



Troubleshooting smart card logon authentication on active directory

Version 2.0

Prepared by: "Vincent Le Toux"

Date: 2024-02-15

Table of Contents

Table of Contents

Revision History

Error messages

The smart card certificate used for authentication was not trusted	5
Key usage	Erreur ! Signet non défini.
Extended Key Usage	Erreur ! Signet non défini.
Key usage	Erreur ! Signet non défini.
Extended Key Usage	Erreur ! Signet non défini.
Your credentials could not be verified	14
You cannot use a smart card to log on because smart card logon is not supported for your user account	16

The requested key container does not exist on the smart card

An error occurred trying to use this smart card

The kerberos protocol encountered an error while validating the KDC certificate during smart card logon.

The function requested is not supported

No valid certificates found

Checking for a healthy smart card

Using certutil	28
Expected diagnostic of a healthy smart card	28
Smart card absent.....	29
A minidriver or a CSP has not been installed.....	30
The smart card resource manager is not running.....	32

Check that the smart card can be used for logon

Key usage	33
Extended Key Usage	34

CRL Troubleshooting

Checking that the certificate revocation check process is working	36
Screenshots for working and not working CRL checks	36
Solving CRL network issues	37
Clear the CRL cache for tests	38
Disable the CRL checks for smart card logon	39

Verifying the certificate mapping

Determine the type of mapping	40
Map a certificate to a user account using UPN mapping.....	41
Map a certificate to a user account using Explicit mapping	43

Annex 1 – Procedures

Get the certificate chain.....	46
Export one certificate	47
Adding a certificate to the NTLM store	49
Method 1: Import a certificate by using the PKI Health Tool	49
Method 2: Import a certificate by using Certutil.exe	49

Revision History

This section records the change history of this document.

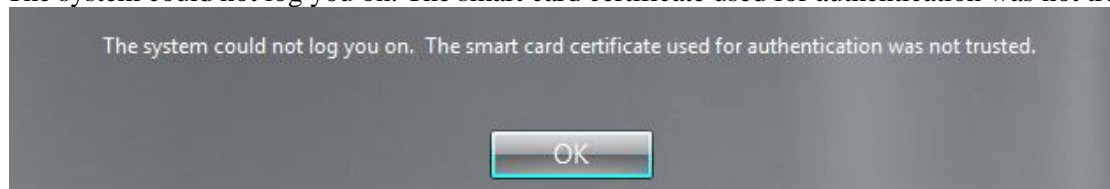
Name	Date	Reason For Changes	Version
Vincent Le Toux	11/06/2014	Creation	1.0
Vincent LE TOUX	2024-02-15	Update	2.0

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".

```
Administrator: C:\Windows\system32\cmd.exe - certutil -scinfo
Performing cert chain verification...
Smart Card Logon: Chain validates
dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000)
ChainFlags = CERT_CHAIN_REVOCACTION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000)
Application[0] = 1.3.6.1.4.1.311.20.2.2 Smart Card Logon
HCCE_LOCAL_MACHINE
CERT_CHAIN_POLICY_NT_AUTH
----- CERT_CHAIN_CONTEXT -----
ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
ChainContext.dwRevocationFreshnessTime: 3 Hours, 40 Minutes, 19 Seconds
SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
SimpleChain.dwRevocationFreshnessTime: 3 Hours, 40 Minutes, 19 Seconds
CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0
Issuer: SERIALNUMBER=200804, CN=Foreigner CA, C=BE
NotBefore: 2/13/2009 12:00 AM
NotAfter: 1/30/2014 12:59 AM
Subject: SERIALNUMBER=80071447162, G=Vincent Xavier, SN=Le Toux, CN=Vincent Le
Toux (Signature), C=FR
Serial: 1000000000006357a105a428e24f79f6
0d a4 d5 e1 cd cb af 29 d1 33 73 84 1a 99 57 2f c5 86 a1 78
Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
CRL 40ad:
Issuer: SERIALNUMBER=200804, CN=Foreigner CA, C=BE
d7 07 ef 1d 66 e6 be e1 6d dd 56 2c e0 d8 97 b2 3d b1 f1 cd
```

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

```
Administrator: C:\Windows\system32\cmd.exe
Performing cert chain verification...
Smart Card Logon: Chain on smart card is invalid
dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000)
ChainFlags = CERT_CHAIN_REVOCACTION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000)
Application[0] = 1.3.6.1.4.1.311.20.2.2 Smart Card Logon
HCCE_LOCAL_MACHINE
CERT_CHAIN_POLICY_BASE
----- CERT_CHAIN_CONTEXT -----
ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
ChainContext.dwRevocationFreshnessTime: 19 Hours, 22 Minutes, 5 Seconds
SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
SimpleChain.dwRevocationFreshnessTime: 19 Hours, 22 Minutes, 5 Seconds
CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0
Issuer: CN=COMODO Code Signing CA 2, O=COMODO CA Limited, L=Salford, S=Greater
Manchester, C=GB
NotBefore: 2/25/2014 2:00 AM
NotAfter: 2/26/2015 1:59 AM
Subject: CN=Vincent Le Toux, O=Vincent Le Toux, STREET=46 rue de l'Alma, L=Cou
rbevoie, S=None, PostalCode=92400, C=FR
Serial: c548553106c8c83335c81d763073bfee
SubjectAltName: RFC822 Name=contact@mysmartlogon.com
e1 9b 93 aa 83 d6 e8 30 78 cd 59 5a f8 29 17 2f 0d 38 61 2e
Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
CRL (null):
Issuer: CN=COMODO Code Signing CA 2, O=COMODO CA Limited, L=Salford, S=Great
er Manchester, C=GB
82 96 74 72 e3 d9 f6 6c 7f 11 21 0d 60 e4 43 f5 ee f1 19 4c
Issuance[0] = 1.3.6.1.4.1.6449.1.2.1.3.2
Application[0] = 1.3.6.1.5.5.7.3.3 Code Signing
```

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%")

- 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

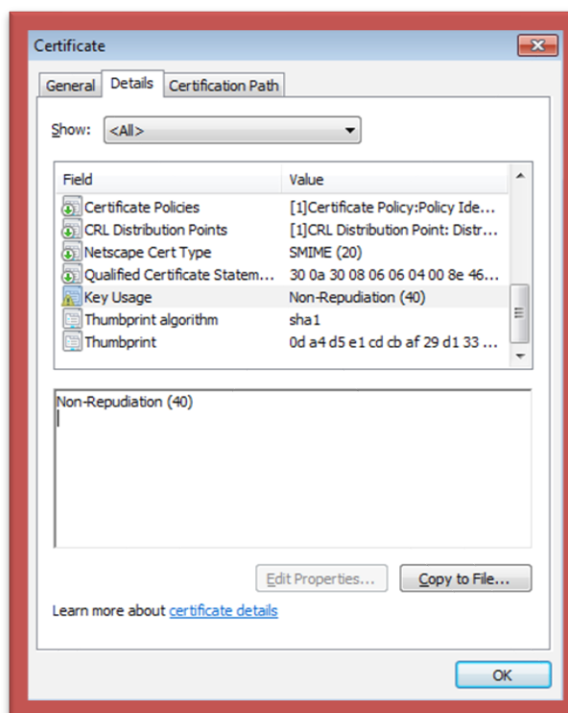
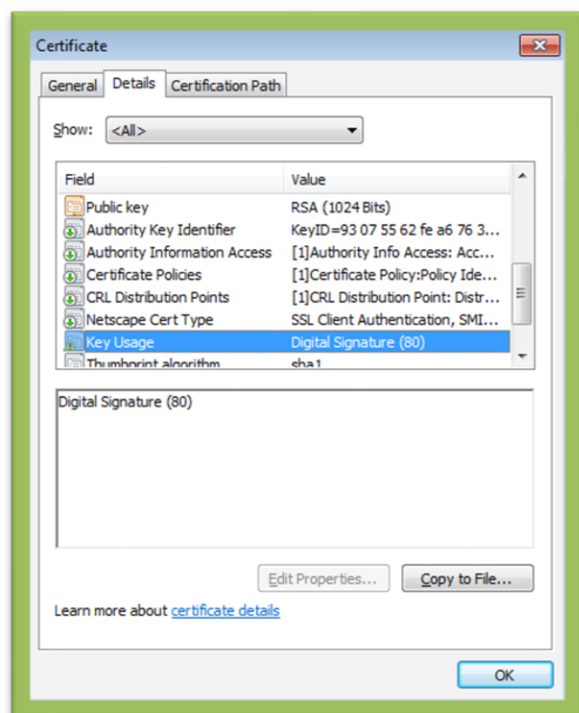
Open the properties of the certificate and search for the property "Key Usage".

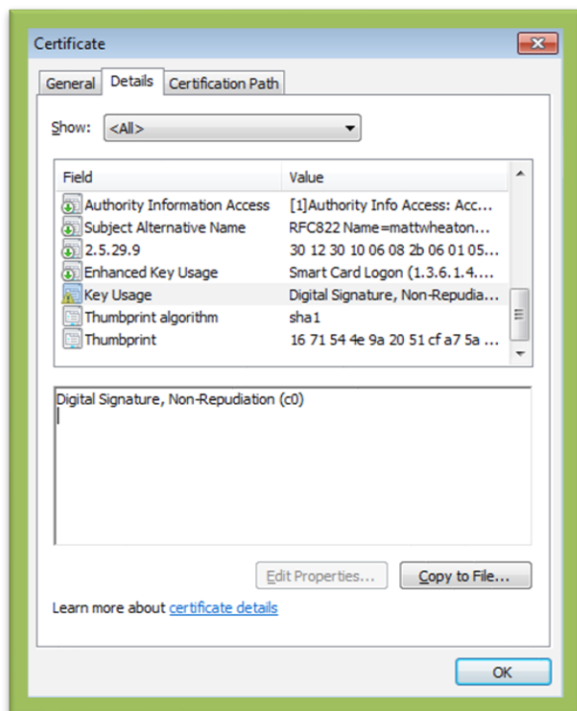
This property should contain one of the following :

- 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.





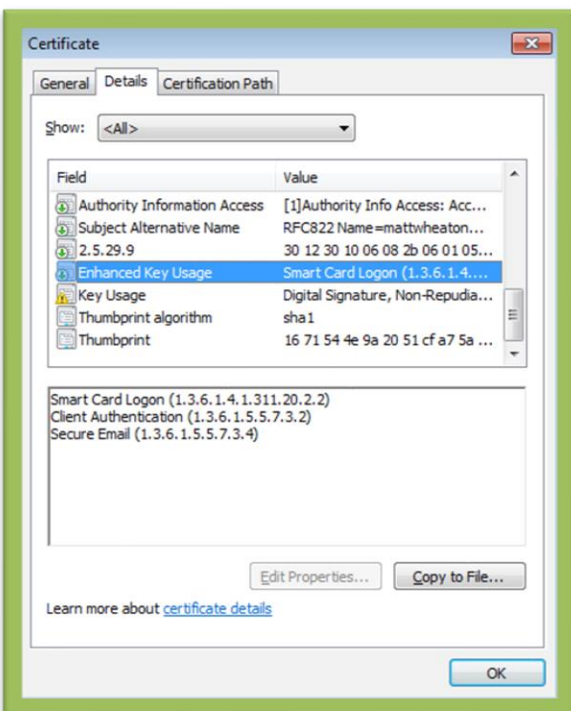
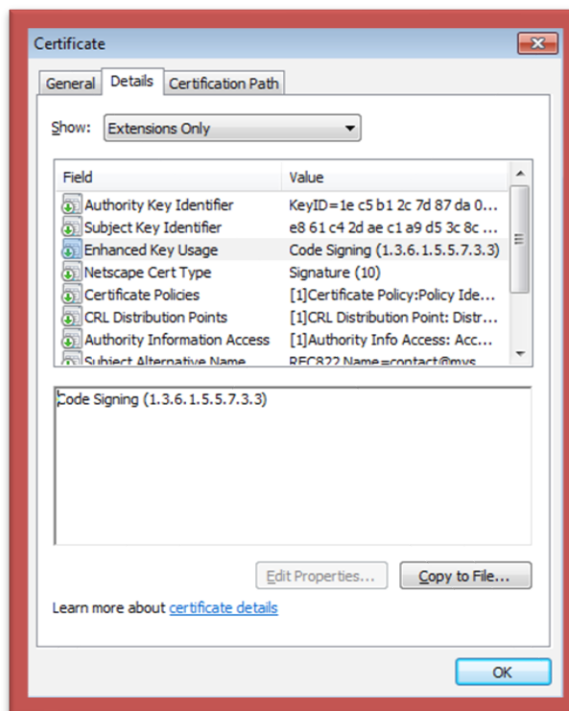
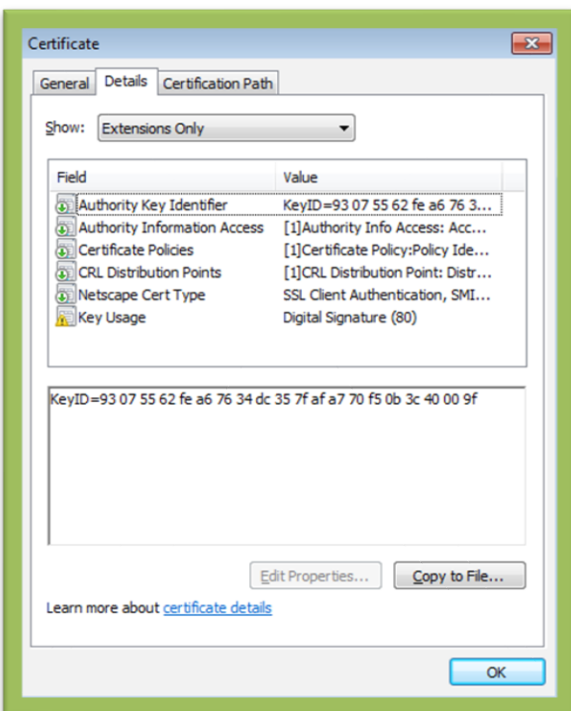
Extended Key Usage

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).



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 `gpupdate /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

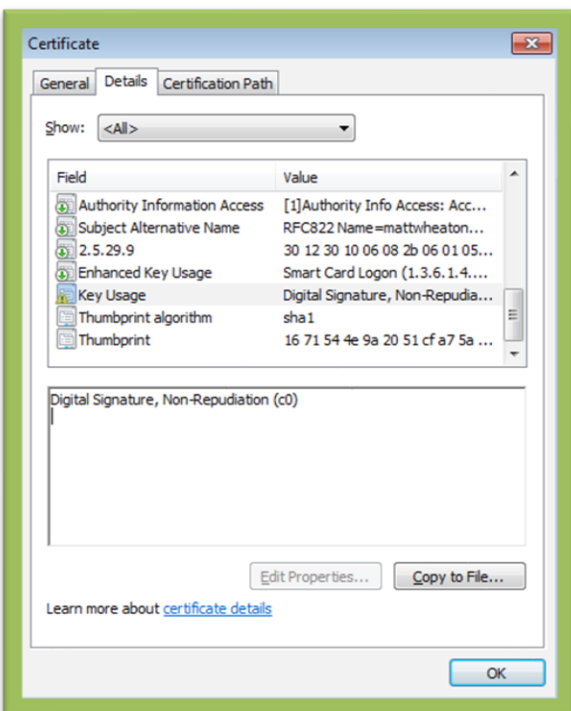
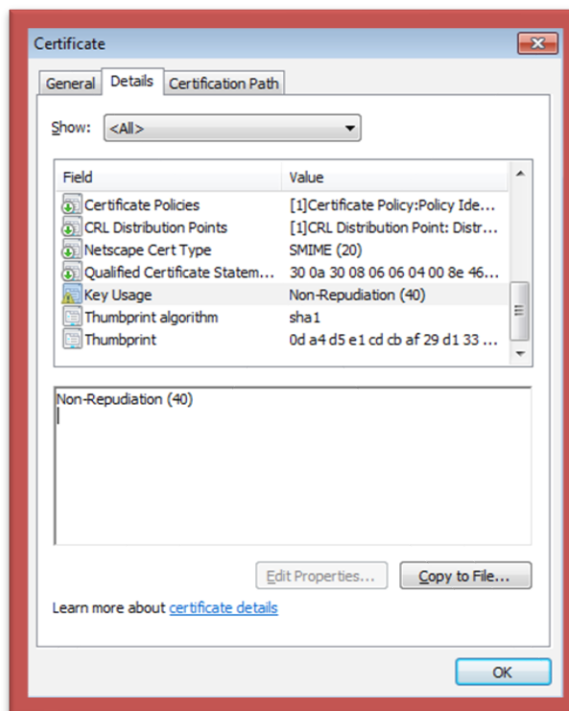
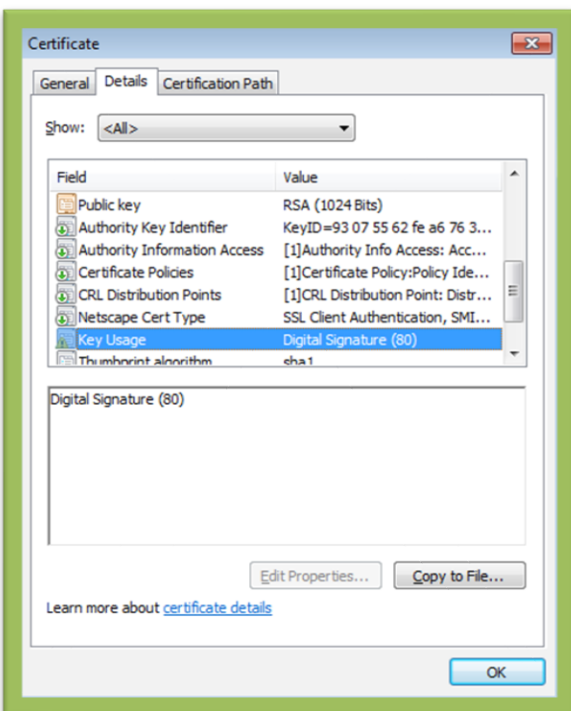
Open the properties of the certificate and search for the property "Key Usage".

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.



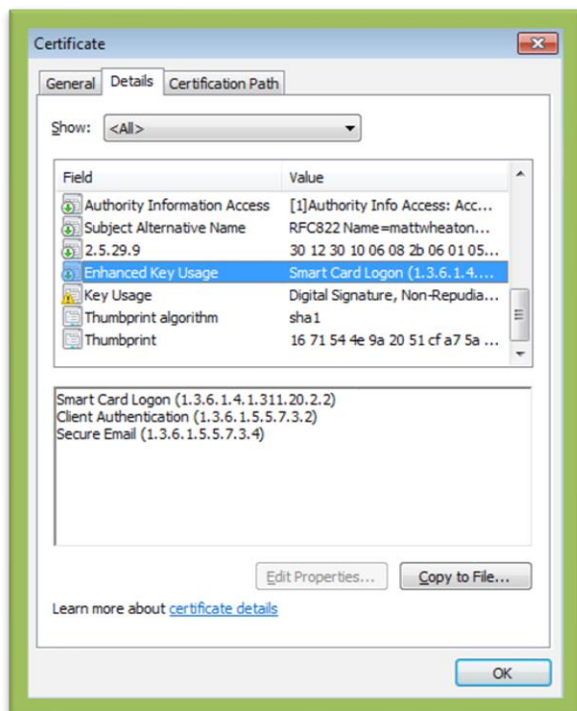
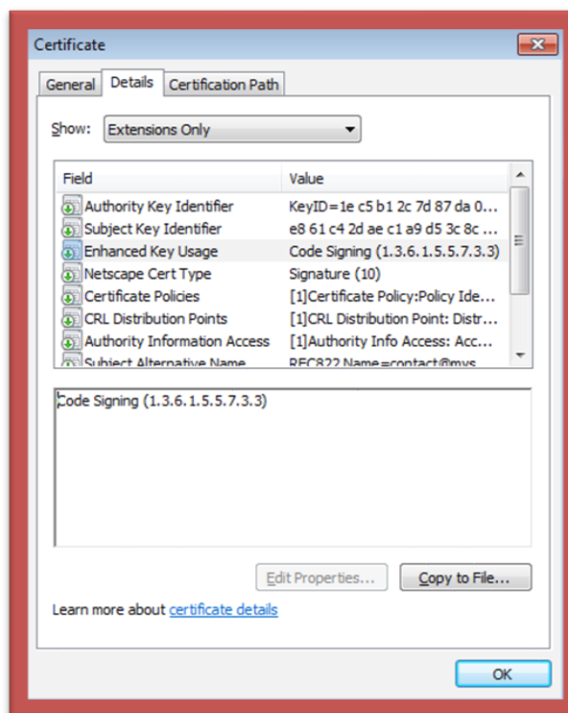
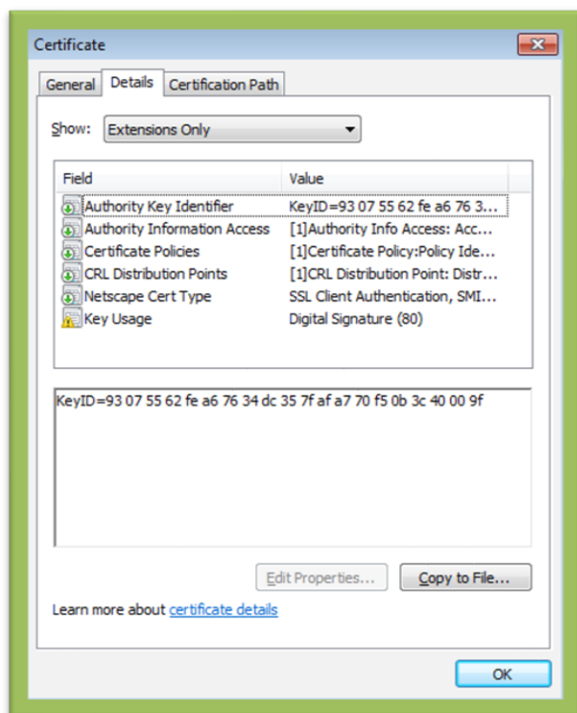
Extended Key Usage

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).





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

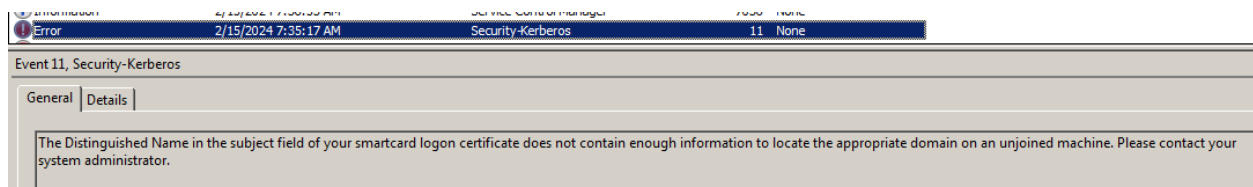
OR the certificate has been associated to more than one account.

OR there is an issue with the mapping which is not recognized.

OR there is an issue with KB5014754

Solution :

1) Check for Event logs in the SYSTEM related to Kerberos



If there is no event or “The Distinguished Name in the subject field of your smartcard logon certificate does not contain enough information to locate the appropriate domain on an unjoined machine. Please contact your system administrator.”, this could be the case.

That means that in general there is no mapping found with your certificate.

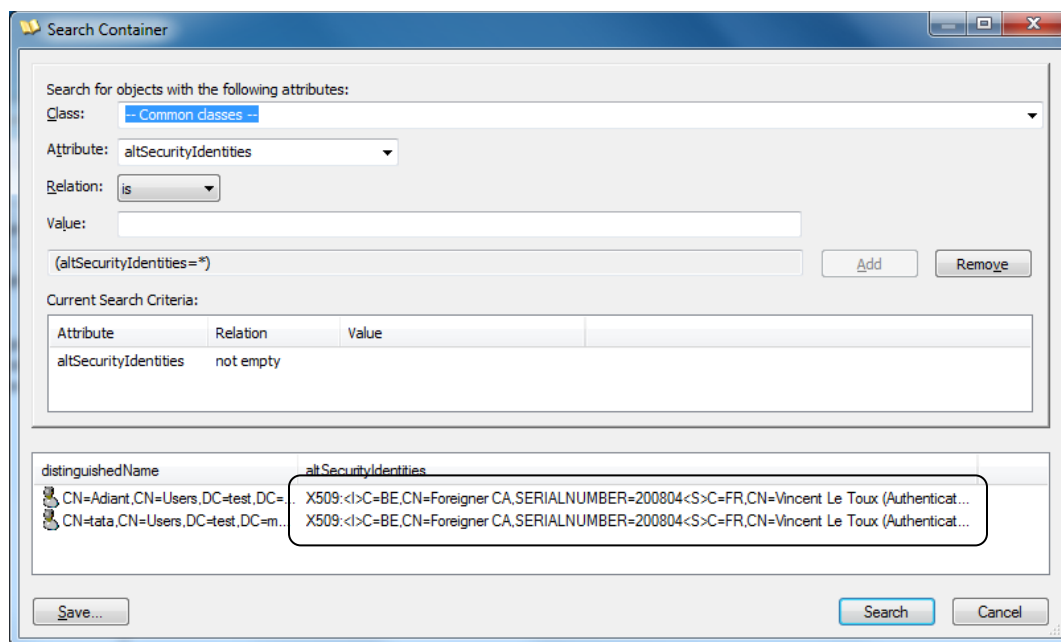
If you are using non usual mapping such as: X509:<I>xxx<S>xxx<SR>, this could be also a cause

Solution re-associate the certificate to the account using explicit or UPN mapping.

2) 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.



3) KB5014754—Certificate-based authentication changes on Windows domain controllers

There has been changed related to string mapping.

Look for event in the SYSTEM event folder.

Event Text The Key Distribution Center (KDC) encountered a user certificate that was valid but could not be mapped to a user in a strong way (such as via explicit mapping, key trust mapping, or a SID). Such certificates should either be replaced or mapped directly to the user through explicit mapping. See <https://go.microsoft.com/fwlink/?linkid=2189925> to learn more.

User: <principal name>

Certificate Subject: <Subject name in Certificate>

Certificate Issuer: <Issuer Fully Qualified Domain Name (FQDN)>

Certificate Serial Number: <Serial Number of Certificate>

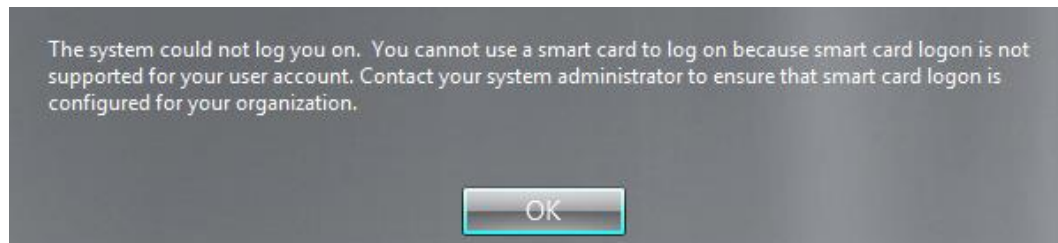
Certificate Thumbprint: <Thumbprint of Certificate>

If this is the case, edit the mapping.

Beware if you are using serial number mapping: the serial number bytes are written in reverse order.

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

Message :

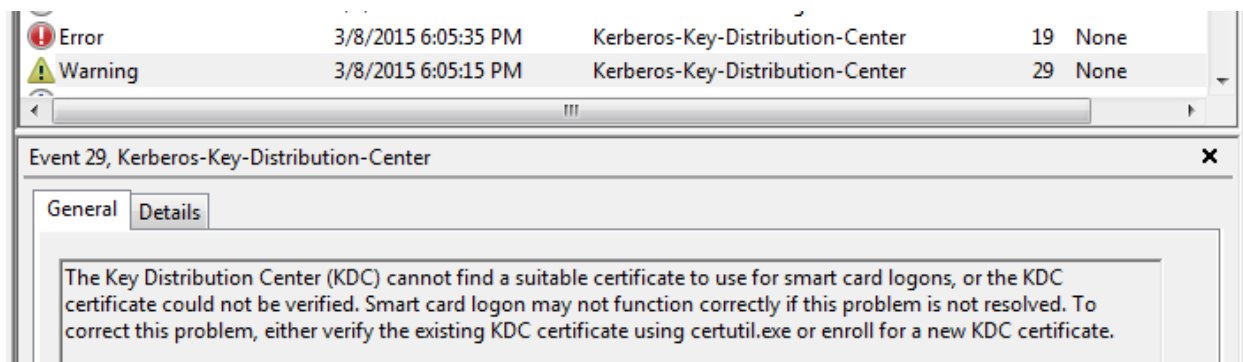


The system could not log you on. You cannot use a smart card to log on because smart card logon is not supported for your user account. Contact your system administrator to ensure that smart card logon is configured for your organization.

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 certutil.exe or enroll for a new KDC certificate."



Solution :

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

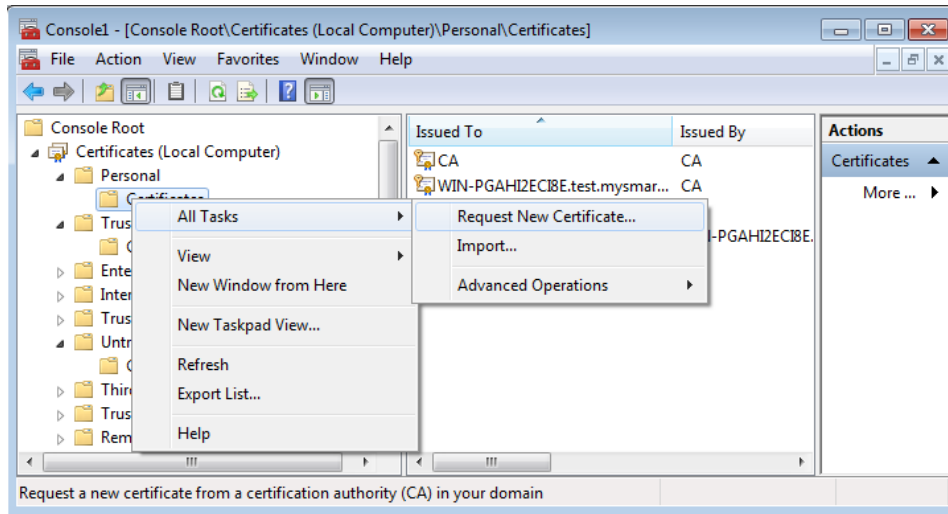
B) You can manually recreate the Domain Controller Authentication certificate.

On the domain controller, open mmc.

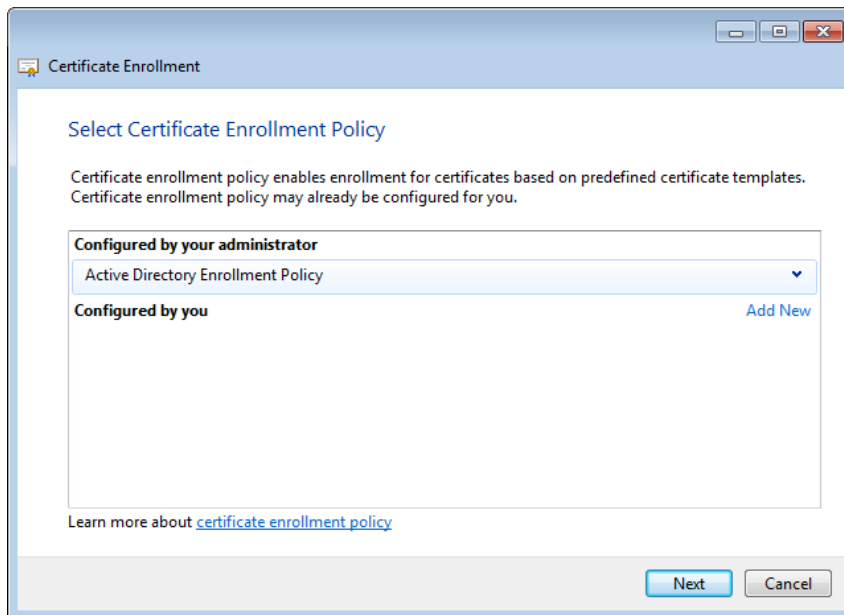
Click File, Click Add/Remove Snap-in.

Select Certificates, click Add, then select Computer account.

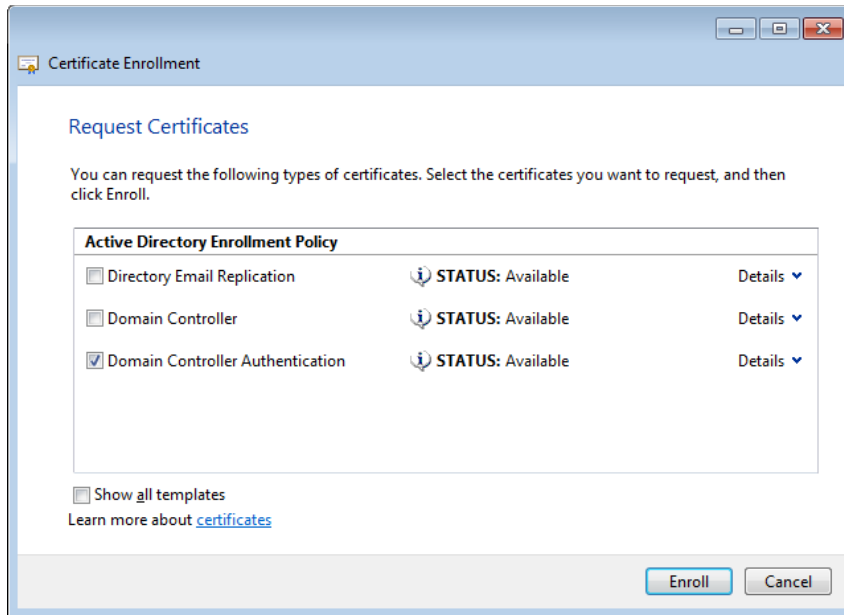
Expand Certificates (Local Computer), right-click Personal, click All Tasks, and then click Request New Certificate.



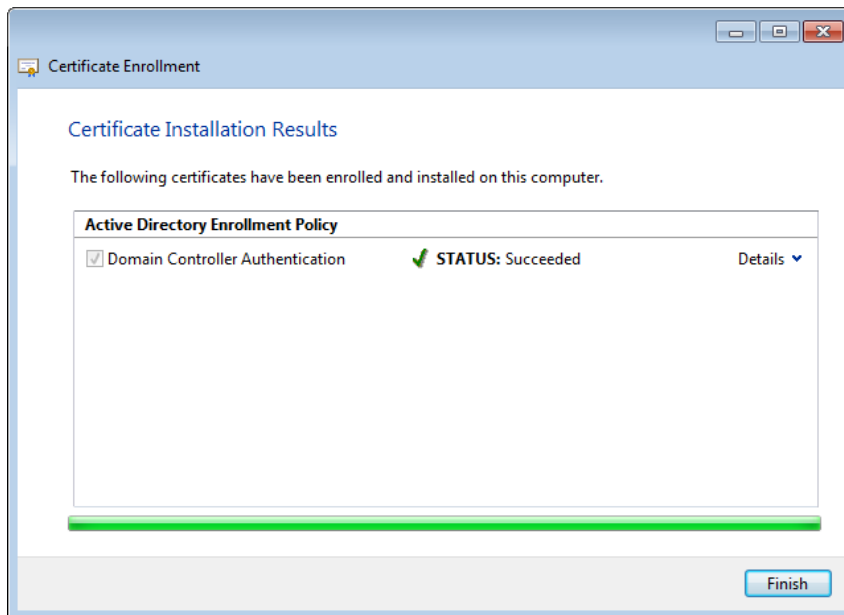
Press Next



Select « Domain Controller Authentication » and press Enroll.

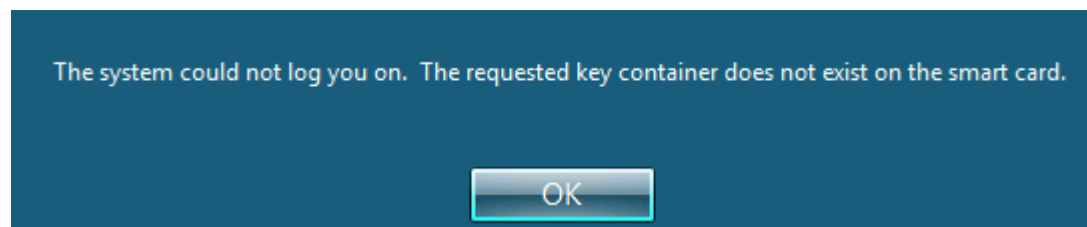


The certificate will be automatically enrolled.



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 :



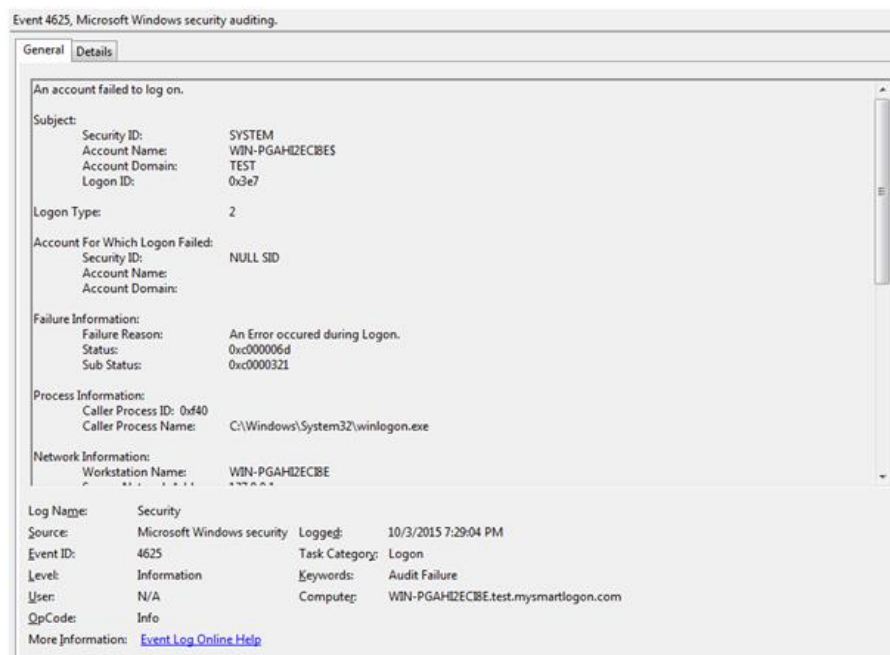
The system could not log you on. An error occurred trying to use this smart card. You can find further details in the event log. Please report this error to the system administrator.

Additional symptom:

Event 4625: An error occurred during Login.

Status: 0xc000006d (logon failure)

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



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 :

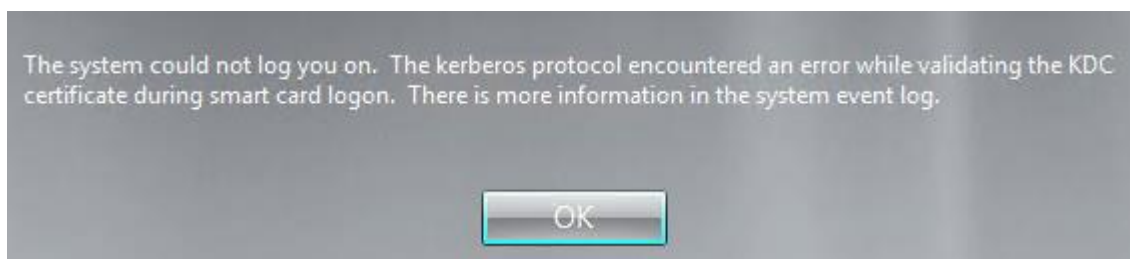
Contact your smart card manufacturer. To get more detail about the problem, you can run api monitor and attach to lsass.exe. You'll be able to report unusual error.

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

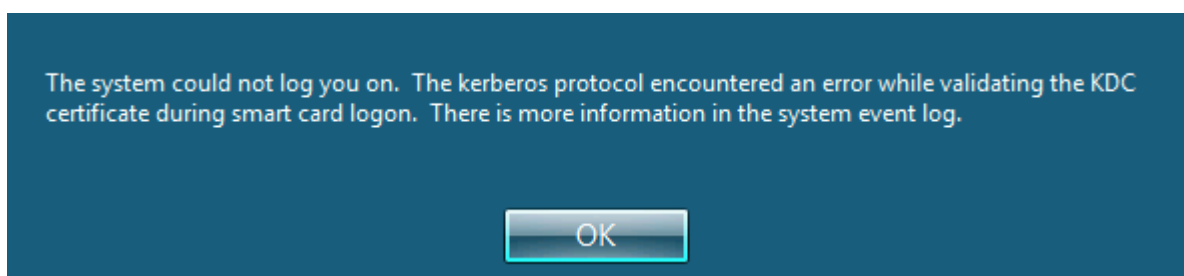
kerberos.DLL	NCryptOpenStorageProvider (0x00000000159d03c0, "OpenSC CSP", 0)	NTE_FAIL	0x80090020 = An internal error...
ncrypt.dll	BCryptResolveProviders (NULL, NCryptKeyStorageInterface, "KEY_STORAGE", "OpenSC CSP", CRYPT_UM, 0, 0x000000000565d930, 0x000...	STATUS_NOT_FOUND	0xc0000225 = The object was n...

The kerberos protocol encountered an error while validating the KDC certificate during smart card logon.

Message :



On terminal server:



The system could not log you on. The kerberos protocol encountered an error while validating the KDC certificate during smart card logon. There is more information in the system event log..

Additional symptom:

Event 9: Security-Kerberos.

(A certificate chain could not be built to a trusted root authority.)

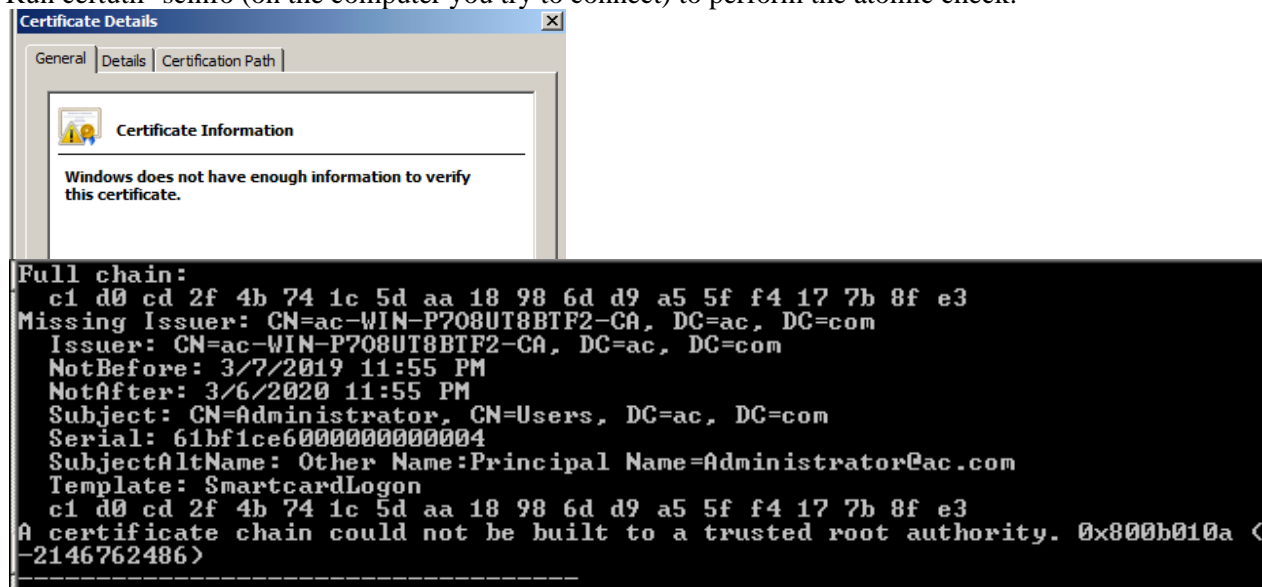


Cause :

The certificate chain couldn't be built.

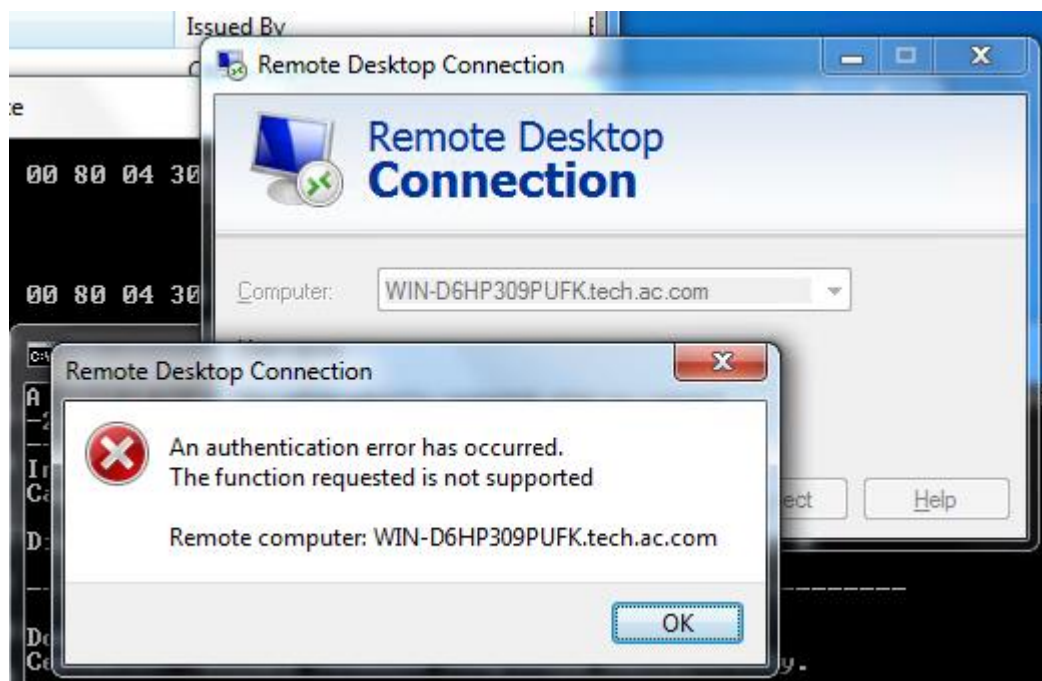
Solution :

Run certutil -scinfo (on the computer you try to connect) to perform the atomic check:



Run it on a computer where it is working. Then copy the root certificate on the client computer on the computer certificate store (mmc -> certificate -> local computer and not certmgr.msc). Run gpupdate /force.

The function requested is not supported



System Number of events: 15,560				
Level	Date and Time	Source	Event ID	Task Category
Information	3/8/2019 10:42:53 AM	Service Control Mana...	7036	None
Information	3/8/2019 10:40:19 AM	Service Control Mana...	7036	None
Error	3/8/2019 10:40:12 AM	LSA (LsaSrv)	6041	None
Warning	3/8/2019 10:39:02 AM	DNS Client Events	1014	None

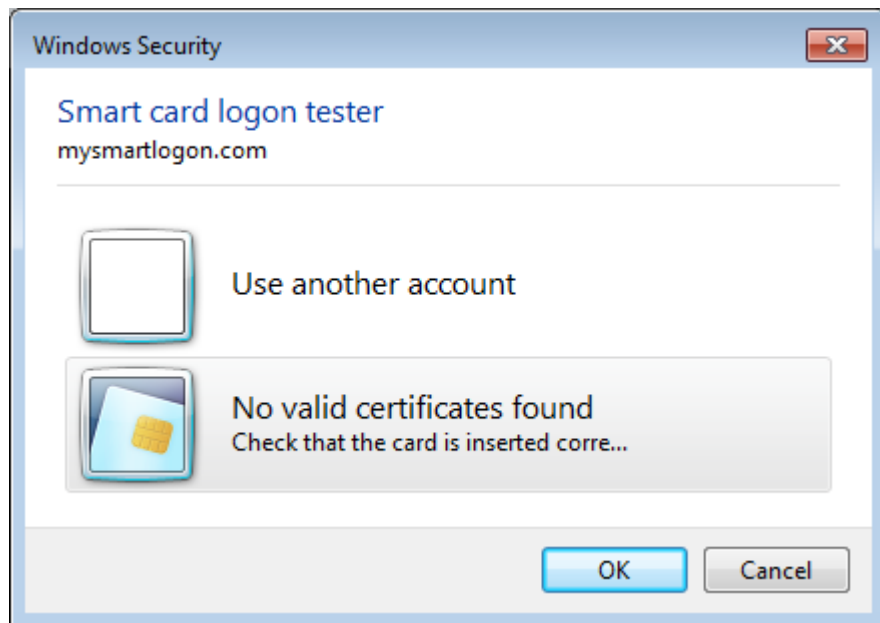
Event 6041, LSA (LsaSrv)	
General	Details
<p>A CredSSP authentication to TERMSRV/WIN-D6HP309PUFK.tech.ac.com failed to negotiate a common protocol version. The remote host offered version 2 which is not permitted by Encryption Oracle Remediation.</p> <p>See https://go.microsoft.com/fwlink/?linkid=866660 for more information.</p>	

see <https://support.microsoft.com/fr-fr/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018>

No valid certificates found

Message :

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



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.

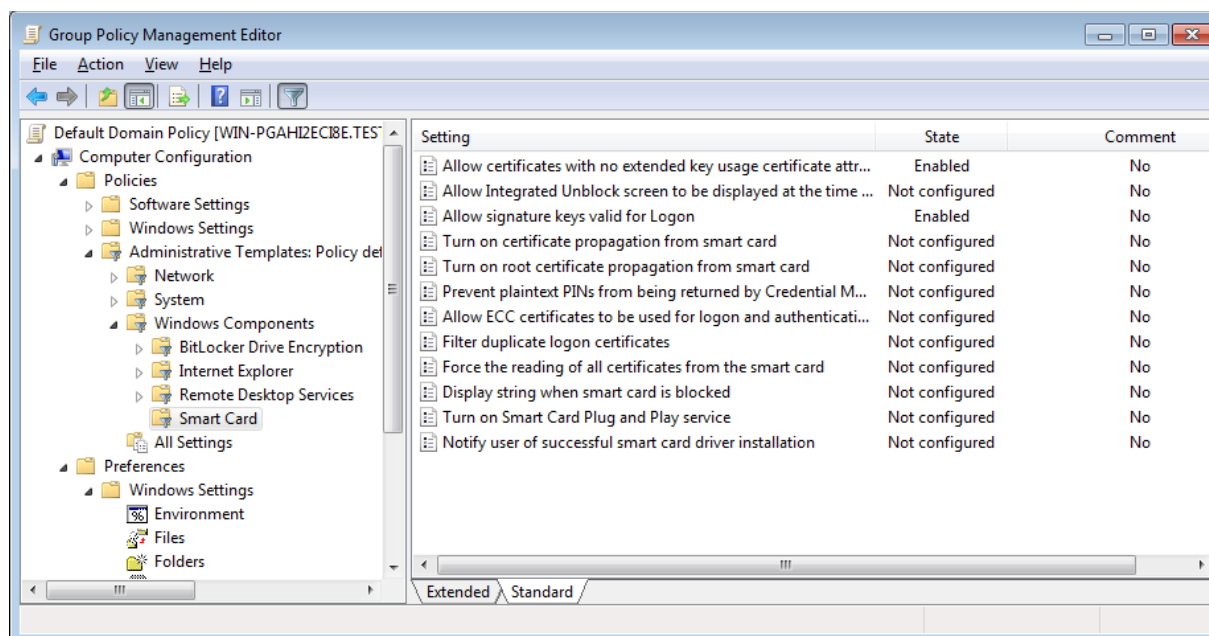
For example, you are trying to access a server using terminal server from a client computer which does not belong to the current domain.

OR

The certificate chain is not trusted.

Solutions

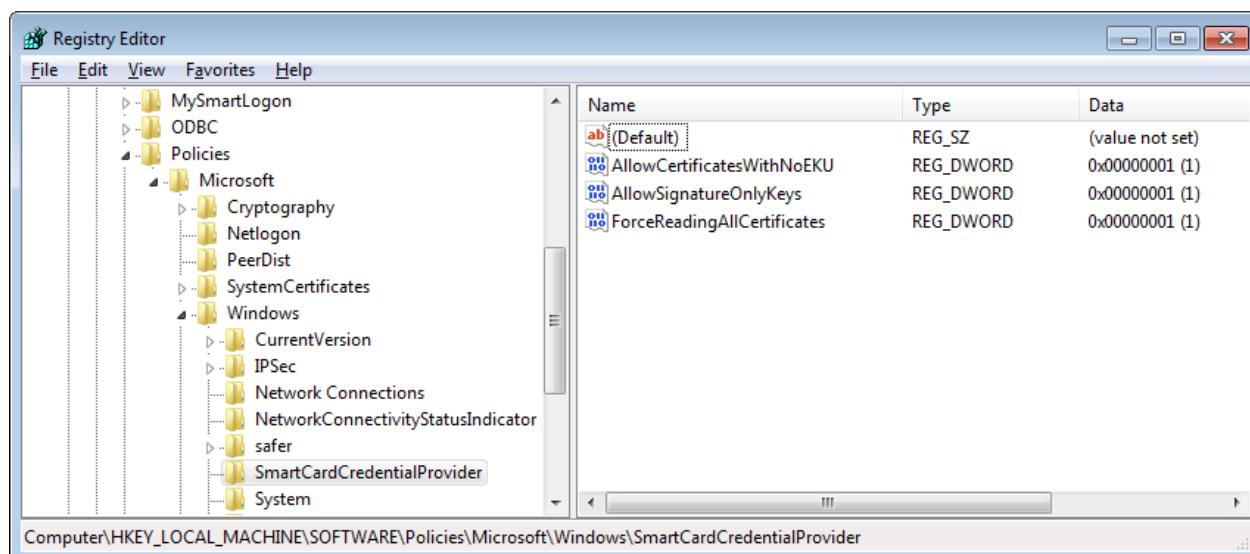
If the UPN mapping is the only mapping authorized, you can remove all the client restriction by setting all the possible GPOs.



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 :

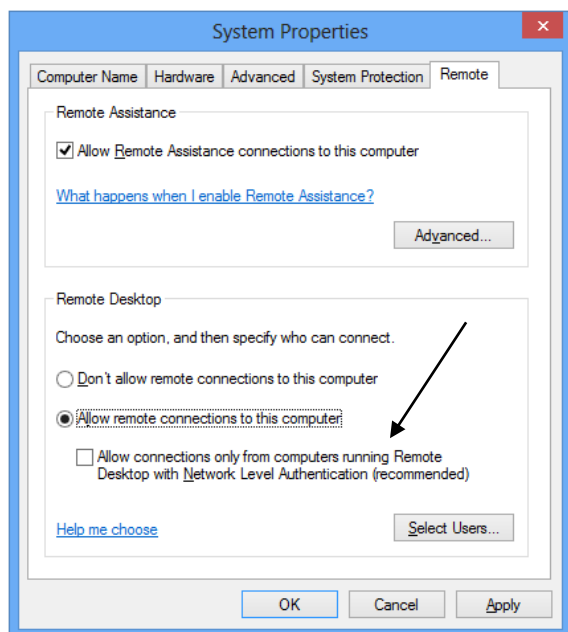
```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider]
"AllowCertificatesWithNoEKU"=dword:00000001
"AllowSignatureOnlyKeys"=dword:00000001
"ForceReadingAllCertificates"=dword:00000001
```

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.

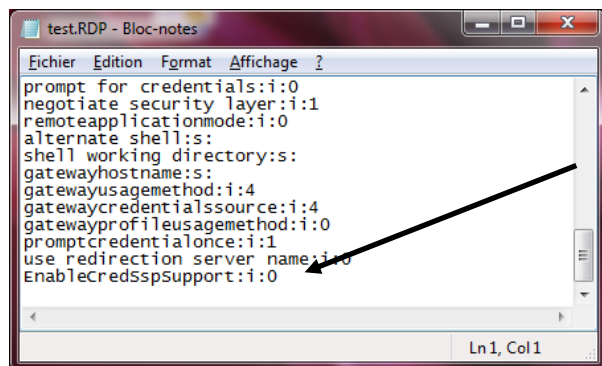
Otherwise, be sure that the root certificate and the intermediates certificates are registered in the user certificate store. This store can be accessed using `certmgr.msc`.

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)".



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**



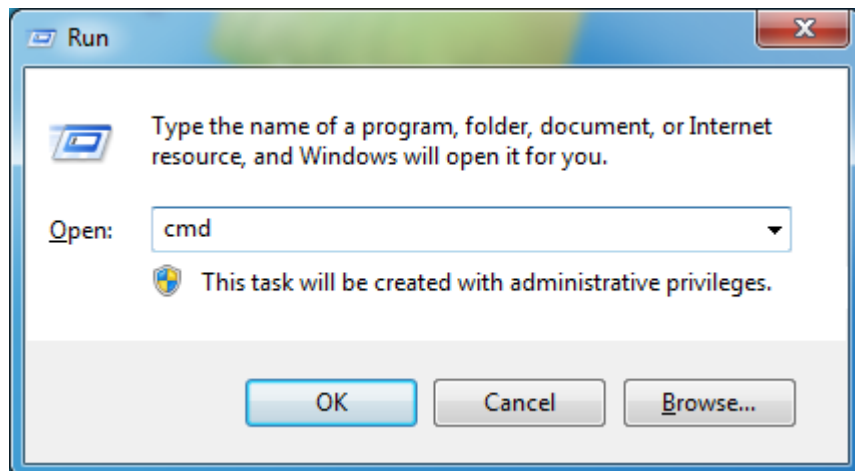
Checking for a healthy smart card

Using certutil

Certutil is a troubleshooting tool provided by Microsoft.

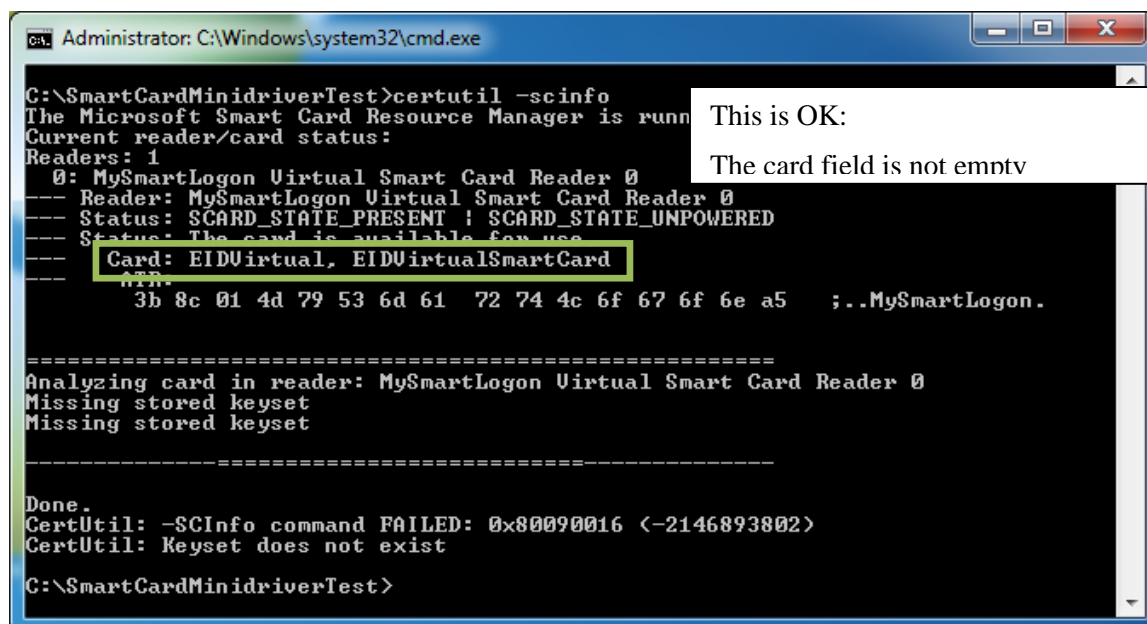
Note : certutil.exe is installed by default starting Windows Vista and Windows 2008. Certutil can be installed on Windows XP by the package "WindowsServer2003-KB304718-AdministrationToolsPack"

You can run certutil by typing Windows +R



Then "cmd" then "certutil -scinfo"

Expected diagnostic of a healthy smart card

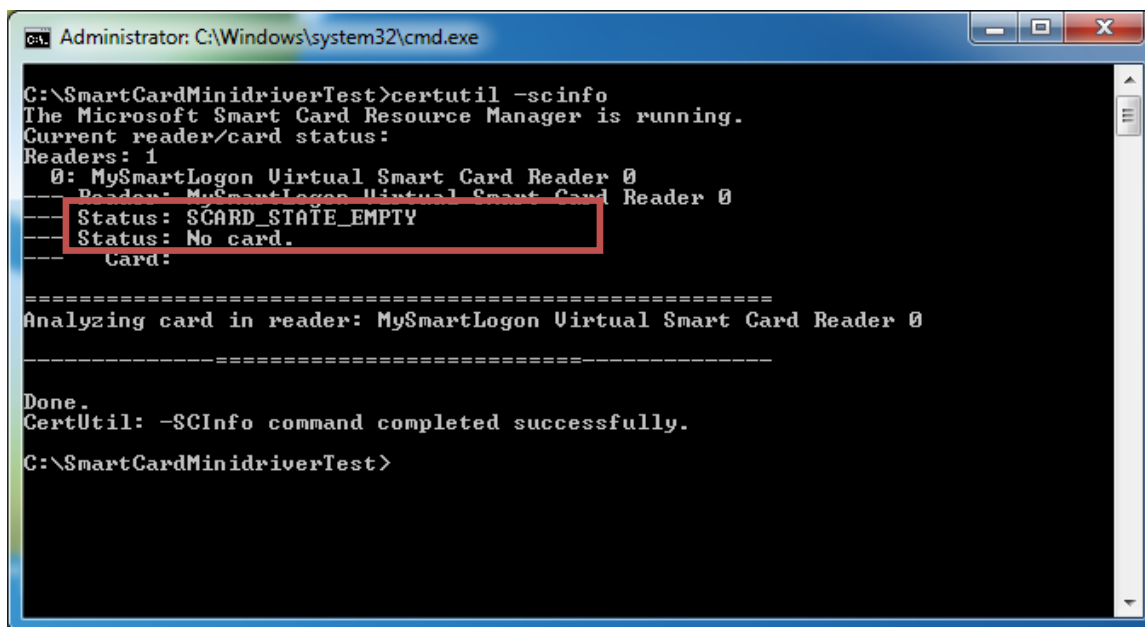


The previous screenshot shows an empty smart card, without any certificate or private key stored (the KeySet does not exist)

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

Smart card absent

An empty smart card reader will produce the following output :



```
Administrator: C:\Windows\system32\cmd.exe

C:\SmartCardMinidriverTest>certutil -scinfo
The Microsoft Smart Card Resource Manager is running.
Current reader/card status:
Readers: 1
  0: MySmartLogon Virtual Smart Card Reader 0
-----
  Reader: MySmartLogon Virtual Smart Card Reader 0
  Status: SCARD_STATE_EMPTY
  Status: No card.
  Card:

=====
Analyzing card in reader: MySmartLogon Virtual Smart Card Reader 0
-----

Done.
CertUtil: -SCInfo command completed successfully.
C:\SmartCardMinidriverTest>
```

(Look at the mention “SCARD_STATE_EMPTY”)

Causes :

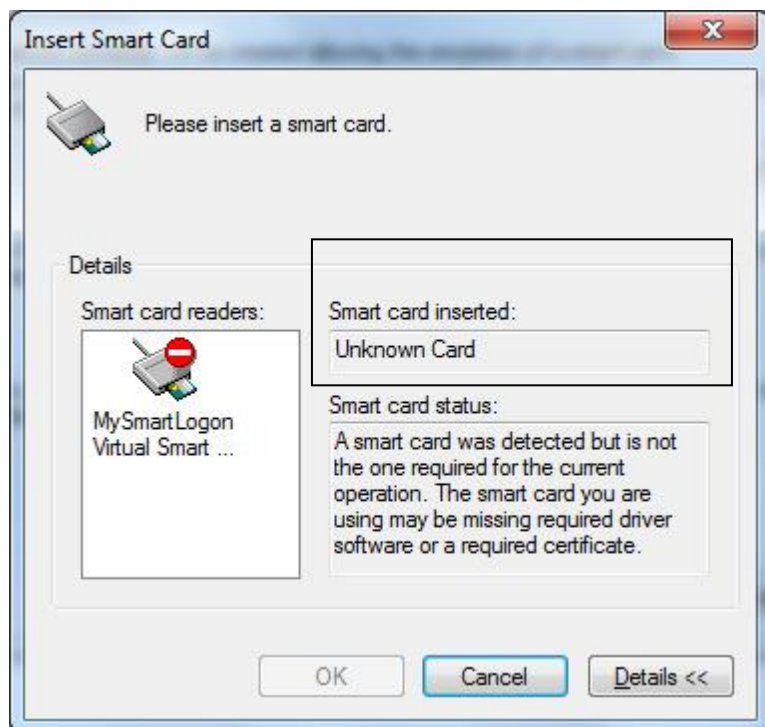
- An incompatible smart card has been connected
- The smart card reader doesn't recognize the smart card

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 :



```

C:\Windows\system32\cmd.exe
Current reader/card status:
Readers: 1
  0: MySmartLogon Virtual Smart Card Reader 0
  --- Reader: MySmartLogon Virtual Smart Card Reader 0
  --- Status: SCARD_STATE_PRESENT
  --- Status: The card is available for use
  --- Card:
  --- ATR:
    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 0
SCardGetCardTypeProviderName: The system cannot find the file specified. 0x2 (WI
N32: 2)
Cannot retrieve Provider Name for SCardGetCardTypeProviderName: The system canno
t find the file specified. 0x2 (WIN32: 0)
Cannot retrieve Provider Name for <null>

=====
Done.
CertUtil: -SCInfo command FAILED: 0x2 (WIN32: 2)
CertUtil: The system cannot find the file specified.

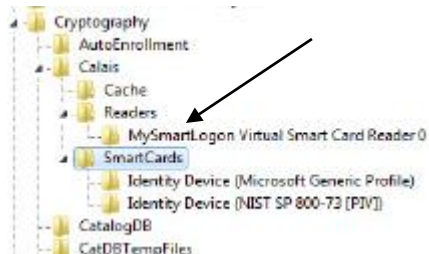
C:\Users\Rudolf LEYBAERT>

```

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.



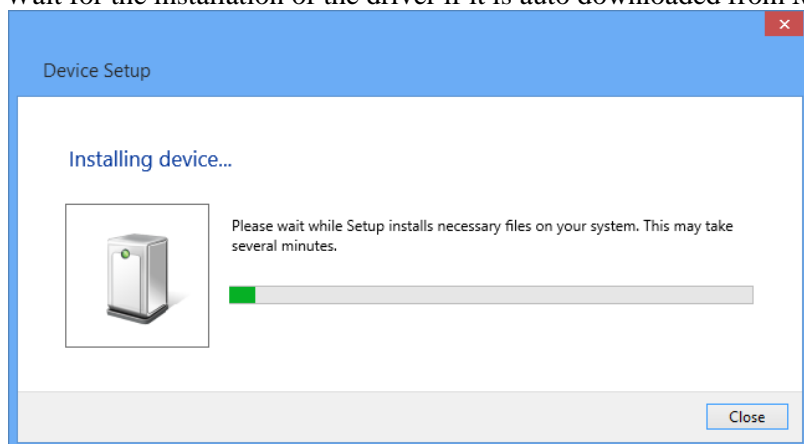
Note : on 64 bits systems there are two CALAIS database : the 64 bits one and the other in *WOW6432Node*.

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, ...)

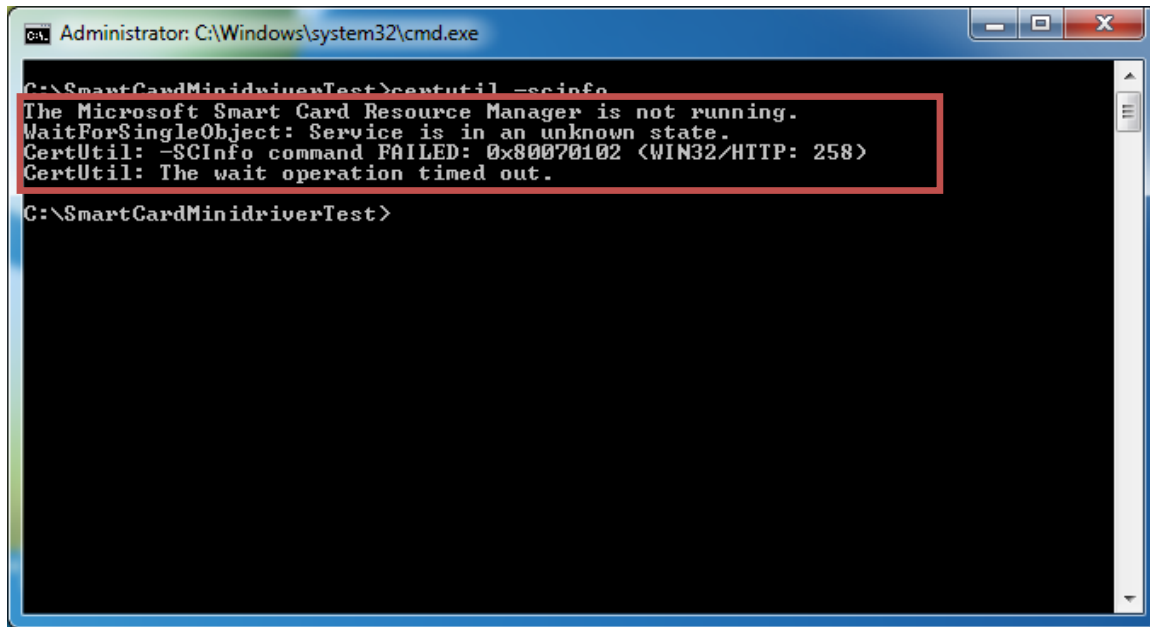
Solutions :

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.



The smart card resource manager is not running

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



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command prompt is at the directory "C:\SmartCardMinidriverTest". The user has entered the command "certutil -scinfo". The output of the command is displayed in a red box, indicating an error: "The Microsoft Smart Card Resource Manager is not running. WaitForSingleObject: Service is in an unknown state. CertUtil: -SCInfo command FAILED: 0x80070102 (WIN32/HTTP: 258) CertUtil: The wait operation timed out." The prompt then returns to "C:\SmartCardMinidriverTest>".

```
Administrator: C:\Windows\system32\cmd.exe
C:\SmartCardMinidriverTest>certutil -scinfo
The Microsoft Smart Card Resource Manager is not running.
WaitForSingleObject: Service is in an unknown state.
CertUtil: -SCInfo command FAILED: 0x80070102 (WIN32/HTTP: 258)
CertUtil: The wait operation timed out.
C:\SmartCardMinidriverTest>
```

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

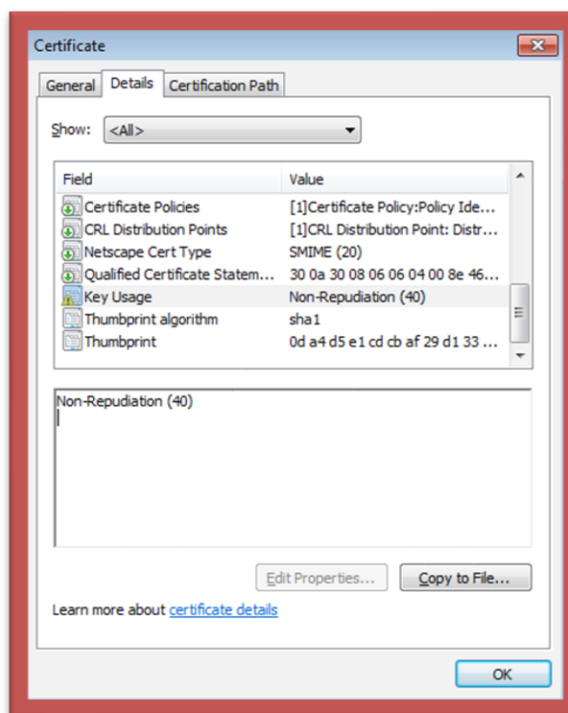
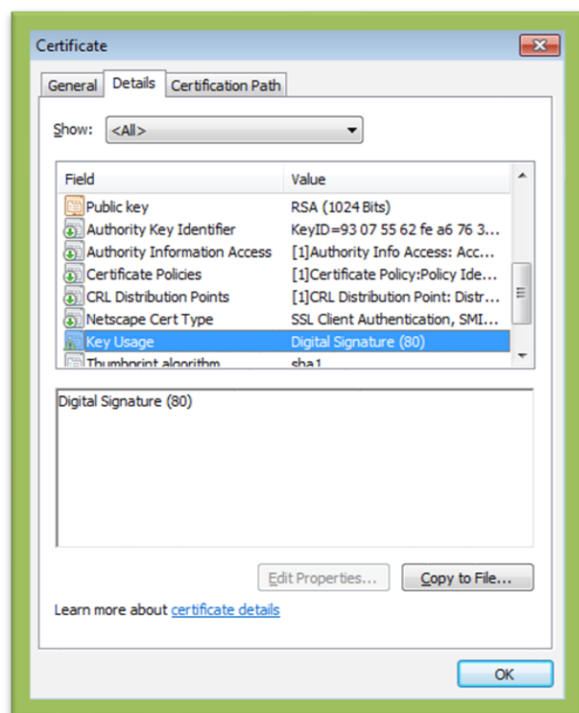
Open the properties of the certificate and search for the property "Key Usage".

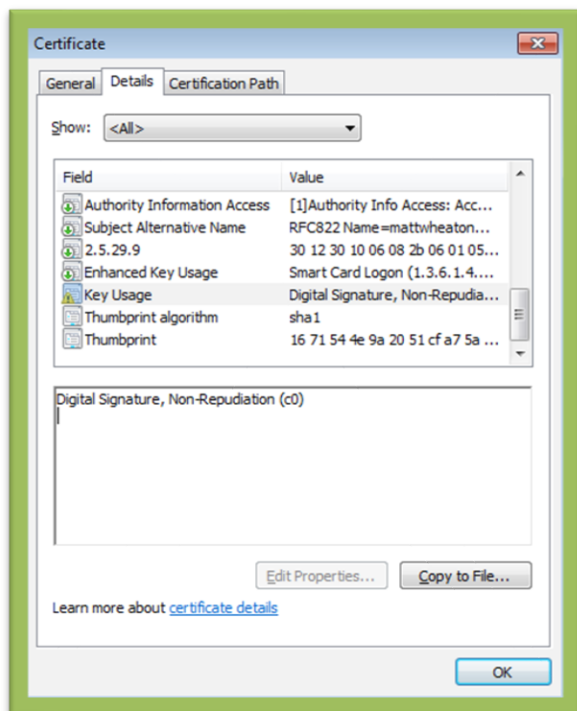
This property should contain one of the following :

- 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.





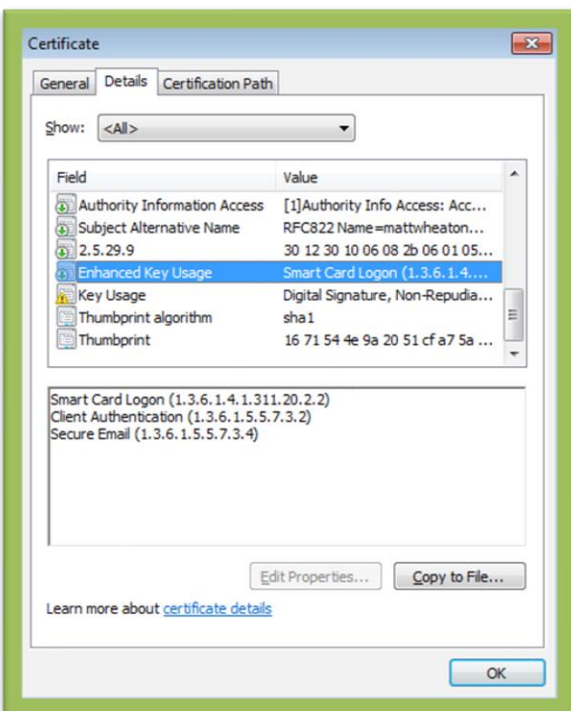
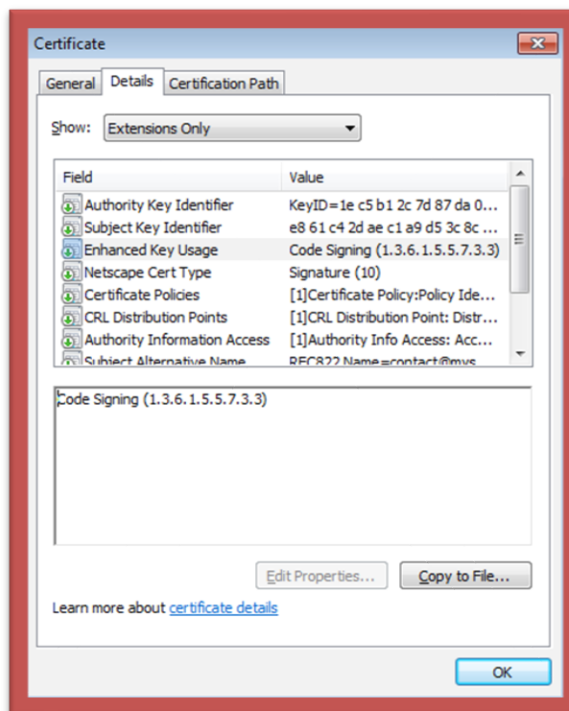
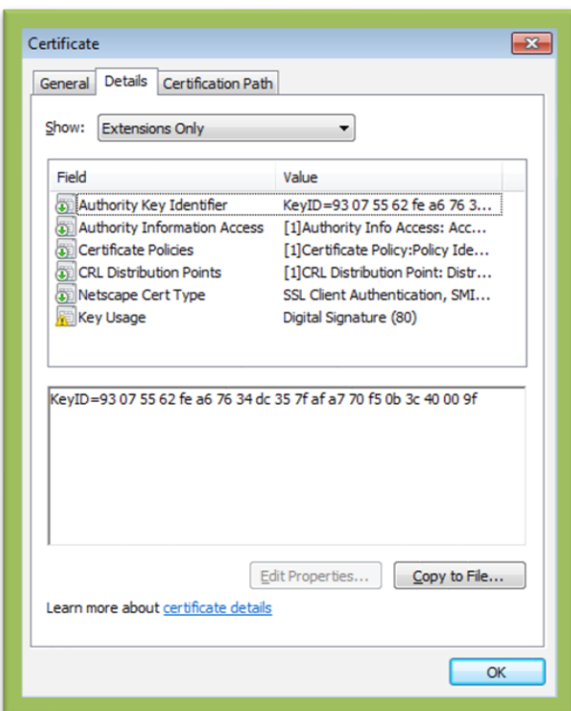
Extended Key Usage

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).

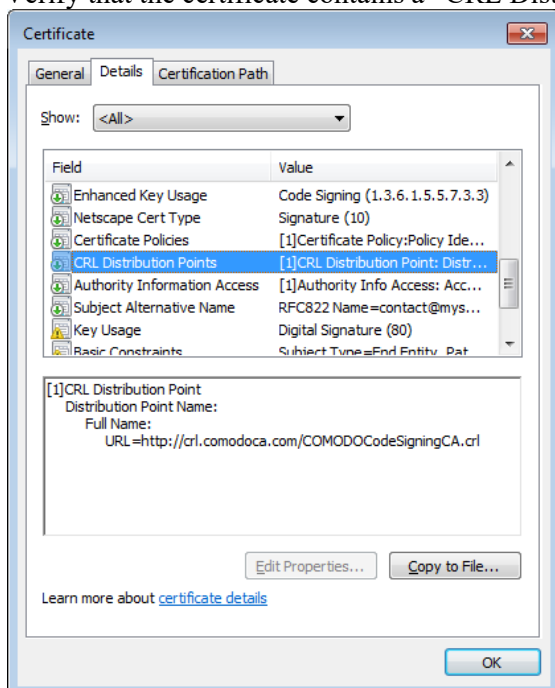


CRL Troubleshooting

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



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 below 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 :



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.

```

Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
----- Certificate AIA -----
No URLs "None" Time: 0
----- Certificate CDP -----
Failed "CDP" Time: 0
Error retrieving URL: This network connection does not exist. 0x800708ca <WIN32: 2250>
http://crl.usertrust.com/AddTrustExternalCARoot.crl
----- Base CRL CDP -----
No URLs "None" Time: 0
----- Certificate OCSP -----
Failed "OCSP" Time: 0
Error retrieving URL: This network connection does not exist. 0x800708ca <WIN32: 2250>
http://ocsp.usertrust.com

```

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.

```

Element.dwErrorStatus = CERT_TRUST_IS_NOT_TIME_VALID (0x1)
----- Certificate AIA -----
Failed "AIA" Time: 0
Error retrieving URL: The operation timed out 0x80072ee2 <WIN32: 12002>
http://crt.comodoca.com/COMODOCodeSigningCA.crt
----- Certificate CDP -----
Failed "CDP" Time: 0
Error retrieving URL: The operation timed out 0x80072ee2 <WIN32: 12002>
http://crl.comodoca.com/COMODOCodeSigningCA.crl
----- Base CRL CDP -----
No URLs "None" Time: 0
----- Certificate OCSP -----
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.

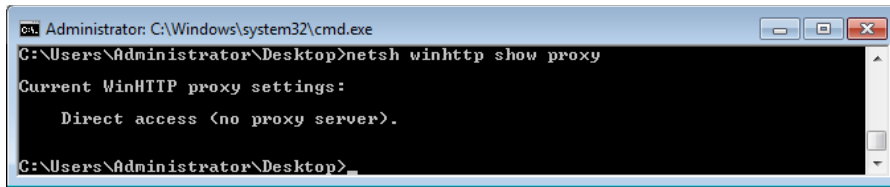
Other error messages are related to network or proxy configuration problem.

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



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator\Desktop>netsh winhttp show proxy
Current WinHTTP proxy settings:
    Direct access (no proxy server).
C:\Users\Administrator\Desktop>
```

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

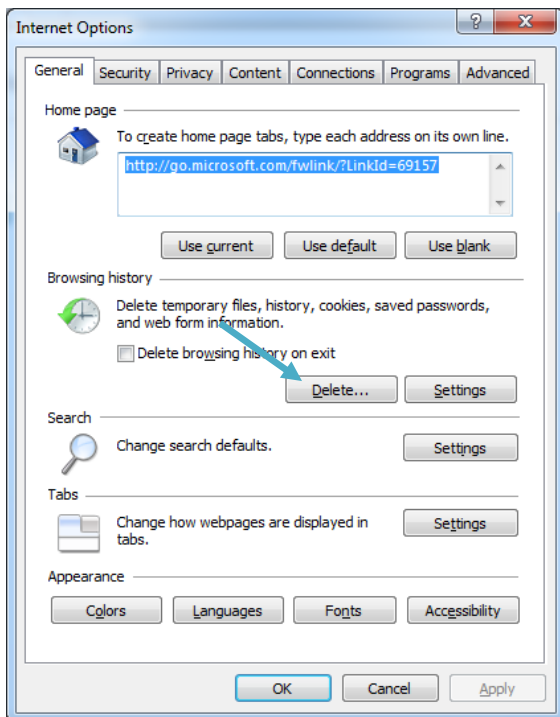
netsh winhttp reset proxy to delete proxy setting and access **HTTP** directly

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.



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 [psexec.exe](#) 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.

```
Administrator: C:\Windows\System32\cmd.exe
C:\Users\Adiant\Desktop>psexec -s certutil -urlcache
PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

res://energy.dll/IDR_XML_DEFAULT_TRANSFORM.XSL
WinINet Cache entries: 1
http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/au
throotst1.cab
http://crl.usertrust.com/UTN-USERFirst-Object.crl
http://ocsp.comodoca.com/MF1wUDBOMeUwSjAJBgUrDgMCGGUABBSOJaE2H4hHYQzP74h1Lu041NG
z2BEAQUhsWxLH2H2gJofCW8DAeEP7bP3vECEQDHDTOODIocD0Pw0Phz9JyL
WinHttp Cache entries: 3
CertUtil: -URLCache command completed successfully.
certutil exited on WIN-1MLHM2RAF4U with error code 0.
C:\Users\Adiant\Desktop>
```

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 OCSP caching can be found in the article [Troubleshooting PKI problems on Windows Vista](#)

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:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001
"CRLTimeoutPeriod"=dword:00000001
```

On the client computer apply:

```
Windows Registry Editor Version 5.00

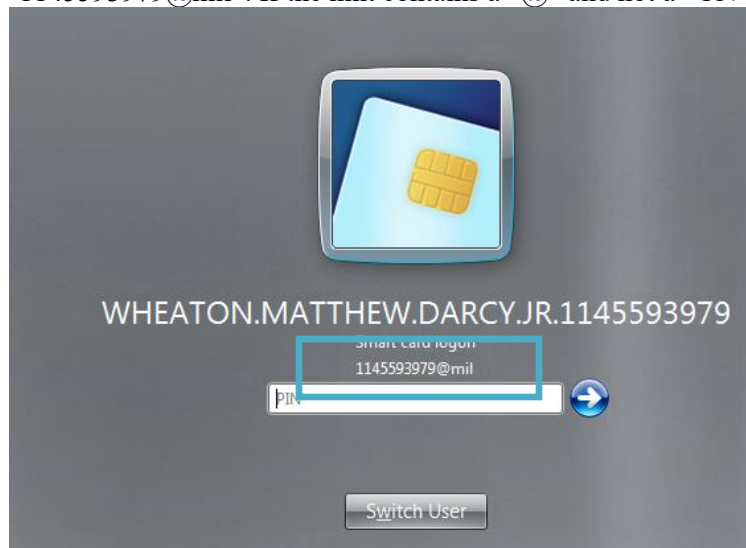
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001
"CRLTimeoutPeriod"=dword:00000001
```

Verifying the certificate mapping

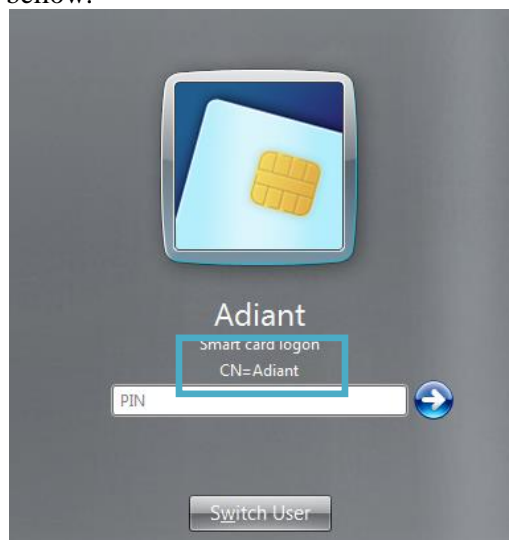
Determine the type of mapping

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.

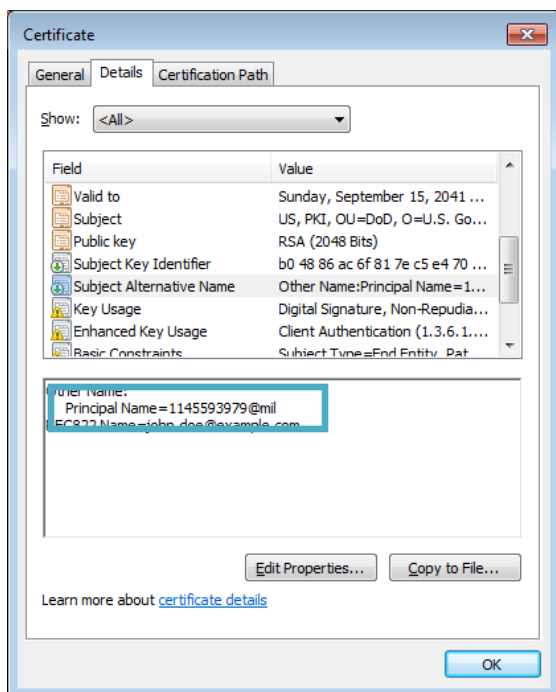


If the string contains a “CN=” or in general a “=”, it is an explicit mapping like showed in the example bellow.

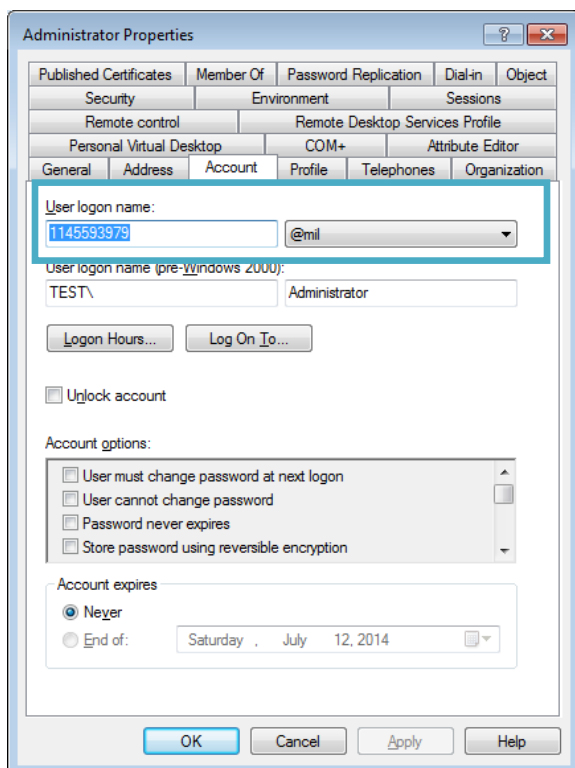


Map a certificate to a user account using UPN mapping

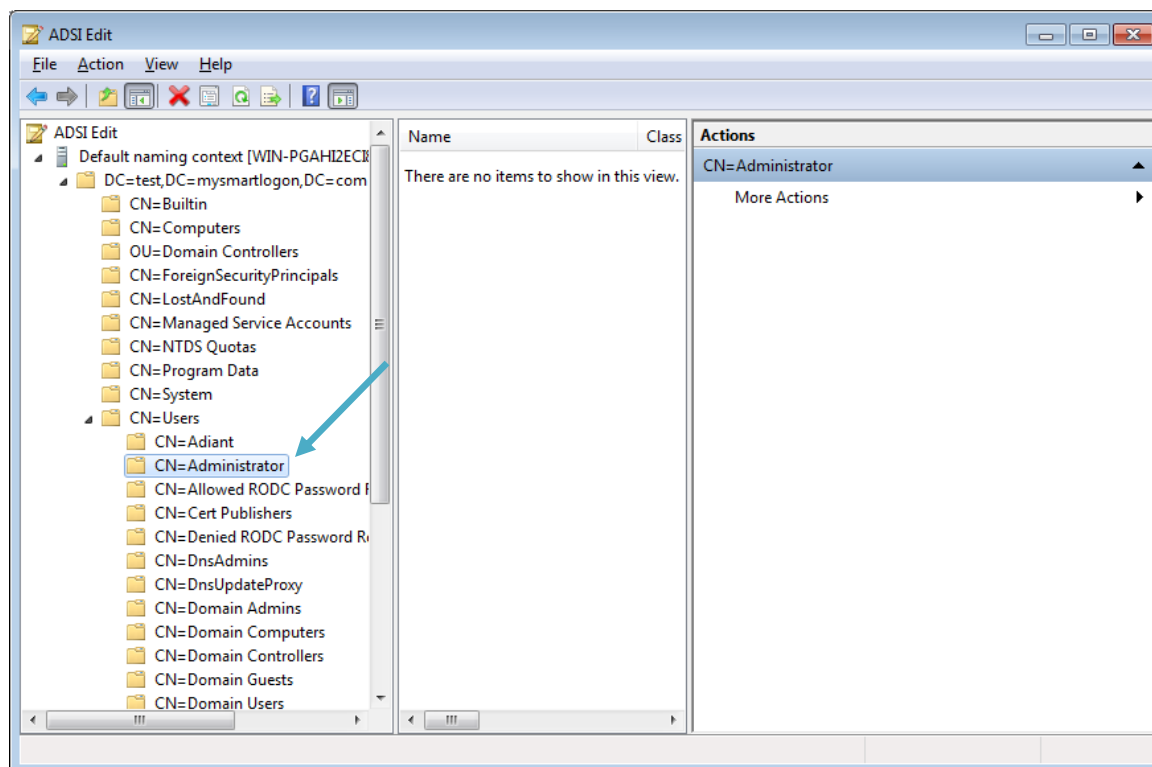
Open the certificate properties and the Details tab. Look for "Subject Alternative Name". At the bottom of the screen, search for "Principal Name". In this case, 1145593979@mil. There can be other definitions like RFC822 Name.



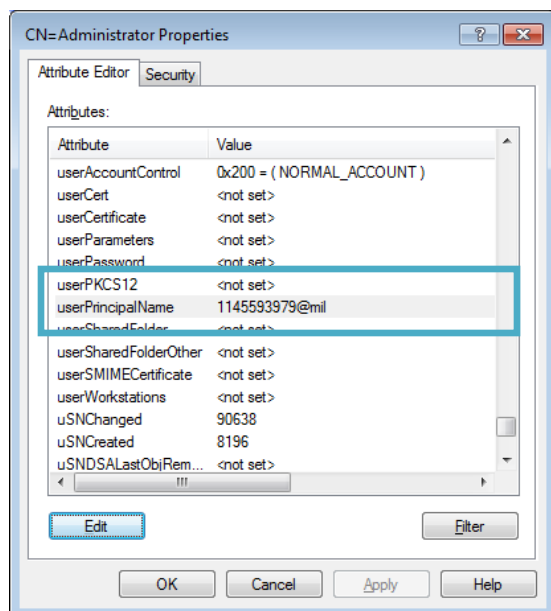
Open the properties of the user, and check that the User logon name matches the string returned previously.



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



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

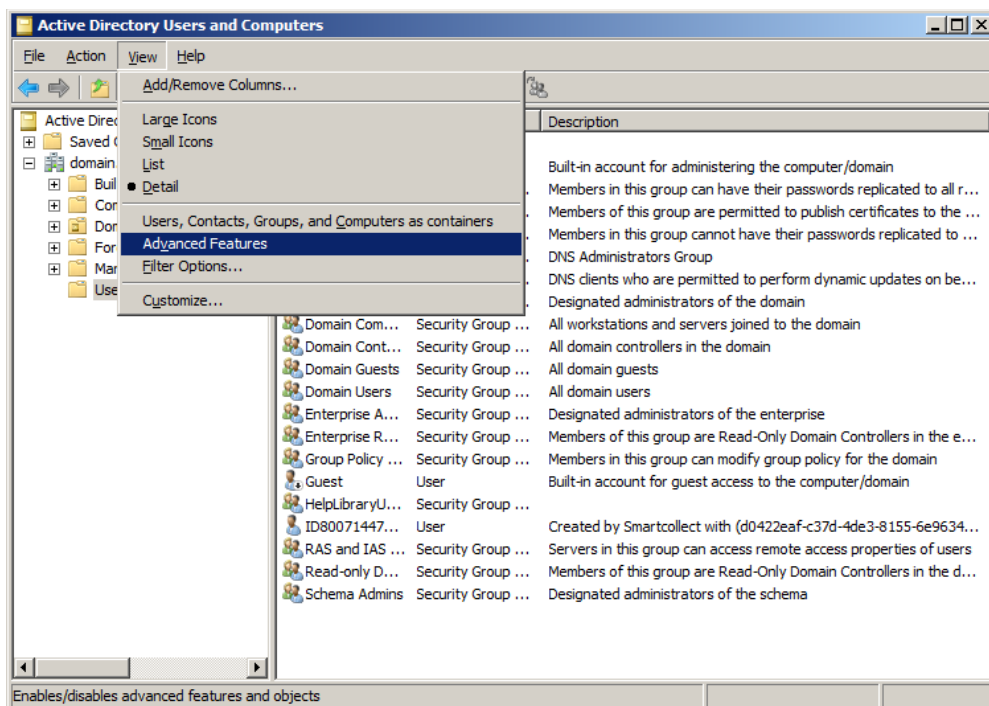


Map a certificate to a user account using Explicit mapping

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

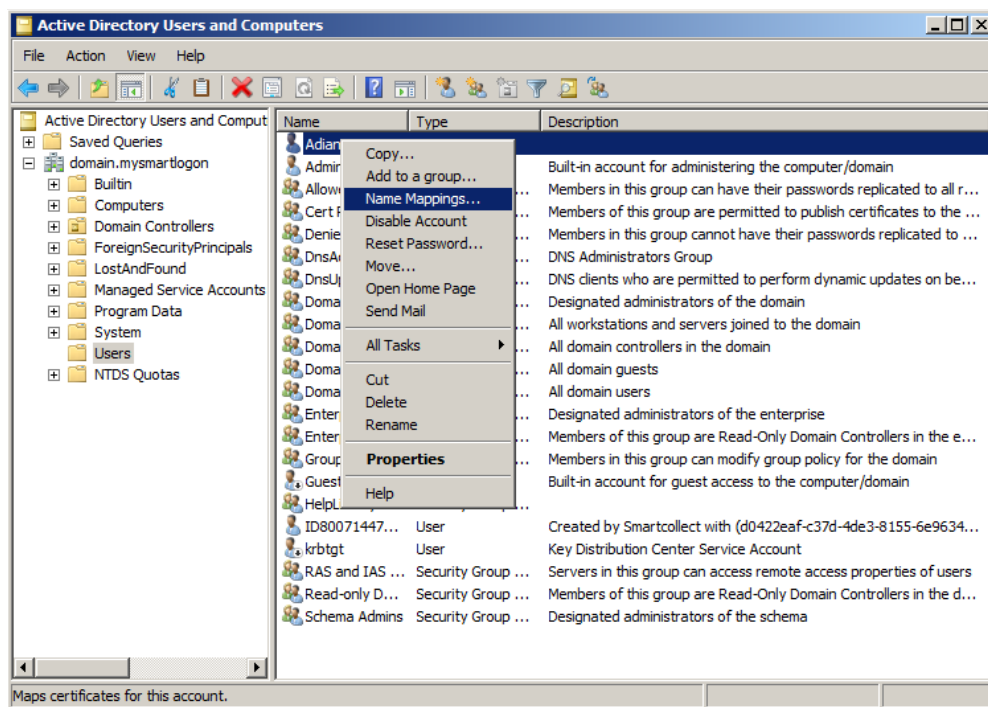
Open the console "Active Directory Users and Computers"

Select View -> Advanced features

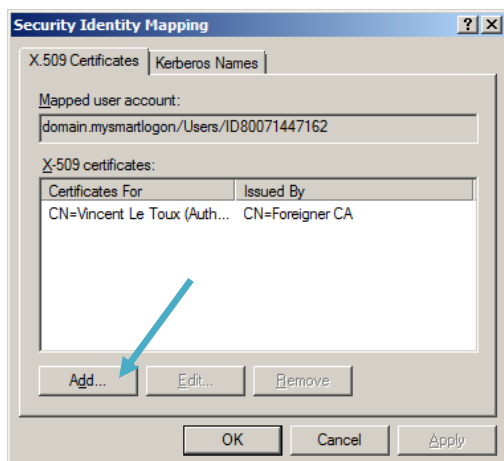


Select the account you want to map a smart card certificate to, then right click "Name mappings".

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



Select the smart card certificate previously exported and validate.



Here are the mapping which are available:

Mapping	Example	Type	Remarks
X509IssuerSubject	"X509:<I>IssuerName<S>SubjectName"	Weak	
X509SubjectOnly	"X509:<S>SubjectName"	Weak	
X509RFC822	"X509:<RFC822>user@contoso.com"	Weak	Email Address
X509IssuerSerialNumber	"X509:<I>IssuerName<SR>1234567890"	Strong	Recommended
X509SKI	"X509:<SKI>123456789abcdef"	Strong	
X509SHA1PublicKey	"X509:<SHA1-PUKEY>123456789abcdef"	Strong	

Note: beware that serial number are written in reverse byte order.

You can see the full algorithm here:

<https://learn.microsoft.com/fr-fr/archive/blogs/spatdsg/howto-map-a-user-to-a-certificate-via-all-the-methods-available-in-the-altsecurityidentities-attribute>

Beware that if you try to combine different kind of mapping (ex: X509:<I>xxx<S>xxx<SR>) the mapping will silently fail (because <SR>xxx will be considered as part of the subject of the certificate)

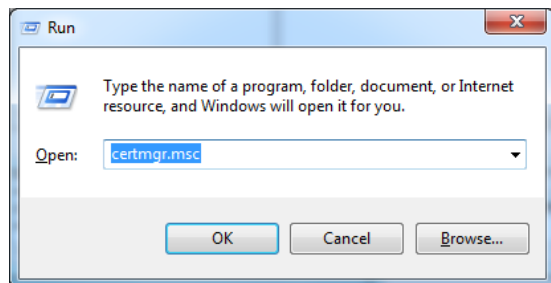
Annex 1 – Procedures

Get the certificate chain

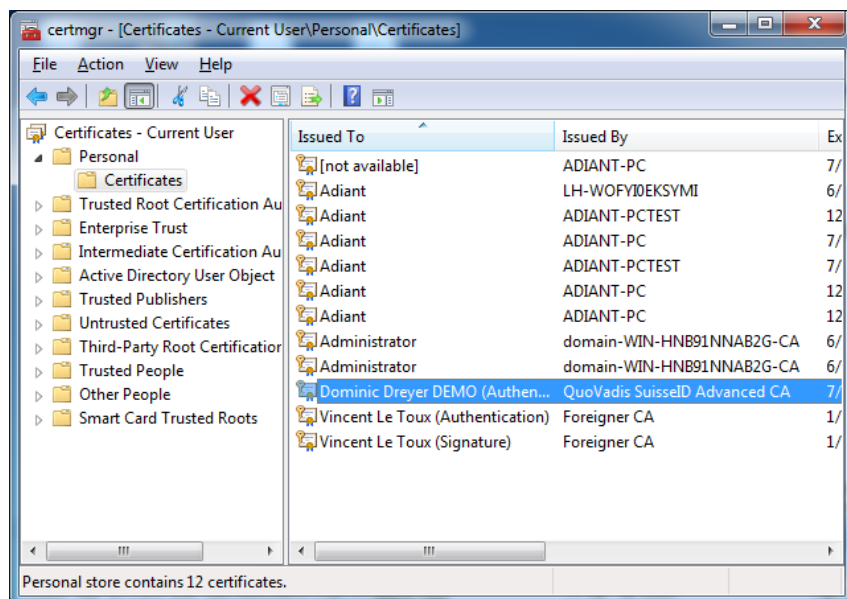
Smart Policy retrieves automatically the certificate chain on the local computer. The certificate **MUST** be trusted.

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.

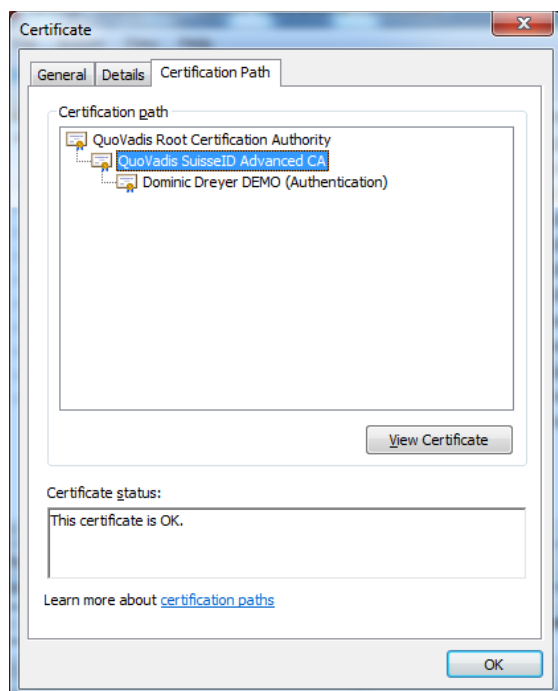


Locate the certificate you want to export its chain



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.

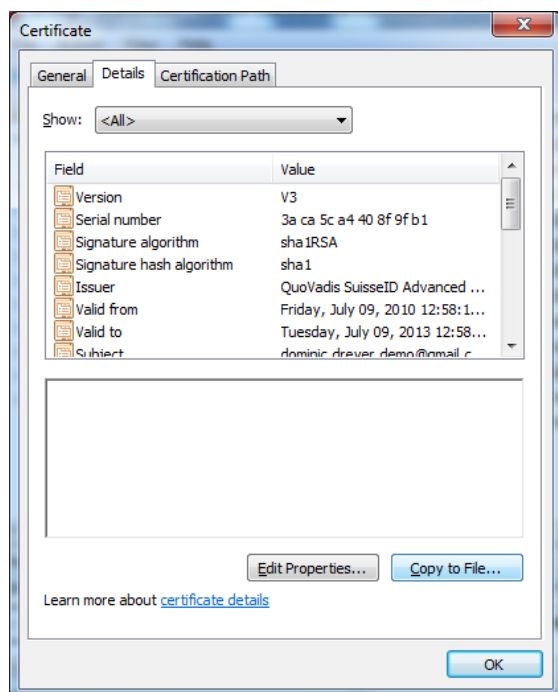


You will then export each certificate of this chain.

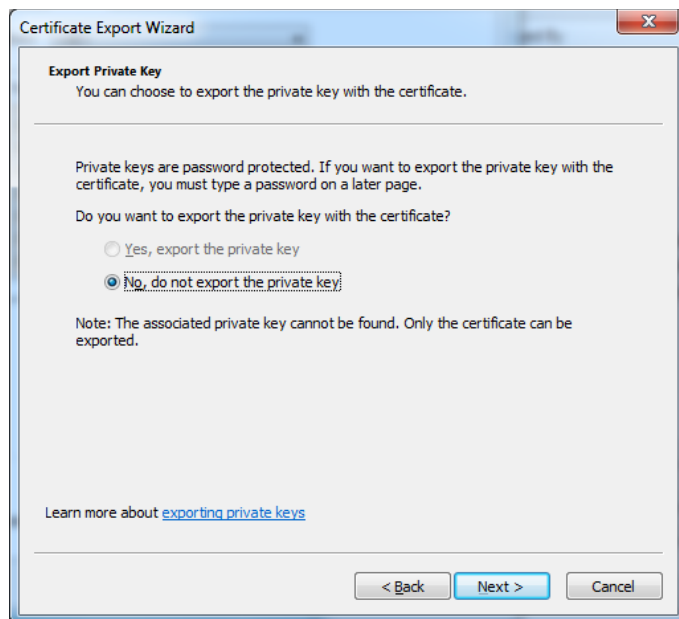
Execute the following procedure for each certificate (you can open an intermediate certificate if you click on "View Certificate")

Export one certificate

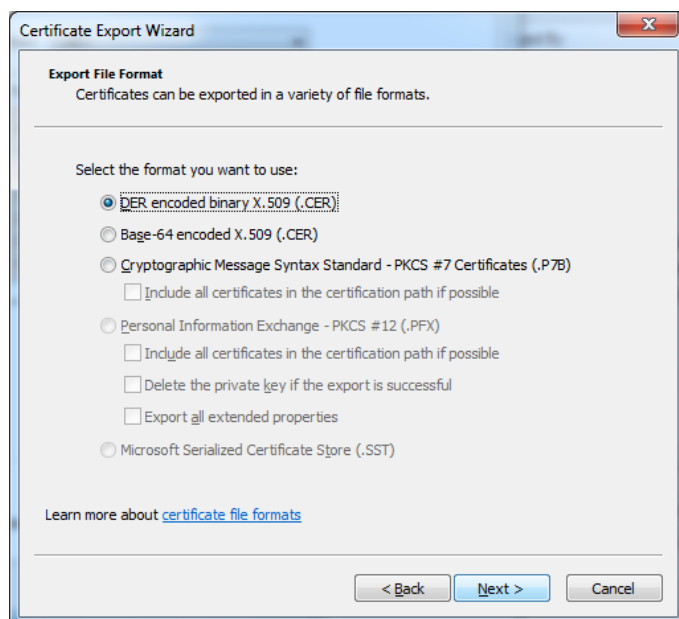
Select the second page of the certificate you want to export and select "Copy to a file".



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 NTAAuth 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 NTAAuth store, follow these steps:

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

```
certutil -dspublish -f filename NTAAuthCA
```

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