

Troubleshooting smart card logon authentication on active directory

Version 1.0

Prepared by: "Vincent Le Toux"

Date: 2014-06-11



Table of Contents

Table of Contents	
Revision History	
Error messages	
The smart card certificate used for authentication was not trusted	5
Your credentials could not be verified	8
You cannot use a smart card to log on because smart card logon is not supported for y	our user account
The requested key container does not exist on the smart card	
No valid certificates found	
Checking for a healthy smart card	
Using certutil	18
Expected diagnostic of a healthy smart card	18
Smart card absent	19
A minidriver or a CSP has not been installed	20
The smart card resource manager is not running	22
Check that the smart card can be used for logon	
Key usage	23
Extended Key Usage	24
CRL Troubleshooting	
Checking that the certificate revocation check process is working	26
Screenshots for working and not working CRL checks	26
Solving CRL network issues	27
Clear the CRL cache for tests	28
Disable the CRL checks for smart card logon	29
Verifying the certificate mapping	
Determine the type of mapping	30
Map a certificate to a user account using UPN mapping	31
Map a certificate to a user account using Explicit mapping	33
Annex 1 – Procedures	
Get the certificate chain	35
Export one certificate	
Adding a certificate to the NTLM store	

Method 1: Import a certificate by using the PKI Health Tool	38
Method 2: Import a certificate by using Certutil.exe	38



Revision History

This section records the change history of this document.

Name	Date	Reason For Changes	Version
Vincent Le Toux	11/06/2014	Creation	1.0



Error messages

The smart card certificate used for authentication was not trusted

Message :

The system could not log you on. The smart card certificate used for authentication was not trusted.



Cause :

The certificate which was presented to the system is not trusted by the client computer or the domain computer. This may be caused by the absence of the root and intermediate certificates in the computer store and/or the NTLM store. Another cause is the system that couldn't verify if the certificate has been revoked.

The more probable cause is that the certificate has no "CRL Distribution Point (CDP) location" or the domain controller couldn't contact the CDP via the network.

Diagnostic :

A) Check for any smart card problems

Run "certutil –scinfo" to detect any problem related to the smart card. For example, a certificate which is not matching the private key.

B) Check that the smart card certificate is trusted

Run "certutil -scinfo" and look for "Smart card logon: chain validates".





If the test fails, the string is transformed to "smart card logon : chain on smart card is invalid"



To verify trust issues more in depth:

- 1) Open the certificate file on the client computer
- 2) Open the "certification path" and note all root and intermediates certificates
- 3) Open the computer certificate store (not the user certificate store)
- 4) Check the presence of the root certificate in the "Trusted Root Certification Authorities store"
- 5) Check the presence of all intermediate certificates, if any, in the "Intermediate Certification Authorities"
- 6) Do the same on the domain controller used for the authentication (it can be determined by the command "echo %LOGONSERVER%")

MySmartLogon

- 7) Check the presence of all intermediate and root certificates in the NTLM store by running the command : certutil -viewstore -enterprise NTAuth
- C) Check the CRL of the smart card certificate

Please see the chapter *Check that* the smart card can be used for logon

Key usage

Open the properties of the certificate and search for the property "Key Usage".

This property should contain one of the following :

- Key Encipherment
- Data Encipherment
- Digital Signature

If it doesn't, the certificate can't be used for smart card logon.

In the following example, the first certificate is ok. The second isn't.

General Details Certification Path Show: Call> Field Value Public key RSA (1024 Bits) Authority Information Access: 10/2ertificate Policy:Policy Ide Qualified Certificate Policy:Policy Ide Edit Droperties Qualified Certificate Policy:Policy Ide II)Certificate Policy:Policy Ide Qualified Certificate Statem 30 0a 30 06 06 04 00 8e 46 Non-Repudation (40) III)Certificate Policy:Policy Ide Metropy: Digital Signature (80) Edit Properties Copy to File Learn more about certificate details OK	Certificate	—	Certificate			x
Show: CMI Field Value Public key RSA (1024 Bits) Authority Key Identifier KeyID-93 07 55 62 fe a6 76 3 Authority Information Access [1]Certificate Policy:Policy Ide Certificate Policies [1]Certificate Policy:Policy Ide Certificate Policies [1]Certificate Policy:Policy Ide Netscape Cert Type SSL Clent Authentication, SMI Digital Signature (80) Idt Properties Copy to Flie Learn more about certificate details OK	General Details Certification Path		General Deta	ils Certification Path	1	
Field Value Public key RSA (1024 Bits) Authority Key Identifier KeyID=93 07 55 62 fe a6 76 3 Authority Information Access [1]Authority Info Access: Acc CRL Distribution Points [1]Certificate Policy:Policy Ide CRL Distribution Points [1]CRL Distribution Points [1]CRL Distribution Point [1]CRL Distribution Point [1]CRL Distribution	Show: <all></all>	-	Show: <all;< th=""><th>></th><th>•</th><th></th></all;<>	>	•	
Public key RSA (1024 Bits) Authority Key Identifier Key ID=33 07 55 62 6a 67 63 Authority Information Access [1]Authority Info Access: Acc Certificate Policy: [1]Certificate Policy: Policy Ide CRL Distribution Points [1]Certificate Policy: Policy Ide Rey Loss [1]Certificate Policy: Policy Ide Rey Loss [1]Certificate Policy: Policy Ide Rey Loss [1]Certificate Policy: Policy Ide Rey Usage Digital Signature (30) Digital Signature (80) Non-Repudiation (40) Edit Properties Copy to Fie Learn more about certificate details OK	Field	Value	Field		Value	*
	Public key Authority Key Identifier Authority Information Access Certificate Policies CRL Distribution Points Netscape Cert Type Key Usage Thumhorint alon:ithm Digital Signature (80)	RSA (1024 Bits) KeyID=93 07 55 62 fe a6 76 3 [1]Authority Info Access: Acc [1]CerL Distribution Point: Distr SSL Clent Authentication, SMI Digital Signature (80) sha1	Certifica CRL Dist CRL DIST CR	te Policies ibution Points e Cert Type Certificate Statem ge init algorithm init tion (40)	[1]Certificate Policy:Policy Ide [1]CRL Distribution Point: Distr SMIME (20) 30 03 03 08 06 06 04 00 8e 46 Non-Repudiation (40) sha1 0d a4 d5 e1 cd cb af 29 d1 33	•
ОК						
		ОК				Ж



General Details Certification Path	
Show: <all></all>	•
Field	Value ^
Authority Information Access Subject Alternative Name 2.5.29.9	[1]Authority Info Access: Acc RFC822 Name=mattwheaton 30 12 30 10 06 08 2b 06 01 05
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4
Thumborint algorithm	bigital Signature, Non-Repudia
Thumbprint	16 71 54 4e 9a 20 51 cf a7 5a
Digital Signature, Non-Repudiation i	(c0)
Digital Signature, Non-Repudiation i	(c0) it Properties

Extended Key Usage

Open the properties of the certificate and search for the property "Extended Key Usage".

The property should be missing, or either contain "Smart Card Logon" or "Client Authentication".

If the attribute is present but does not contain one of these tags, the certificate can't be used for smart card logon.

In the following example, the first certificate doesn't have this attribute (OK). In the second example, the attribute is populated, but with one usage not listed (Not OK).



rtificate	7
eneral Details Certification Path	
how: Extensions Only	-
Field	Value
Authority Key Identifier	KeyID=93 07 55 62 fe a6 76 3
Authority Information Access	[1]Authority Info Access: Acc
Certificate Policies	[1]Certificate Policy:Policy Ide
CRL Distribution Points	[1]CRL Distribution Point: Distr
Netscape Cert Type	SSL Client Authentication, SMI
	/
KeyID=93 07 55 62 fe a6 76 34 dc	35 7f af a7 70 f5 0b 3c 40 00 9f
KeyID=93 07 55 62 fe a6 76 34 dc	35 7f af a7 70 f5 0b 3c 40 00 9f
KeyID=93 07 55 62 fe a6 76 34 dc	35 7f af a7 70 f5 0b 3c 40 00 9f dit Properties
KeyID=93 07 55 62 fe a6 76 34 dc	35 7f af a7 70 f5 0b 3c 40 00 9f dit Properties
KeyID=93 07 55 62 fe a6 76 34 dc	35 7f af a7 70 f5 0b 3c 40 00 9f dit Properties
KeyID=93 07 55 62 fe a6 76 34 dc .earn more about <u>certificate details</u>	35 7f af a7 70 f5 0b 3c 40 00 9f dit Properties
KeyID=93 07 55 62 fe a6 76 34 dc .earn more about <u>certificate details</u>	35 7f af a7 70 f5 0b 3c 40 00 9f dit Properties

Certificate	×
General Details Certification Path	
Show: Extensions Only	•
Field	Value 🔺
Authority Key Identifier Subject Key Identifier Enhanced Key Usage Netscape Cert Type Cert Dificate Policies CRL Distribution Points Authority Information Access Subject Alternative Name Code Signing (1.3.6.1.5.5.7.3.3)	KeyID=1e c5 b1 2c 7d 87 da 0 e8 61 c4 2d ae c1 a9 d5 3c 8c Code Signing (1.3.6.1.5.5.7.3.3) Signature (10) [1]Certificate Policy:Policy Ide [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc BEC822 Name=contact/itmus
Ec	it Properties
	ОК

	Details	Certification Path		_
how:	<all></all>		•	
Field			Value	*
Au Sul	thority In bject Alte	formation Access rnativ <mark>e N</mark> ame	[1]Authority Info Access: Acc RFC822 Name=mattwheaton	
1 2.5	5.29.9		30 12 30 10 06 08 2b 06 01 05	
. En	hanced Ki	ey Usage	Smart Card Logon (1.3.6.1.4	
Ke	y Usage		Digital Signature, Non-Repudia	
Th	umbprint	algorithm	sha1	E
🛅 Th	umbprint		16 71 54 4e 9a 20 51 cf a7 5a	
Smart (Client #	Card Logo	n (1.3.6.1.4.1.31) ation (1.3.6.1.5.5.	1.20.2.2) 7.3.2)	+
Smart (Client / Secure	Card Logo Authentica Email (1.	n (1.3.6.1.4.1.311) abon (1.3.6.1.5.5. 3.6.1.5.5.7.3.4)	1.20.2.2) 7.3.2) it Properties	•



CRL Troubleshooting.

Solution :

Trust issues :

- If the certificate is not trusted by the computer certificate store of the client computer or the domain controller, add the certificates missing in a GPO or directly in the certificate stores involved.
- If a root or intermediate certificate is missing in the NTLM store, you can add it using the command : certutil -dspublish -f [cert file] NtAuthCA

Don't forget that the certificates need 8 hours to be deployed for the NTLM store. You force the deployment using the command gpdupate /force on the domain controller and on the client computer.

CRL issues :

Please see the chapter *Check that* the smart card can be used for logon

Key usage

Open the properties of the certificate and search for the property "Key Usage".

This property should contain one of the following :

- Key Encipherment
- Data Encipherment
- Digital Signature

If it doesn't, the certificate can't be used for smart card logon.

In the following example, the first certificate is ok. The second isn't.



Certificate	Certificate
General Details Certification Path	General Details Certification Path
Show: <all></all>	Show: <ali></ali>
Field Value Public key RSA (1024 Bits) Authority Key Identifier KeyID=93 07 55 62 fe a6 76 3 Authority Information Access [1]Authority Info Access: Acc Certificate Policies [1]Certificate Policy:Policy Ide CRL Distribution Points [1]CRL Distribution Point: Distr CRL Netscape Cert Type SSL Client Authentication, SMI Key Usage Digital Signature (80)	Field Value Image: Certificate Policy: Policy Ide [1]Certificate Policy: Policy Ide Image: CRL Distribution Points [1]CRL Distribution Point: Distr Image: CRL Distribution Points [1]CRL Distribution Points Image: CRL Distr
Edit Properties Copy to File Learn more about certificate details	Edit Properties Copy to File Learn more about certificate details
Certificate	
Show: <all></all>	
Field Value Authority Information Access Subject Alternative Name RFC822 Name=mattwiheaton 2.5.29.9 30 12 30 10 06 08 2b 06 01 05 Enhanced Key Usage Smart Card Logon (1.3.6.1.4 Key Usage Digital Signature, Non-Repudia Thumbprint algorithm sha1 Thumbprint 16 71 54 4e 9a 20 51 cf a7 5a 	
Digital Signature, Non-Repudiation (c0)	
Edit Properties Copy to File	
ОК	

Extended Key Usage

Open the properties of the certificate and search for the property "Extended Key Usage".

The property should be missing, or either contain "Smart Card Logon" or "Client Authentication".

If the attribute is present but does not contain one of these tags, the certificate can't be used for smart card logon.



In the following example, the first certificate doesn't have this attribute (OK). In the second example, the attribute is populated, but with one usage not listed (Not OK).

General Details Certification Path Show: Extensions Only Field Value Authority Information Access: [1]Authority Information Access: [1]Authority Information Access: [1]Certificate Policy:Policy Ide Certificate Policies [1]Certificate Policy:Policy Ide Certificate Policy: SSL Clent Authentication, SML [Certificate Policy: SSL Clent Authentication, SML [Certificate Policy: Digital Signature (80) [Edit Properties Copy to File Learn more about certificate details [Certificate [Certif			Certif
Show: Extensions Only Field Value Authority Key Identifier KeyID=93 07 55 62 fe a6 76 3 Authority Information Access [1] Authority Info Access: Acc Certificate Policies [1] Certificate Policy:Policy Ide Certificate Policies [1] Certificate Policy:Policy Ide ReyID=93 07 55 62 fe a6 76 34 dc 35 7f af a7 70 f5 0b 3c 40 00 9f Edit Properties Copy to File Learn more about certificate details Certificate Certificate Certificate	General Details Certification Path		Gen
Show: Extensions Only Field Value Authority Key Identifier KeyID=93 07 55 62 fe a6 76 3 Authority Information Access [1]Authority Info Access: Acc Certificate Policies [1]Certificate Policy:Policy Ide CRL Distribution Points [1]CRL Distribution Points [Copy to File] [Copy to File] [Common about certificate details [Certificate [Certificate [Certificate [Certificate [Certification Path] [Show: All> [Certification Path] [Show: All> [Certificate Point Prince [Certificate Point Po			
Field Value Authority Key Identifier KeyID=93 07 55 62 fe a6 76 3 Authority Information Access: [1]Authority Info Access: Acc Certificate Policies [1]Certificate Policy:Policy Ide CRL Distribution Points [1]CRL Distribution Point: Distr Netscape Cert Type SSL Clent Authentication, SMI Netscape Cert Type SSL Clent Authentication, SMI Key Usage Digital Signature (80) KeyID=93 07 55 62 fe a6 76 34 dc 35 7f af a7 70 f5 0b 3c 40 00 9f Edit Properties Copy to File Learn more about certificate details	Show: Extensions Only	-	Sho
Authority Key Identifier KeyID=93 07 55 62 fe a6 76 3 Authority Information Access [1]Authority Info Access: Acc Certificate Policies [1]Certificate Policy:Policy Ide CRL Distribution Points [1]CRL Distribution Point: Distr Netscape Cert Type SSL Client Authentication, SMI Edit Properties Copy to File Learn more about certificate details OK Certificate Certificate Show: Certification Path Show: Certification Path	Field	Value	E F
Authority Information Access [1]Authority Info Access: Acc Certificate Policies [1]Certificate Policy:Policy Ide CRL Distribution Points [1]CRL Distribution Point: Distr Netscape Cert Type SSL Client Authentication, SMI Netscape Digital Signature (80) Key Usage Digital Signature (80) Edit Properties Copy to File Learn more about certificate details Certificate Certificate General Details Certification Path Show:	Authority Key Identifier	KeyID=93 07 55 62 fe a6 76 3	
CRL Distribution Points [1]Certificate Policy:Policy Ide CRL Distribution Points [1]CRL Distribution Point: Distr Netscape Cert Type SSL Client Authentication, SML Netscape Cert Type SSL Client Authentication, SML Edit Properties Copy to File Learn more about certificate details Coc Certificate General Details Certification Path Show: CAll>	Authority Information Access	[1]Authority Info Access: Acc	
CRC Distribution Points [1]CRC Distribution Point: Distr Netscape Cert Type SSL Clent Authentication, SML Digital Signature (80) Key/ID=93 07 55 62 fe a6 76 34 dc 35 7f af a7 70 f5 0b 3c 40 00 9f Edit Properties Copy to File Learn more about certificate details OK certificate Show: Call>	Certificate Policies	[1]Certificate Policy:Policy Ide	
Key Usage Digital Signature (80) KeyID=93 07 55 62 fe a6 76 34 dc 35 7f af a7 70 f5 0b 3c 40 00 9f Edit Properties Copy to File Learn more about certificate details OK Central Details Certification Path Show: Call>	Netscape Cert Type	SSL Client Authentication, SMI	
KeyID=93 07 55 62 fe a6 76 34 dc 35 7f af a7 70 f5 0b 3c 40 00 9f Edit Properties Copy to File Learn more about certificate details OK	Key Usage	Digital Signature (80)	
KeyID=93 07 55 62 fe a6 76 34 dc 35 7f af a7 70 f5 0b 3c 40 00 9f Edit Properties Copy to File Learn more about certificate details Coc Certificate Show: Call>			
KeyID=93 07 55 62 fe a6 76 34 dc 35 7f af a7 70 f5 0b 3c 40 00 9f Edit Properties Edit Properties Copy to File Learn more about certificate details OK ettificate Show: cAll>			
Edit Properties Copy to File Learn more about certificate details	KeyID=93 07 55 62 fe a6 76 34 dc	35 7f af a7 70 f5 0b 3c 40 00 9f	þ
Edit Properties Copy to File Learn more about certificate details OK Certificate General Details Certification Path Show: <all></all>			
Edit Properties Copy to File Learn more about certificate details			
Edit Properties Copy to File Learn more about <u>certificate details</u>			
Edit Properties Copy to File Learn more about <u>certificate details</u> OK ertificate General Details Certification Path Show: <all></all>			
Edit Properties Copy to File Learn more about certificate details CK ertificate ertificate Ertificate Show: cAll>			
ertificate ertificate details OK OK ertificate Ertificate Extinction Cox Extincti	Ēd	lit Properties	
ertificate General Details Certification Path Show: cAll>	Learn more about <u>certificate details</u>		Le
ertificate			
ertificate		ОК	
ertificate			
	General Details Certification Path		
Field Value	Show: <all></all>	•	
Authority Information Access [1]Authority Info Access: Acc	Show: <all></all>	Value ^	
Subject Alternative Name RFC822 Name=mattwheaton	Show: <all> Field Authority Information Access</all>	Value [1]Authority Info Access: Acc	
2.5.29.9 30 12 30 10 06 08 25 06 01 05	Show: <all> Field Field Subject Alternative Name</all>	Value [1]Authority Info Access: Acc RFC822 Name=mattwheaton	
Key Usage Digital Signature, Non-Repudia	Show: <all> Field Field Subject Alternative Name Subject Name Su</all>	Value [1]Authority Info Access: Acc RFC822 Name=mattwheaton 30 12 30 10 06 08 2b 06 01 05 Smatt Card Locop (1 2 5 1 4	
Thumbprint algorithm sha 1	Show: <all> Field Field Subject Alternative Name Subject Alternative Name Field Field Subject Alternative Name Field Fie</all>	Value ^ [1]Authority Info Access: Acc ^ RFC822 Name=mattwheaton 30 30 12 30 10 06 08 2b 06 01 05 5 Smart Card Logon (1.3.6.1.4 Digital Signature, Non-Repuda	
Thumbprint 16 71 54 4e 9a 20 51 cf a7 5a	Show: <all> Field Field Subject Alternative Name C.5.29.9 FinAnced Key Usage Key Usage Thumbprint algorithm</all>	Value [1]Authority Info Access: Acc RFC822 Name=mattwheaton 30 12 30 10 06 08 2b 06 01 05 Smart Card Logon (113.6.1.4 Digital Signature, Non-Repudia sha1	
	n Access lame	Value [1] Authority Info Access: Acc RFC822 Name=mattwiheaton 30 12 30 10 06 08 2b 06 01 05 Smart Card Logon (1.3.6.1.4 Digital Signature, Non-Repudia sha1 16 71 54 4e 9a 20 51 cf a7 5a 20.2.2) 7.3.2) 	
Edit Properties Copy to File	Show: <all> Field Field Control Access Control Control</all>	Value [1] Authority Info Access: Acc RFC822 Name=mattwheaton 30 12 30 10 06 08 2b 06 01 05 Smart Card Logon (1.3.6.1.4 Digital Signature, Non-Repudia sha1 16 71 54 4e 9a 20 51 cf a7 5a to 2.22) 7.3.2) It Properties Copy to File	
Edit Properties Copy to File	Show: All> Field Field Subject Alternative Name Subject Alternative Name Enhanced Key Usage Thumbprint algorithm Thumbprint Smart Card Logon (1.3.6.1.4.1.311 Client Authentication (1.3.6.1.5.5.7 Secure Email (1.3.6.1.5.5.7.3.4) Learn more about certificate details	Value	
Edit Properties Copy to File	Show: <all> Field Field Authority Information Access Subject Alternative Name Subject Alternative Name Subject Alternative Name Enhanced Key Usage Thumbprint algorithm Thumbprint Smart Card Logon (1.3.6.1.4.1.311 Client Authentication (1.3.6.1.5.5.7 Secure Email (1.3.6.1.5.5.7.3.4) Ed Learn more about certificate details</all>	Value [1]Authority Info Access: Acc RFC822 Name=mattwheaton 30 12 30 10 06 08 2b 06 01 05 Smart Card Logon (1.3.6.1.4 Digital Signature, Non-Repudia sha1 16 71 54 4e 9a 20 51 cf a7 5a To 20.2.2) 7.3.2) It Properties Copy to File	





CRL Troubleshooting.



Your credentials could not be verified

Message:



The system could not log you on. Your credentials could not be verified.

Cause :

The domain controller couldn't find the account which is associated to the smart card

OR the certificate has been associated to more than one account.

Solution :

Associate the certificate to the account using explicit or UPN mapping.

OR verify that the certificate has not been assigned using explicit mapping twice.

Run AdExplorer.exe and go the menu "search".

Search for the attribute "altSecurityIdentities" with the relation "Not Empty". Then check for duplicate results.

D Search Container				×
Search for objects with the following a	ttributes:			_
Attribute: altSecurityIdentities	•			
Relation: is				
Value:				
(altSecurityIdentities=*)			Add Remo	ve
Current Search Criteria:				
Attribute Relation	Value			
altSecurityIdentities not empty				
distinguishedName	altSecurityIdentities			
CN=Adiant,CN=Users,DC=test,DC=.	. X509: <i>C=BE,CN=Foreigner CA,SERIALNUM X509:<i>C=BE,CN=Foreigner CA,SERIALNUM</i></i>	BER=200804 <s>C=FR,CN=Vince BER=200804<s>C=FR CN=Vince</s></s>	nt Le Toux (Authenticat	
B civitata, civitoseis, be-test, be-iii	Asis. C/C-BE, CN-Foliagilai CA, SEMINENOM	BEI1-200044320-111,014-11108	The Le Toux (Authenticat	
Save			Search Ca	ancel



You cannot use a smart card to log on because smart card logon is not supported for your user account

Message :



The system could not log you on. You cannot use a smart card to log on because smart card logon is not supported for your user account. Contact your system administrator to ensure that smart card logon is configured for your organization.

Cause :

The domain controller has no certificate issued by the Enterprise PKI component in its computer certificate store.

This can be confirmed by the event 19 or 29: "The key distribution center (KDC) cannot find a suitable certificate to use for smart card logons, or the KDC certificate could not be verified. Smart card logon may not function correctly if this problem is not resolved. To correct this problem, either verify the existing KDC certificate using certuil.exe or enroll for a new KDC certificate."

Error	3/8/2015 6:05:35 PM	Kerberos-Key-Distribution-Center	19	None	
🔔 Warning	3/8/2015 6:05:15 PM	Kerberos-Key-Distribution-Center	29	None	-
٠Î		III			•
Event 29, Kerberos-Key	y-Distribution-Center				×

Solution :

A) You can force the application of the domain controller GPO to re-create the certificate using "gpupdate /force".

B) You can manually recreate the Domain Controller Authentication certificate.

On the domain controller, open mmc.

Click File, Click Add/Remove Snap-in.

Select Certificates, click Add, then select Computer account.



Expand Certificates (Local Computer), right-click Personal, click All Tasks, and then click Request New Certificate.

🚡 Console1 - [Console Root\Certificates (Lo	ocal Compu	ter)\Personal\Certificates]		- • •
🔚 File Action View Favorites Wind	dow Help	•		_ 8 ×
🗢 🔿 📶 📋 🙆 🛃 🗖)			
Console Root	*	Issued To	Issued By	Actions
Certificates (Local Computer)		°⊊ CA	CA	Certificates 🔺
▲ Personal		🙀 WIN-PGAHI2ECI8E.test.mysmar	CA	More 🕨
All Tasks	•	Request New Certificate		
C View	•	Import	I-PGAHI2ECI8E.	
▷ 📫 Ente New Window from He	re	Advanced Operations	•	
Inter Inter Inter Inter New Taskpad View			_	
C Refresh				
Export List				
⊳ 🚞 Rem Help				
<	4	< III	Þ	
Request a new certificate from a certification	authority (CA) in your domain		

Press Next

🗔 Ce	ertificate Enrollment	
	Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based on predefin Certificate enrollment policy may already be configured for you.	ed certificate templates.
	Configured by your administrator	
	Active Directory Enrollment Policy	~
	Configured by you	Add New
	Learn more about <u>certificate enrollment policy</u>	
		Next Cancel



ertificate Enrollment		
Request Certificates		
You can request the following types of certi click Enroll.	ficates. Select the certificates you wa	nt to request, and then
Active Directory Enrollment Policy		
Directory Email Replication	i STATUS: Available	Details 🗸
Domain Controller	i) STATUS: Available	Details 🗸
Domain Controller Authentication	I STATUS: Available	Details 💌
Show <u>all</u> templates		
Learn more about <u>certificates</u>		
		Enroll Cancel

The certificate will be automatically enrolled.

📮 Ce	rtificate Enrollment		
	Certificate Installation Results		
	The following certificates have been enrolled	and installed on this computer.	
	Active Directory Enrollment Policy		
	✓ Domain Controller Authentication	✓ STATUS: Succeeded	Details ♥
			Finish



The requested key container does not exist on the smart card

Message :



The system could not log you on. The requested certificate does not exist on the smart card. The system could not log you on. The requested key container does not exist on the smart card. The system could not log you on. The requested keyset does not exist on the smart card.

Cause :

There is a problem with the smart card driver. The problem can be seen when trying to connect with terminal server.

Solution :

Check using certutil -scinfo that the driver is installed on the server and on the client computer.



An error occurred trying to use this smart card

Message :

em could not log n the event log. P	you on. An er	rror occurred tryin is error to the syste	g to use this sma em administrato	art card. You can find furt r.
r the event log. r	ease report an	is enor to the syst	an durini istrato	
		ОК	_	
	em could not log n the event log. Pl	em could not log you on. An e n the event log. Please report th	em could not log you on. An error occurred tryin n the event log. Please report this error to the syste OK	em could not log you on. An error occurred trying to use this sma n the event log. Please report this error to the system administrator OK

The system could not log you on. An error occurred trying to use this smart card. You can find further details in the event log. Please report this error to the system administrator.

Additional symptom:

Event 4625: An error occured during Login.

Status: 0xc00006d (logon failure)

Substatus: 0xc0000321 (The Kerberos protocol encountered an error while attempting to use the smart card subsystem.) [source]

ent 4625, Micros	oft Windows securit	ty auditing.			
ieneral Details					
An account fail	led to log on.				
Subject:					
Securi	ity ID:	SYSTEM			
Accou	unt Name:	WIN-PGAH	IZECIBES		
Accou	ont Domain:	Ov3e7			
cogor		0.00			E
Logon Type:		2			
Account For W	hich Logon Failed:				
Securi	ity ID:	NULL SID			
Accou	unt Name:				
Accou	unt Domain:				
Failure Informa	ition:				
Failur	e Reason:	An Error oc	cured during Log	ion.	
Sub Status	n tatus:	0xc00000321			
Process Inform	ation:				
Caller	Process Name:	C:\Window	s\System32\winle	ogon.exe	
				and the second se	
Network Inform	nation: station Name	WINL DGAH	DECIRE		
-	** * * * * * *	137661	ELCOL		
Log Name:	Security				
Source	Microsoft Wind	lows security	Logge <u>d</u> :	10/3/2015 7:29:04 PM	
Event ID:	4625		Task Category:	Logon	
Level:	Information		Keywords:	Audit Failure	
<u>U</u> ser:	N/A		Computer:	WIN-PGAHIZECIBE.test.mysmartlogon.com	
OpCode:	Info				
More Informatio	on: Event Log Onli	ne Help			

Cause :

There is a problem with the smart card driver and/or the configuration. The system was unable to pick a detailed error message.



Solution :

Contact your smart card manufacturer. To get more detail about the problem, you can run api monitor and attach to lsass.exe. You'll be able to report unusual error.

Example: in the following example, kerberos was unable to load the KSP

kerberos.DLL	NCryptOpenStorageProvider (0x0000000159d03x0, "OpenSC CSP", 0)	NTE_FAIL	0x80090020 = An internal error
ncrypt.dll	-BCryptResolveProviders (NULL, NCRYPT_KEY_STORAGE_INTERFACE, "KEY_STORAGE", "OpenSC CSP", CRYPT_UM, 0, 0x00000000565d930, 0x000	STATUS_NOT_FOUND	0xc0000225 = The object was n



No valid certificates found

Message :

"No valid certificates found" or the certificate is not shown on the logon screen.

Windows Security		×
Smart card lo mysmartlogon.c	ogon tester	
	Use another account	
	No valid certificates found Check that the card is inserted corre	
	OK Canc	el

Causes :

The only mapping allowed is the UPN mapping

OR

The usage attributes described in the certificate forbid the use of this certificate for smart card logon.

For example, you are trying to access a server using terminal server from a client computer which does not belong to the current domain.

OR

The certificate chain is not trusted.

Solutions

If the UPN mapping is the only mapping authorized, you can remove all the client restriction by setting all the possible GPOs.



Group Policy Management Editor			- • •
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp			
🗢 🔿 🔁 🗊 🔒 🛛 🖬 🕎			
 Default Domain Policy [WIN-PGAHI2ECI8E.TES' Computer Configuration Policies Software Settings Windows Settings Administrative Templates: Policy del System System Windows Components BitLocker Drive Encryption Internet Explorer 	Setting Setting Allow certificates with no extended key usage certificate attr Allow Integrated Unblock screen to be displayed at the time Allow signature keys valid for Logon Turn on certificate propagation from smart card Turn on root certificate propagation from smart card Prevent plaintext PINs from being returned by Credential M Allow ECC certificates to be used for logon and authenticati Filter duplicate logon certificates Force the reading of all certificates from the smart card Content of the smar	State Enabled Not configured Enabled Not configured Not configured Not configured Not configured Not configured	Comment No No No No No No No
Kemote Desktop Services	Turn on Smart Card Plug and Play service Notify user of successful smart card driver installation	Not configured Not configured	No No
	Extended Standard		

In this case :

- Allow certificates with no extended key usage certificate attribute
- Allow signature keys valid for logon
- Force the reading of all certificates from the smart card

You can verify that the GPO is deployed by verifying the registry keys :



If the certificate is still not shown, it can't be used for smart card logon.

Please see the chapter : Check that the smart card can be used for logon

As an alternative, you can use the following registry key file :



Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialPro
vider]
"AllowCertificatesWithNoEKU"=dword:00000001
"AllowSignatureOnlyKeys"=dword:00000001
"ForceReadingAllCertificates"=dword:0000001

To check that the smart card certificate is trusted, run certutil -scinfo and at the end of the procedure, double-click on the certificate and check that the mention "the certificate is ok" is shown.

Otherwise, be sure that the root certificate and the intermediates certificates are registered in the user certificate store. This store can be accessed using certmgr.msc.

A workaround for the terminal server client (mstsc.exe) used without administrator rights, exists :

You can disable NLA on the server using the system properties. Just **deselect** "Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)".

System	n Properties ×
Computer Name Hardware Advar	nced System Protection Remote
Remote Assistance	
Allow <u>R</u> emote Assistance conn	ections to this computer
What happens when I enable Ren	note Assistance?
	Ad <u>v</u> anced
Remote Desktop	
Choose an option, and then specif	y who can connect.
<u>D</u> on't allow remote connection	s to this computer
Allow remote connections to the	is computer
Allow connections only from Desktop with <u>N</u> etwork Leve	computers running Remote al Authentication (recommended)
Help me choose	Select Users
	OK Cancel Apply

You have to disable NLA on the client for this session by editing the rdp file related to this connection using notepad and append the following line : **EnableCredSspSupport:i:0**





Checking for a healthy smart card

Using certutil

Certutil is a troubleshooting tool provided by Microsoft.

Note : certutil.exe is installed by default starting Windows Vista and Windows 2008. Certutil can be installed on Windows XP by the package "WindowsServer2003-KB304718-AdministrationToolsPack"

You can run certutil by typing Windows +R

🖅 Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	cmd 🗸
	This task will be created with administrative privileges.
	OK Cancel <u>B</u> rowse

Then "cmd" then "certutil -scinfo"

Expected diagnostic of a healthy smart card

Administrator: C:\Windows\system32\cmd.exe
C:\SmartCardMinidriverTest>certutil -scinfo The Microsoft Smart Card Resource Manager is runn Current reader/card status: Readers: 1 Ø: MySmartLogon Uirtual Smart Card Reader Ø Reader: MySmartLogon Uirtual Smart Card Reader Ø Status: SCARD_STATE_PRESENT ! SCARD_STATE_UNPOWERED Status: The card is available for use Card: EIDUirtual, EIDUirtualSmartCard 3b 8c 01 4d 79 53 6d 61 72 74 4c 6f 67 6f 6e a5 ;MySmartLogon.
Analyzing card in reader: MySmartLogon Virtual Smart Card Reader Ø Missing stored keyset Missing stored keyset
Done. CertUtil: -SCInfo command FAILED: 0x80090016 <-2146893802> CertUtil: Keyset does not exist C:\SmartCardMinidriverTest>

The previous screenshot shows an <u>empty</u> smart card, without any certificate or private key stored (the KeySet does not exist)

(Look at the ATR and the mention "SCARD_STATE_PRESENT")



Smart card absent

An empty smart card reader will produce the following output :



(Look at the mention "SCARD_STATE_EMPTY")

Causes :

- An incompatible smart card has been connected
- The smart card reader doesn't recognize the smart card

Solution :

• Check the connections between the smart card and the reader



A minidriver or a CSP has not been installed

A minidriver or a CSP (the driver of the smart card and not for the reader) not installed will produce the following results :

Insert Smart Card		
Please insert a s	mart card.	
Details	Smot cord incoded:	
	Unknown Card	
MySmartLogon	Smart card status:	
Virtual Smart	A smart card was detected but is not the one required for the current operation. The smart card you are using may be missing required driver software or a required certificate.	
C:\Windows\system32\cm	OK Cancel <u>D</u> etails <<	
Gurrent reader/card :	status:	×
Readers: 1 Ø: NySmartLogon Uin Reader: MySnartLo Status: SCARD_STA Card: Card: 3b 8c 01 4d	rtual Smart Card Reader 0 ogon Virtual Snart Card Reader 0 AIE_PRESENI is augilable for use 79 53 6d 61 72 74 4c 6f 67 6f 6e a5	;MySmartLogon.
Analyzing card in rea SCardGetCardTypeProv: N32: 2) Cannot retrieve Prov: t find the file spec: Cannot retrieve Prov:	ader: MySmartLogon Uirtual Smart Card R iderName: The system cannot find the fi ider Name for SCardGetCardTypeProviderN ificd. Øx2 <\\I N99: 2> ider Name for	eader 0 Le specified. 0x2 (WI ame: The systen canno
Done. CertUtil: -SCInfo con CertUtil: The system C:\Users\Rudolf LEYB	nmand FAILED: 0x2 (WIN32: 2) cannot find the file specified. AERT>_	τ.

An ATR entry, here 3b 8c 01 ..., means that a smart card has been inserted.

However the empty line for "Card" means that the system couldn't find a driver. Moreover, the system returns an error about "Cannot retrieve Provider Name for <null>".



Also the "CALAIS" database in the registry won't show an entry for the smart card.



Note: on 64 bits systems there are two CALAIS database: the 64 bits one and the other in *WOW6432Node*.

Causes :

- No CSP or minidriver has been installed
- A 32 bits but not 64 bits CSP or minidriver has been installed on a 64 bits system
- The smart card doesn't have cryptographic capabilities exposed (EMV cards, NFC, ...)

Solutions :

- 1. Ask your manufacturer for proper software
- 2. Use compatible smart card
- 3. Wait for the installation of the driver if it is auto downloaded from Microsoft Update.

Device Setup		×
Installing device	e	
	Please wait while Setup installs necessary files on your system. This may take several minutes.	
	Cle	se



The smart card resource manager is not running

If the smart card service is not running, the following error will be showed :



Causes :

- The "Smart card" service has been disabled
- A smart card reader has not been connected

Solutions

• Go to "services" (administrative tools), find the service and start it



Check that the smart card can be used for logon

Key usage

Open the properties of the certificate and search for the property "Key Usage".

This property should contain one of the following :

- Key Encipherment
- Data Encipherment
- Digital Signature

If it doesn't, the certificate can't be used for smart card logon.

In the following example, the first certificate is ok. The second isn't.

Certificate		Certificate	X
General Details Certification Path		General Details Certification Path]
Show: <all></all>		Show: <all></all>	-
Field Value	*	Field	Value ^
Public key RSA (1024 Bits) Authority Key Identifier KeyID=93 07 55 62 fe a6 76 Authority Information Access [1]Authority Info Access: A Certificate Policies [1]Certificate Policy:Policy Id CRL Distribution Points [1]Certificate Policy:Policy Id CRL Distribution Points [1]Certificate Policy:Policy Id Netscape Cert Type SSL Client Authentication, SN Key Usage Digital Signature (80) Digital Signature (80) Edit Properties	3 c e t t File	Certificate Policies CRL Distribution Points Qualified Certificates Statem Qualified Certificates Statem CRC y Usage Thumbprint algorithm Thumbprint Non-Repudiation (40)	[1]Certificate Policy:Policy Ide [1]Certificate Policy:Policy Ide [1]CRL Distribution Point: Distr SMIME (20) 30 03 00 80 60 60 40 08 e 46 Non-Repudiation (40) sha1 0d a4 d5 e1 cd cb af 29 d1 33 * tit Properties Copy to File
Learn more about <u>ceruncate details</u>		Learn more about <u>ceruncate details</u>	
	ок		ОК



General Details Certification Path	
Show: <all></all>	•
Field	Value ^
Authority Information Access Subject Alternative Name 2.5.29.9	[1]Authority Info Access: Acc RFC822 Name=mattwheaton 30 12 30 10 06 08 2b 06 01 05
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4
Thumborint algorithm	bigital Signature, Non-Repudia
Thumbprint	16 71 54 4e 9a 20 51 cf a7 5a
Digital Signature, Non-Repudiation i	(c0)
Digital Signature, Non-Repudiation i	(c0) it Properties

Extended Key Usage

Open the properties of the certificate and search for the property "Extended Key Usage".

The property should be missing, or either contain "Smart Card Logon" or "Client Authentication".

If the attribute is present but does not contain one of these tags, the certificate can't be used for smart card logon.

In the following example, the first certificate doesn't have this attribute (OK). In the second example, the attribute is populated, but with one usage not listed (Not OK).



ertificat	e		×
General	Details	Certification Path	
Show:	Extensio	ns Only	•
Field			Value
	uthority Ke uthority In ertificate P RL Distribu etscape Ce ey Usage	y Identifier formation Access iolicies tion Points ert Type	KeyID=93 07 55 62 fe a6 76 3 [1]Authority Info Access: Acc [1]Certificate Policy:Policy Ide [1]CRL Distribution Point: Distr SSL Client Authentication, SMI Digital Signature (80)
KeyID	=93 07 55	62 fe a6 76 34 dc	35 7h at a7 70 f5 0b 3c 40 00 9f
Learn r	nore abou	E t <u>certificate details</u>	it Properties
			ОК

Certificate		x	
General Details Certification Path			
Show: Extensions Only	•		
Field	Value	*	
Authority Key Identifier Subject Key Identifier Subject Key Identifier Brhanced Key Usage Netscape Cert Type Certificate Policies CRL Distribution Points Authority Information Access Subject Alternative Name Code Signing (1.3.6.1.5.5.7.3.3)	KeyID=1e c5 b1 2c 7d 87 da 0 e8 61 c4 2d ae c1 a9 d5 3c 8c Code Signing (1.3.6.1.5.5.7.3.3) Signature (10) [1]Certificate Policy:Policy Ide [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc BEC822 Name=contact@mvs	4 III	
Edit Properties Copy to File			
	0	ĸ	

how: <all></all>	•	
Field	Value	*
Authority Information Access Subject Alternative Name	[1]Authority Info Access: Acc RFC822 Name=mattwheaton	
2.5.29.9	30 12 30 10 06 08 2b 06 01 05	
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4	
Key Usage	Digital Signature, Non-Repudia	
Thumbprint algorithm	sha1	E
Thumbprint	16 71 54 4e 9a 20 51 cf a7 5a	-
Smart Card Logon (1.3.6.1.4.1.31: Client Authentication (1.3.6.1.5.5.	1.20.2.2) 7.3.2)	
Smart Card Logon (1.3.6. 1.4. 1.31 Client Authentication (1.3.6. 1.5. 5. Secure Email (1.3.6. 1.5. 5. 7.3. 4)	1.20.2.2) 7.3.2) fit Properties	•



CRL Troubleshooting

This chapter will investigate CRL processing more deeply, this is the verification process to determine if a certificate has been revoked.

Checking that the certificate revocation check process is working

1) Verify that the certificate contains a "CRL Distribution Point" by opening the certificate

Certificate	×
General Details Certification Path	
Show: <all></all>	•
Field	Value 🔺
Enhanced Key Usage Netscape Cert Type Certificate Policies	Code Signing (1.3.6.1.5.5.7.3.3) Signature (10) [1]Certificate Policy:Policy Ide
CRL Distribution Points	[1]CRL Distribution Point: Distr
Authority Information Access	[1]Authority Info Access: Acc RFC822 Name=contact@mys
Key Usage	Digital Signature (80)
Rasic Constraints	Subject Type=End Entity_Pat
[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.comodoca.	com/COMODOCodeSigningCA.crl
Ec	lit Properties
-	ОК

If no CDP is referenced in a smart card logon certificate and if the CRL checking is not disabled, the smart card logon will fail. See bellow to disable the CRL checking.

- 2) Check that the client computer can contact the CDP by running certutil -urlfetch verify test.cer
- 3) Run this test again using the system account (the proxy used by the system is not the same) by running psexec -s running certutil -urlfetch -verify test.cer
- 4) Run this test on the domain controller, using the system account

Screenshots for working and not working CRL checks

For your information, below you see a working CRL check :

Uerified "Base CRL (0493)" Time: 4 10.01 http://orl.comedoca.com/COM010CodeSigningCA.crl	
Base CRL CDP No URLs "None" Time: Ø Certificate OCSP Verified "OCSP" Time: 4 [0.0] http://ocsp.comodoca.com	
CRL (null): Issuer: CN=COMODO Code Signing CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB	Ŧ



A failed CRL check with no network. Please look at "This network connection does not exists – error 0x800708CA. In this case the computer is not connected to a network.



A failed CRL check with a timeout problem. Please look at the message "The operation timed out" – error 0x80072ee2. In this case, it may be due to a proxy configuration problem. See below for a solution.

CANTER AND CONTRACT AND AND CONTRACT AND AND CONTRACT
Failed "AIA" Time: 0 Error retrieving URL: The operation timed out 0x80072ee2 (WIN32: 12002) http://crt.comodoca.com/COMODOCodeSigningCA.crt
 Failed "CDP" Time: Ø Error retrieving URL: The operation timed out Øx80072ee2 (WIN32: 12002) http://crl.comodoca.com/COMODOCodeSigningCA.crl
Base CRL CDP No URLs "None" Time: 0 Failed "OCSP" Time: 0 Error retrieving URL: The operation timed out 0x80072ee2 (WIN32: 12002) http://ocsp.comodoca.com

You can read this document from Microsoft : How Certificate Revocation Works for more information.

Solving CRL network issues

If the certificate doesn't have a CDP (a CRL distribution point), the CRL checks must be disabled on both the client computer and on the domain controller. See below for a solution.

Other error messages are related to network or proxy configuration problem.

IMPORTANT : the system component which is doing the authentication has its own proxy configuration which is separate from that of individual user accounts. The system proxy settings DO NOT support WPAD scripts nor web proxy autoconfiguration with DNS or DHCP discovery.

You can display current system **WININET** proxy settings from command line with the following commands on **Windows XP/2003** or **Windows Vista** and newer respectively: **proxycfg netsh winhttp show proxy**



You can change the proxy settings with the same commands on **Windows XP/2003** and **Windows Vista** and newer respectively:

proxycfg -p to set a static proxy

proxycfg -d to delete proxy setting and access HTTP directly

netsh winhttp set proxy to set a static proxy

netsh winhttp reset proxy to delete proxy setting and access HTTP directly

Clear the CRL cache for tests

By default, CRL is cached once it has been retrieved on the disk and in the memory of the process which retrieved it. Here is description of how to clear the caches that CryptoAPI maintains to test for certificate revocation.

First, unplug the network to disable the active revocation process.

If the CRL is published via HTTP / HTTPS, you have to clear the browsing history of WinHttp via the Options panel of Internet Explorer. Select *Delete* on the *Browsing History* zone.

Internet Options
General Security Privacy Content Connections Programs Advanced
Home page
To create home page tabs, type each address on its own line.
Use <u>c</u> urrent Use de <u>f</u> ault Use <u>b</u> lank
Browsing history
Delete temporary files, history, cookies, saved passwords, and web form information.
Delete browsing history on exit
Delete Settings
Search
Change search defaults. Settings
Tabs
Change how webpages are displayed in Settings tabs.
Appearance
Colors Languages Fonts Accessibility
OK Cancel Apply

Then you have to clear the CryptoAPI disk cache.

Run the command "*certutil -urlcache* * *delete*" for a normal user and "*psexec -s certutil -urlcache* * *delete*" using the utility <u>psexec.exe</u> provided by SysInternals to clear the cache information of the system account. You can check the cache status using "*psexec -s certutil -urlcache*". *Psexec* needs an elevated prompt to be run.



You can look at the CryptnetUrlCache folder of the SYSTEM account folder (this folder is located in "%WINDIR%\config\systemprofile\AppData\LocalLow\Microsoft\) to monitor this operation.

Then clear the cache of the all processes by running in an elevated prompt :

certutil -setreg chain\ChainCacheResyncFiletime @now

More information about CRL OCSCP caching can be found in the article <u>Troubleshooting PKI problems</u> on <u>Windows Vista</u>

Disable the CRL checks for smart card logon

WARNING : disabling CRL checking can be considered, depending on the context, as a security vulnerability

On the domain controller, apply the following reg file :

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:0000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:0000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:0000001
"CRLTimeoutPeriod"=dword:0000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:0000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:0000001
```



Verifying 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 "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 bellow.





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, 1145593979@mil. There can be other definitions like RFC822 Name.

Certificate		×	
General Details Certification Path			
Show: <all></all>	•		
Field Valid to Subject Public key Subject Key Identifier Subject Alternative Name Key Usage Reinhanced Key Usage Basic Constraints Vier Name: Principal Name=1145593979@m EC922 Name=jobo.doe@example	Value 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 Turne=End Entity. Pat		
Edit Properties			
	0	к	

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

Administrator Propertie	s				? 🗙
Published Certificates	Member Of	Password	Replica	ation	Dial-in Object
Security	Env	vironment			Sessions
Remote control		Remote	Deskto	p Service	es Profile
Personal Virtual De	sktop	COM+		Attr	ibute Editor
General Address	Account	Profile	Telep	hones	Organization
<u>U</u> ser logon name: 1145593979		@mil			•
User logon name (pre-)	Windows 2000	J):			
TEST	_	Administra	ator		
Logon Hours	Log On To				
Unjock account Account options:	Unlock account Account options: User must change password at next logon User cannot change password				
Store password u	Store password using reversible encryption				Ŧ
Account expires					
Never					
<u>E</u> nd of:	Saturday ,	July 12	2, 2014		
	ж	Cancel	A	Joply	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					
Eile Action View Help					
🗢 🔿 🞽 🗊 🗙 🗉 🤷 📑 🚺					
ADSI Edit	Name Cla	ass Actions			
Default naming context [WIN-PGAHI2ECI	These are in income as the suring this side.	CN=Administrator	^		
DC=test,DC=mysmartlogon,DC=com	There are no items to show in this view	ew. More Actions	•		
CN=Builtin					
OII-Domain Controllers					
CN=ForeignSecurityPrincipals					
CN=LostAndFound					
CN=Managed Service Accounts 😑					
CN=NTDS Quotas					
📔 CN=Program Data					
📫 CN=System					
a 🚞 CN=Users					
CN=Adiant					
CN=Administrator					
CN= Allowed RODC Password F					
CN=Cert Publishers					
CN=Denied RODC Password Ri					
CN=DnsUpdateProxy					
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	I=Administrator Propert	ies ? 💌
A	ttribute Editor Security	
	Attri <u>b</u> utes:	
	Attribute	Value
	userAccountControl userCert userCertificate userParameters userPassword	0x200 = (NORMAL_ACCOUNT) <not set=""> <not set=""> <not set=""></not></not></not>
	userPKCS12 userPrincipalName	<not set=""> 1145593979@mil cost set></not>
	userSharedFolderOther userSMIMECertificate userWorkstations uSNChanged uSNCreated uSNDSALastObiRem (111	<pre><not set=""> <not set=""> <not set=""> <not set=""> </not> </not> </not> </not> </pre>
	Edit	
	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"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, then right click "Name mappings".

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



Active Directory Users and Com	iputers			
 Active Directory Users and Comput Saved Queries Soved Queries Computens Computers Domain Controllers ForeignSecurityPrincipals LostAndFound Managed Service Accounts System Users NTDS Quotas 	Name Type Adiar Copy Adiar Copy Adlow Adiar Adiar Copy Adiar Adiar Adiar Copy Adiar Adiar Adiar Copy Adiar Adiar Adiar Adiar Adiar Mail Bona Move Doma Send Mail Boma Cut Doma Cut Doma Delete Enter Rename Enter Rename Group Properties Goust 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 Administrators Group DNS dients who are permitted to perform dynamic updates on be Designated administrators of the domain All workstations and servers joined to the domain All domain guests All domain guests All domain users Designated administrators of the enterprise Members of 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 Mapping	<u>?</u> ×
X.509 Certificates Kerberos Names	
Mapped user account: domain.mysmartlogon/Users/ID80071447162	_
X-509 certificates:	
Certificates For Issued By	
UN=Vincent Le Toux (Autr UN=Poreigner UA	
Add	
OK Cancel Ap	ply



Annex 1 – Procedures

Get the certificate chain

Smart Policy retrieves automatically the certificate chain on the local computer. The certificate MUST be trusted.

The following procedure describes how to manually check the certificate chain

Type Windows Key + R to open the run window and type "certmgr.msc" to open the user certificate store.

📼 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	certmgr.msc 👻
	OK Cancel <u>B</u> rowse

Locate the certificate you want to export its chain

🚡 certmgr - [Certificates - Current U	ser\Personal\Certificates]		x
<u>File Action View H</u> elp			
🗢 🔿 🖄 🖬 🔏 🖬) 🗟 🔽 🖬		
Certificates - Current User	Issued To	Issued By	Ex
Personal	🛱 [not available]	ADIANT-PC	7/
Certificates	🛱 Adiant	LH-WOFYI0EKSYMI	6/
Finisted Root Certification Au Enterprise Trust	🛱 Adiant	ADIANT-PCTEST	12
Enterprise Trust Intermediate Certification Au	🕼 Adiant	ADIANT-PC	7/
Active Directory User Object	🚰 Adiant	ADIANT-PCTEST	7/
Trusted Publishers	🛱 Adiant	ADIANT-PC	12
Untrusted Certificates	🛱 Adiant	ADIANT-PC	12
Third-Party Root Certification	🛱 Administrator	domain-WIN-HNB91NNAB2G-CA	6/
Trusted People	Administrator	domain-WIN-HNB91NNAB2G-CA	6/
Other People	🛱 Dominic Dreyer DEMO (Authen	QuoVadis SuisseID Advanced CA	7/
Image: Smart Card Trusted Roots	🛱 Vincent Le Toux (Authentication)	Foreigner CA	1/
	🛱 Vincent Le Toux (Signature)	Foreigner CA	1/
4 III +	•		۰.
Personal store contains 12 certificates.			

Double click on it and go to the last page.

The "certificate status" should display "This certificate is ok". If not, the root or some intermediate certificates may be missing.



Certificate
General Details Certification Path
Certification path
QuoVadis Root Certification Authority
View Certificate
Certificate <u>s</u> tatus:
This certificate is OK.
Learn more about <u>certification paths</u>
ОК

You will then export each certificate of this chain.

Execute the following procedure for each certificate (you can open an intermediate certificate if you click on "View Certificate")

Export one certificate

Select the second page of the certificate you want to export and select "Copy to a file".

Certificate		x
General Details Certification Path	1	
Show: <all></all>	•	
Field	Value	<u> </u>
Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to	V3 3a ca 5c a4 40 8f 9f b1 sha IRSA sha 1 QuoVadis SuisseID Advanced Friday, July 09, 2010 12:58:1 Tuesday, July 09, 2013 12:58 dominic drever demo@omail.c	T
Learn more about <u>certificate details</u>	dit Properties Copy to File	

If you are trying to export the last certificate of the chain, you may be asked if you want to export the private key. Don't export the private key !





Select the CER format - either DER or base 64 encoding - as all software (except SAP) recognizes both formats.





Adding a certificate to the NTLM store²

Method 1: Import a certificate by using the PKI Health Tool

To import a CA certificate into the Enterprise NTAuth store, follow these steps:

- 1. Export the certificate of the CA to a .cer file. The following file formats are supported:
 - a. DER encoded binary X.509 (.cer)
 - b. Base-64 encoded X.509 (.cer)
- 2. Install the Windows Server 2003 Resource Kit Tools. The tools package requires Windows XP or later.
- 3. Start Microsoft Management Console (Mmc.exe), and then add the PKI Health snap-in:
- 4. On the Console menu, click Add/Remove Snap-in.
- 5. Click the **Standalone** tab, and then click the **Add** button.
- 6. In the list of snap-ins, click Enterprise PKI.
- 7. Click **Add**, and then click **Close**.
- 8. Click OK.
- 9. Right-click Enterprise PKI, and then click Manage AD Containers.
- 10. Click the NTAuthCertificates tab, and then click Add.
- 11. On the **File** menu, click **Open**.
- 12. Locate and then click the CA certificate, and then click **OK** to complete the import.

Method 2: Import a certificate by using Certutil.exe

To import a CA certificate into the Enterprise NTAuth store, follow these steps:

- 1. Export the certificate of the CA to a .cer file. The following file formats are supported:
 - DER encoded binary X.509 (.cer)
 - Base-64 encoded X.509 (.cer)
- 2. At a command prompt, type the following command, and then press ENTER:

certutil -dspublish -f filename NTAuthCA

² http://support.microsoft.com/kb/295663