
Certificates For CN=Vincent Le Toux (A	Issued By uth CN=Foreigner CA				
Add Ed	it <u>R</u> emove				
	OK Cancel	Apply			

## **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**.

Active Directory Users and Com	puters			
File Action View Help				
🗢 🔿 💋 🖬 🤾 📋 🗙	🗐 🙆 😖 🚺 🖬	1 🙁 🐮 🤋	7 🖻 🖗	
Active Directory Users and Com	Name	Туре	Description	<b>^</b>
Saved Queries     Saved Q	Adiant Administrator Allowed RO Cert Publish Cert Publish Denied ROD DrsAdmins DnsUpdateP	User User Security Group Security Group Security Group Security Group Security Group	Built-in account for ad Members in this group Members of this group Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato	
Program Data     System     Users	Bomain Co Bomain Co	Security Group Security Group Security Group	All workstations and ser All domain controllers i	E
Find	i Users se A	Security Group Security Group	All domain users Designated administrato	
New All Tasks	► se R ► Polic	Security Group Security Group	Members of this group Members in this group c	
View	•	User User	Built-in account for gue Key Distribution Center	
Refresh Export List Properties	i IAS nly D i Ad	Security Group Security Group Security Group User	Servers in this group can Members of this group Designated administrato	
Delegates con Help				



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

Delegation of Control Wizard	<b>—</b> ×
<b>Permissions</b> Select the permissions you want to delegate.	R
Show these permissions: Show these permissions: Seneral Seneration/deletion of specific child objects Permissions:	
Read adminDisplayName     Write adminDisplayName     Read alt SecurityIdentities     Write alt SecurityIdentities     Read Assistant     Write Assistant	•
< Back Next > Cancel	Help

For the UPN the name is "Logon Name".

Delegation of Control Wizard	×
<b>Permissions</b> Select the permissions you want to delegate.	P
Show these permissions:	
<u> </u>	
✓ Property-specific	
Creation/deletion of specific child objects	
P <u>e</u> missions:	
Write loginShell	*
Read Logon Name	
Write Logon Name	
Read Logon Name (pre-Windows 2000)	
Write Logon Name (pre-Windows 2000)	
Head Logon Workstations	-
< <u>B</u> ack Next > Cancel	Help

Click Next, and then click Finish.

Delegation of Control Wizard	
<sup>(2)</sup>	Completing the Delegation of Control Wizard You have successfully completed the Delegation of Control wizard.
	You chose to delegate control of objects in the following Active Directory folder: test.mysmartlogon.com/Users The groups, users, or computers to which you have given control are: Adiant (TEST\Adiant) They have the following permissions:
	To close this wizard, click Finish.



### Delegate the NTLM certificate store

Launch ADSI Edit

Z ADSI Edit					
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp					
ADSI Edit Default naming context [WIN-PGAHI2ECI8E.test.mysmar CN=Builtin CN=Computers OU=Domain Controllers CN=ForeignSecurityPrincipals CN=LostAndFound CN=Managed Service Accounts CN=NTDS Quotas CN=Program Data CN=System CN=Users	Name Default naming context [WI	Class domainDNS	Actions ADSI Edit More Actions		
4 III >	•	ł			

#### Select Connect to



Choose the well known Naming Context "Configuration"



Connect	tion Settings	
<u>N</u> ame:	Configuration	
Path:	LDAP://WIN-PGAHI2ECI8E.test.mysmartlogon.com/Configuration	
Conne	ection Point	
© Se	elect or type a <u>D</u> istinguished Name or Naming Context:	
	<b>-</b>	
Select a well known Naming Context:		
	Configuration -	
Comp	uter =lect or type a domain or server: (Server   Domain [:nort])	
Default (Domain or server that you logged in to)     Use SSL-based Encryption		
Ad <u>v</u> ar	OK Cancel	

Select the NTAuthCertificates in Services->Public Key Services



Right click on the item and select properties.



CN=NTAuthCertificates Properties			
Attribute Editor Security			
Group or user names:			
& Domain Admins (TEST\Domain Admins)			
Enterprise Admins (TEST\Enterprise Admins)			
Administrators (TEST VAdministrators)			
	A <u>d</u> d	<u>R</u> emove	
Permissions for Everyone	Allow	Deny	
Full control			
Read	<b>v</b>		
Write			
Special permissions	1		
For special permissions or advanced settings, click Advanced.			
Leam about access control and permissions			
OK Cancel	Apply	Help	

#### Add the user or the group

Select Users, Computers, Service Accounts, or Groups	? <mark>×</mark>			
Select this object type:				
Users, Groups, or Built-in security principals	Object Types			
From this location:				
test.mysmartlogon.com	Locations			
Enter the object names to select (examples):				
Adiant	Check Names			
Advanced OK	Cancel			
	.4			
CNI=NTAuthCartificates Branatics				
Attribute Editor Security				
Group or user names:				
Adiant				
& Everyone				
Domain Admins (TEST\Domain Admins)				
Administrators (TEST\Administrators)				
Add <u>R</u> emov	/e			
Permissions for Adiant Allow Deny				
Full control				
Read 🔍 📃				
Write				
Special permissions				
For special permissions or advanced settings, click Advanced.	d			
Leam about access control and permissions				
OK Cancel Apply H	lelp			

Then Click on Advanced

MySmartLogon

view or mission	edit details for a permission entry, select the	entry and then clic	k Edit.
Туре	Name	Permission	Inherited From
Alow	Adiant	Read	<not inherited=""></not>
Allow Allow Allow Allow Allow	Domain Admins (TEST\Domain Admins) Enterprise Admins (TEST\Enterprise A Administrators (TEST\Administrators) Domain Admins (TEST\Domain Admins) Enterprise Admins (TEST\Enterprise A	Full control Full control Full control Special Full control	<not inherited=""> <not inherited=""> <not inherited=""> CN=Configuration,DC=test,DC=mysma CN=Configuration,DC=test,DC=mysma</not></not></not>
A <u>d</u> d Include	Edit     Remov       c inheritable permissions from this object's pan       permission entries	e ent	Restore de <u>f</u> aults

Select the user or the group and click on Edit

Add permissions "Write cACertificate"

🐌 Permission Entry for NTAuthCertificates 🛛 🛛 🔁		
Object Properties		
<u>N</u> ame: Adiant		Change
Apply to: This object only		-
Permissions:	Allow	Deny
Write bridgeheadServerListBL		A 1
Read cACertificate	<b>V</b>	
Write cACertificate	<b>V</b>	
Read cACertificateDN	1	
Write cACertificateDN		
Read cAConnect	1	
Write cAConnect		
Read canonicalName	<b>V</b>	
Write canonicalName		
Read cAUsages	1	
Write cAUsages		
Apply these permissions to objects an containers within this container only	id/or	Clear All
Managing permissions		
	ОК	Cancel



#### 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 User, Computer, or Group	? 🛃
Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
test.mysmartlogon.com	Locations
Enter the object name to select (examples):	
adiant	Check Names
l	
Advanced	OK Cancel

Select the permission "Edit settings"

Add Group or User	<b>—</b>
Group or user name:	
TEST\Adiant	<u>B</u> rowse
Permissions:	
Edit settings	•
	OK Cancel