Fehlersuche für die automatische Zertifikatbeantragung (Autoenrollment) via RPC/DCOM (MS-WCCE)

Uwe Gradenegger / Juni 2021 / Funktionstest, Troubleshooting / AEPolicy, Autoenrollment, certlm.msc, certutil, Cryptographic Service Provider (CSP), Ereignisanzeige, Group Policy, MS-WCCE, RPC_S_SERVER_UNAVAILABLE, Trusted Platform Module (TPM), Windows Powershell, Zertifikatvorlage

Folgendes Szenario angenommen:

- Es ist eine Zertifikatvorlage für die automatische Beantragung von Zertifikaten konfiguriert (Autoenrollment).
- Die Zertifikatvorlage ist auf einer ins Active Directory integrierten Zertifizierungsstelle (Enterprise Certification Authority) veröffentlicht.
- Die für die automatische Zertifikatbeantragung konfigurierten Benutzer oder Computer beantragen allerdings nicht wie vorgesehen Zertifikate.

Nachfolgend eine Anleitung zur Fehlersuche.

> Dieser Artikel beschreibt die Fehlersuche von Autoenrollment über RPC/DCOM. Viele der Aussagen lassen sich auch auf die Zertifikatbeantragung über WSTEP (CEP/CES) übertragen.

Eingrenzen des Problembereiches

> Kennen Sie **TameMyCerts**? TameMyCerts ist ein Add-On für die Microsoft Zertifizierungsstelle (Active Directory Certificate Services). Es erweitert die Funktion der Zertifizierungsstelle und ermöglicht die Anwendung von Regelwerken, um die sichere Automatisierung von Zertifikat-Ausstellungen zu realisieren. TameMyCerts ist einzigartig im Microsoft-Ökosystem, hat sich bereits in unzähligen Unternehmen auf der ganzen Welt bewährt und steht unter einer freien Lizenz. Es kann über GitHub heruntergeladen und kostenlos verwendet werden. Professionelle Wartung wird ebenfalls angeboten.

Zunächst muss geklärt werden, in welchem Kontext der Fehler auftritt.

- Tritt er für Zertifikate eines Benutzers auf?
- Tritt er für Zertifikate eines Computers auf?

Für die Fehlersuche bei der Beantragung von Benutzer-Zertifikaten ist es meist erforderlich, sich mit dem betreffenden Benutzer gemeinsam in dessen Sitzung einzuklinken. Tritt der Fehler im Kontext eines

Computers auf, ist es oft möglich, ohne den Benutzer auf dem System mit einer administrativen Kennung zu arbeiten.

Möglichkeiten zur Remote-Fehlersuche

Folgende Methoden des Zugriffs auf das betreffende System ergeben sich somit für die Fehlersuche:

- Bildschirmfreigabe (Screen Sharing, zusammen mit und im Kontext des Endbenutzers)
- Administrativ / Interaktive Anmeldung (Konsole/Remote Desktop)
- Administrativ / per Remote-Konsole über PSExec Remoting (nicht empfehlenswert)
- Administrativ / per Remote-Konsole über PowerShell Remoting

> Es wird im Allgemeinen nicht empfohlen, sich mit einem administrativen Domänenkonto an einem Clientsystem anzumelden, da hier die Gefahr eines Credential-Diebstahls sehr hoch ist.

Da der kleinste gemeinsame Nenner oft die Kommandozeile ist, wird die Fehlersuche nachfolgend auch mit dieser vorgenommen.

Einordnung des Fehlerbildes

Grundsätzlich kann man Autoenrollment Fehler in folgende Bereiche einteilen, die nachfolgend näher beschrieben werden:

- Die Zertifikatanforderung wird nicht gestellt
- Die Zertifikatanforderung wird gestellt, kommt aber nicht an der Zertifizierungsstelle an
- Die Zertifikatanforderung wird gestellt, kommt auch an der Zertifizierungsstelle an, wird dort allerdings abgelehnt

Die Zertifikatanforderung wird nicht gestellt

Wird die Zertifikatanforderung überhaupt nicht gestellt, sollten folgende Punkte beleuchtet werden:

- Ist bereits ein Zertifikat der betreffenden Zertifikatvorlage vorhanden?
- Ist Autoenrollment auf dem Client aktiviert?
- Wird der Autoenrollment Prozess ausgelöst?
- Ist das betreffende Konto zur Zertifikatbeantragung berechtigt?
- Kann der Client die Vertrauenskette zur Zertifizierungsstelle herstellen?
- Kann der Client ein Schlüsselpaar erzeugen?

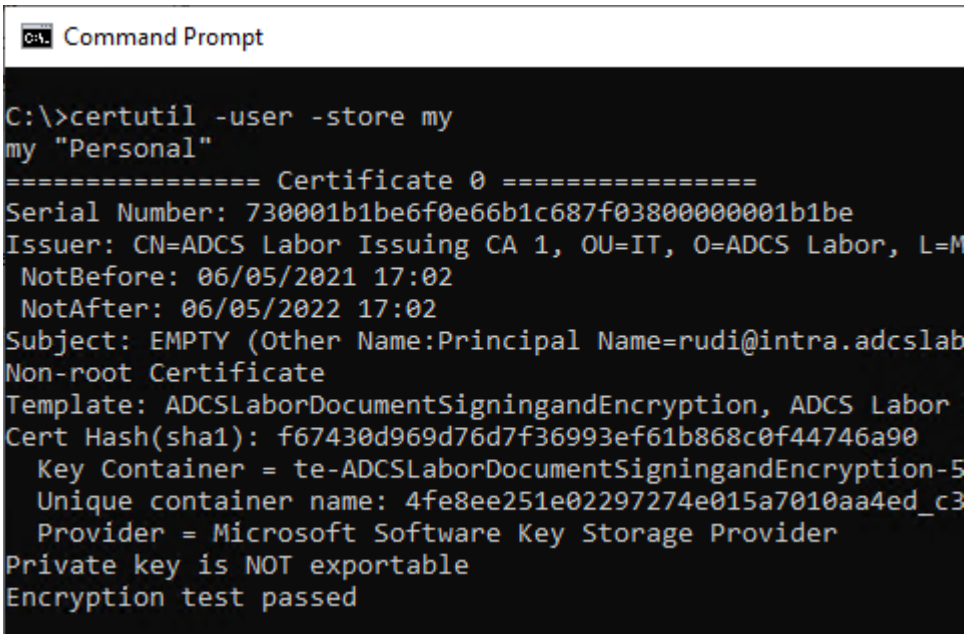
Details: Ist bereits ein Zertifikat der betreffenden Zertifikatvorlage vorhanden?

Für den Benutzerkontext:

```
certutil -user -store my
```

Für den Computerkontext:

```
certutil -store my
```



Mit diesem Befehl werden auch archivierte Zertifikate angezeigt. Daher ist es übersichtlicher, die Windows PowerShell zu verwenden.

Für den Benutzerkontext:

```
Get-ChildItem -Path Cert:\CurrentUser\My
```

Für den Computerkontext:

```
Get-ChildItem -Path Cert:\LocalMachine\My
```

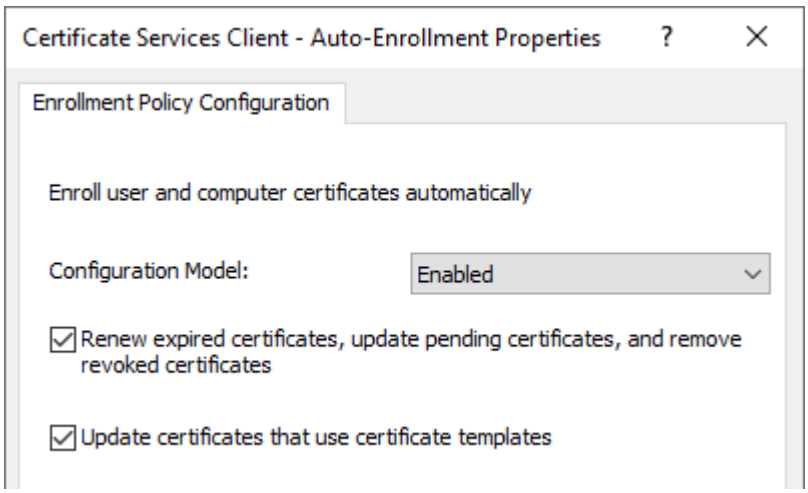
Details: Ist Autoenrollment auf dem Client aktiviert?

Wenn Autoenrollment auf dem Client nicht aktiviert ist, äußert sich dies üblicherweise dadurch, dass trotz der eindeutigen Trigger keine Zertifikatbeantragung stattfindet.

Die Konfiguration für Autoenrollment wird üblicherweise per Gruppenrichtlinie festgelegt. Nur weil eine Gruppenrichtlinie vorhanden, konfiguriert und verlinkt ist, heißt es aber nicht, dass diese auch beim Client angekommen ist.

Eine Mögliche Ursache kann z.B. fehlende Domänenkonnektivität sein oder eine Filterung anhand einer Sicherheitsgruppe oder eines anderen Kriteriums.

> Bitte auch beachten, dass
> bei Ausführung eines Prozesses via RunAs keine Gruppenrichtlinien angewendet werden und dementsprechend unter Umständen (z.B. bei Erstanmeldung via RunAs) auch kein AutoEnrollment erfolgt.



- Die Aktivierung des Autoenrollment Prozesses ("Configuration model") bewirkt zunächst, dass ein Replikat des "Public Key Services" Objektes aus der Konfigurationspartition des Active Directory geladen wird. Sie muss mindestens aktiviert sein, damit die weiteren Optionen verwendet werden können.
- Die Einstellung "*Renew expired certificates, update pending certificates, and remove revoked certificates*" bewirkt, dass abgelaufene Zertifikate automatisch erneuert werden, sofern sie von einer Active Directory integrierten Zertifizierungsstelle ausgestellt wurden. Außerdem werden genehmigte Zertifikatanforderungen von Zertifizierungsstellen abgeholt, sofern diese vorliegen. Widerrufene Zertifikate werden archiviert.
- Die Einstellung "*Update certificates that use certificate templates*" bewirkt, dass Zertifikate automatisch beantragt werden, welche für den Antragsteller für Autoenrollment freigegeben sind. Sie muss also auf dem Client aktiviert sein, damit Zertifikate automatisch beantragt werden können.

Die Autoenrollment Konfiguration wird lokal in der Registrierung gespeichert:

Für den Benutzerkontext:

```
HKCU\Software\Policies\Microsoft\Cryptography\AutoEnrollment\AEPolicy
```

Für den Computerkontext:

```
HKLM\Software\Policies\Microsoft\Cryptography\AutoEnrollment\AEPolicy
```

Im folgenden werden die einzelnen Konfigurationsoptionen für "AEPolicy" beschrieben.

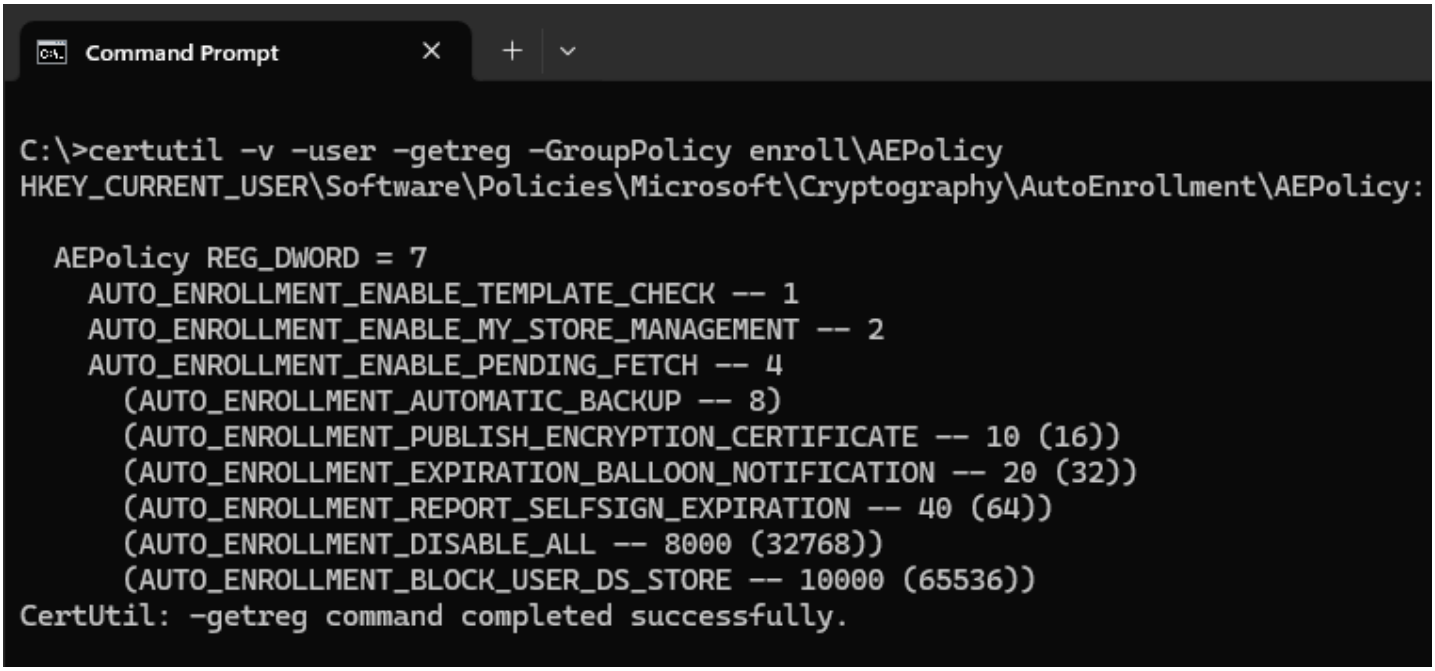
Wert	Beschreibung	Ergebnis
0x00000000 oder nicht vorhanden	AutoEnrollment Prozess ist **aktiviert** "*Update Certificates that use certificates templates*" ist **deaktiviert**	**keine** automatische Beantragung von Zertifikaten **keine** automatische Erneuerung abgelaufener Zertifikate **keine** automatische Abholung genehmigter Zertifikatanforderungen **keine** automatische Archivierung widerrufener Zertifikate
0x00000001	AutoEnrollment Prozess ist **aktiviert** "*Update Certificates that use certificates templates*" ist **aktiviert** "*Renew expired certificates, update pending certificates, and remove revoked certificates*" ist **deaktiviert**	automatische Beantragung von Zertifikaten **keine** automatische Erneuerung abgelaufener Zertifikate **keine** automatische Abholung genehmigter Zertifikatanforderungen **keine** automatische Archivierung widerrufener Zertifikate
0x00000006	AutoEnrollment Prozess ist **aktiviert** "*Update Certificates that use certificates templates*" ist **deaktiviert** "*Renew expired certificates, update pending certificates, and remove revoked certificates*" ist **aktiviert**	**keine** automatische Beantragung von Zertifikaten automatische Erneuerung abgelaufener Zertifikate automatische Abholung genehmigter Zertifikatanforderungen automatische Archivierung widerrufener Zertifikate
0x00000007	AutoEnrollment Prozess ist **aktiviert** "*Update Certificates that use certificates templates*" ist **aktiviert** "*Renew expired certificates, update pending certificates, and remove revoked certificates*" ist **aktiviert**	automatische Beantragung von Zertifikaten automatische Erneuerung abgelaufener Zertifikate automatische Abholung genehmigter Zertifikatanforderungen automatische Archivierung widerrufener Zertifikate
0x00008000	AutoEnrollment ist **deaktiviert**	**keine** automatische Beantragung von Zertifikaten **keine** automatische Erneuerung abgelaufener Zertifikate **keine** automatische Abholung genehmigter Zertifikatanforderungen

Wert	Beschreibung	Ergebnis
		keine automatische Archivierung widerrufener Zertifikate

Damit die automatische Zertifikatbeantragung erfolgt, muss "AEPolicy" somit den Wert **0x1** oder besser den Wert **0x7** aufweisen. Der Wert kann mit den folgenden Kommandozeilenbefehlen abgefragt werden.

Für den Benutzerkontext:

```
certutil -v -user -getreg -GroupPolicy enroll\AEPolicy
```



Alternativ kann der Schlüssel aus der Registrierung direkt ausgelesen werden:

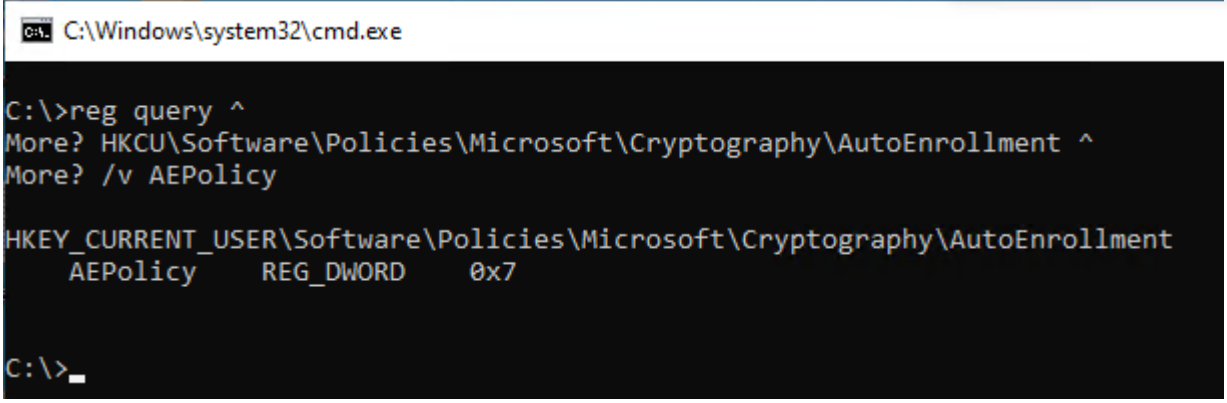
```
reg query HKCU\Software\Policies\Microsoft\Cryptography\AutoEnrollment /v AEPolicy
```

Für den Maschinenkontext:

```
certutil -v -getreg -GroupPolicy enroll\AEPolicy
```

Alternativ kann der Schlüssel aus der Registrierung direkt ausgelesen werden:

```
reg query HKLM\Software\Policies\Microsoft\Cryptography\AutoEnrollment /v AEPolicy
```



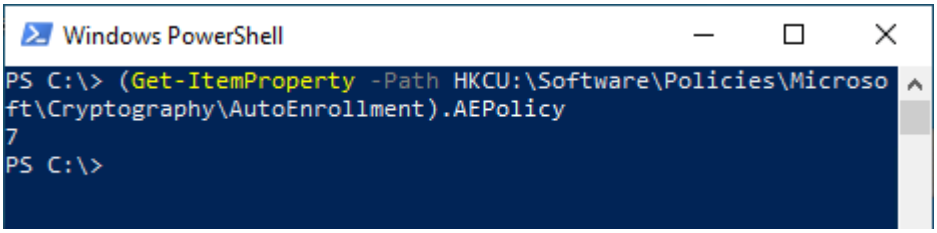
Der Wert kann auch über die Windows PowerShell aus der Registry abgefragt werden.

Für den Benutzerkontext:

```
(Get-ItemProperty -Path
HKCU:\Software\Policies\Microsoft\Cryptography\AutoEnrollment).AEPolicy
```

Für den Maschinenkontext:

```
(Get-ItemProperty -Path
HKLM:\Software\Policies\Microsoft\Cryptography\AutoEnrollment).AEPolicy
```



Angelegt können die Einstellungen auch ohne Gruppenrichtlinie mit folgenden Befehlen. Der Wert aus dem Beispielcode ist gegebenenfalls anhand der obenstehenden Tabelle anzupassen.

Für den Benutzerkontext:

```
New-Item -Path HKCU:\Software\Policies\Microsoft\Cryptography\AutoEnrollment
Set-ItemProperty -Path HKCU:\Software\Policies\Microsoft\Cryptography\AutoEnrollment -Name
AEPolicy -Value 0x7 -Force
```

Für den Maschinenkontext:

```
New-Item -Path HKLM:\Software\Policies\Microsoft\Cryptography\AutoEnrollment
Set-ItemProperty -Path HKLM:\Software\Policies\Microsoft\Cryptography\AutoEnrollment -Name
AEPolicy -Value 0x7 -Force
```

Details: Wird der Autoenrollment Prozess ausgelöst?

Die Auslöser für die Ausführung des Autoenrollment-Prozesses auf Domänenmitgliedern sind:

- Bei Anmeldung des Benutzers (bei Computern, wenn sich das Computerkonto anmeldet, also beim Systemstart).
- Per Timer alle 8 Stunden.
- Bei einer Aktualisierung der Gruppenrichtlinien, vorausgesetzt, es gab eine Änderung.

Im Aufgabenplaner befinden sich entsprechende Aufgaben unter "Microsoft" – "Windows" – "CertificateServicesClient".

Es ist also durchaus möglich, dass noch kein Trigger für die Zertifikatbeantragung ausgelöst wurde (siehe hierzu auch Artikel "Es wird kein Zertifikat per Autoenrollment beantragt, wenn ein Benutzer per Virtual Private Network (VPN) verbunden ist").

Manuell kann der Prozess mit folgenden Befehlen ausgelöst werden.

Für den Benutzerkontext:

```
certutil -pulse -user
```

Für den Computerkontext:

```
certutil -pulse
```

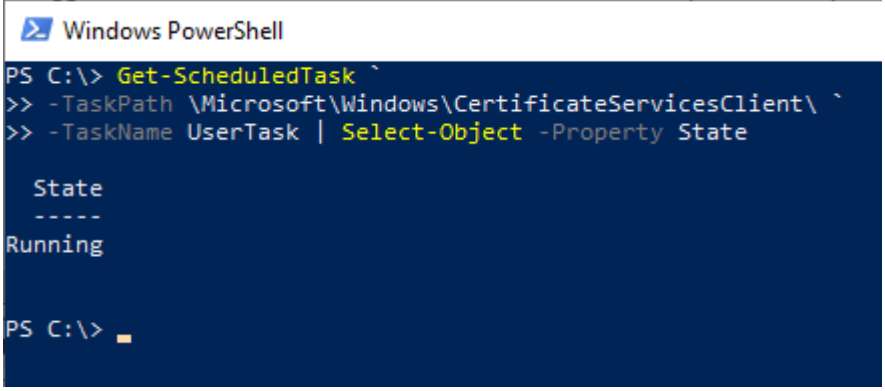
Ob der Prozess ausgelöst wurde, kann man anhand des Status der Aufgaben im Aufgabenplaner ermitteln. Dies kann auch per Windows PowerShell erfolgen:

Für den Benutzerkontext:

```
Get-ScheduledTask `
-TaskPath \Microsoft\Windows\CertificateServicesClient\ `
-TaskName UserTask | Select-Object -Property State
```

Für den Computerkontext:

```
Get-ScheduledTask `
-TaskPath \Microsoft\Windows\CertificateServicesClient\ `
-TaskName SystemTask | Select-Object -Property State
```



> Bitte beachten: Es kann auch sein, dass der Prozess dauerhaft läuft und nie beendet wird. Dies ist beispielsweise dann der Fall, wenn ein manuelles Eingreifen des Benutzers notwendig ist, der Benutzer diese Interaktion allerdings nicht durchführt.

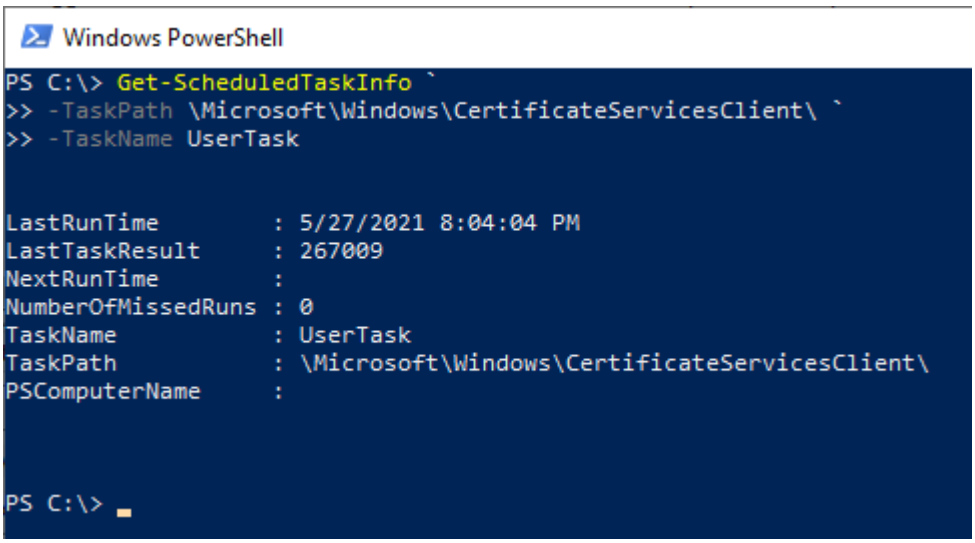
Die letzte Ausführungszeit und das Ergebnis des Task kann ebenfalls per Windows PowerShell eingesehen werden.

Für den Benutzerkontext:

```
Get-ScheduledTaskInfo `
-TaskPath \Microsoft\Windows\CertificateServicesClient\ `
-TaskName UserTask
```

Für den Computerkontext:

```
Get-ScheduledTaskInfo `
-TaskPath \Microsoft\Windows\CertificateServicesClient\ `
-TaskName SystemTask
```



Details: Ist das betreffende Konto zur Zertifikatbeantragung berechtigt?

Damit eine Zertifikatbeantragung erfolgen kann, muss der Benutzer bzw. der Computer an zwei Stellen berechtigt sein:

- In den Sicherheitsberechtigungen der betreffenden Zertifikatvorlage
- In den Sicherheitseinstellungen der Zertifizierungsstelle, welche die Zertifikatvorlage anbietet

Beide Informationen sind im Active Directory hinterlegt. Ist der Benutzer nicht berechtigt, erfolgt keine Zertifikatbeantragung.

Vorsicht bei Verwendung von Sicherheitsgruppen für die Erteilung der Berechtigungen: Nur weil der Benutzer bzw. der Computer im Active Directory Mitglied einer Sicherheitsgruppe ist, heißt das noch nicht, dass diese auch bereits im Kerberos Ticket angewendet wurde. Hat sich der Benutzer seit Hinzufügen zur Gruppe noch nicht neu angemeldet bzw. wurde der Computer noch nicht neu gestartet, wurde die Gruppenmitgliedschaft auch noch nicht angewendet.

> Der Autoenrollment Client inspiziert nicht das lokale Kerberos-Ticket, sondern die Zugriffsberechtigungen im Active Directory. Daher würde hier das Phänomen auftreten, dass zwar eine Zertifikatbeantragung ausgelöst wird, die Zertifikatbeantragung jedoch mangels Berechtigung von der Zertifizierungsstelle abgelehnt würde (Ereignis Nr. 53 mit Fehlercode CERTSRV_E_TEMPLATE_DENIED auf der Zertifizierungsstelle).

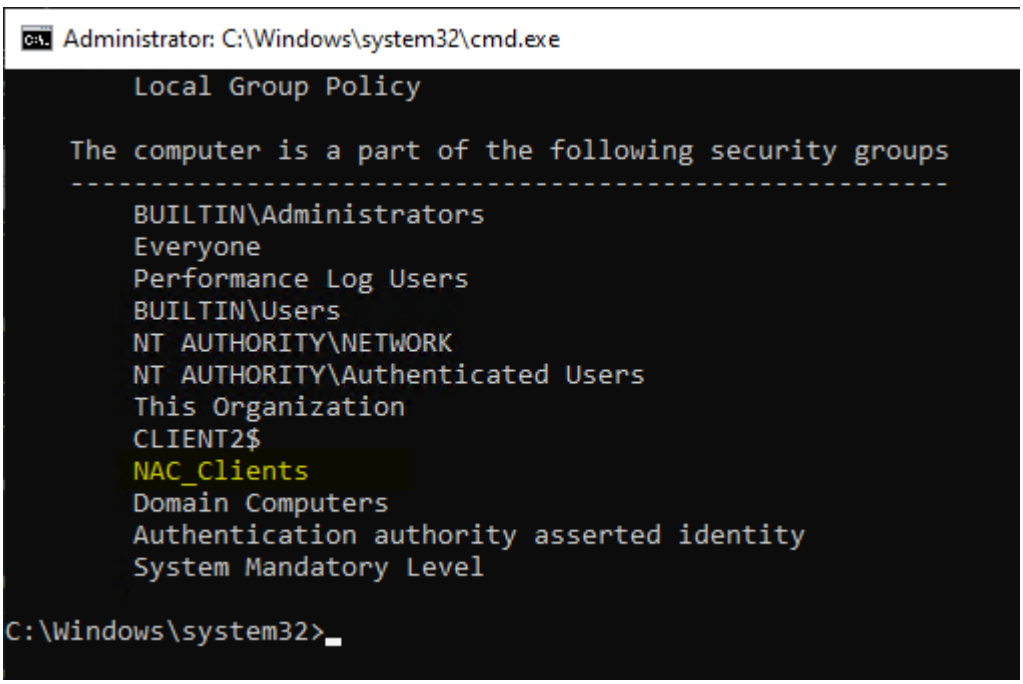
Ob die Gruppenmitgliedschaft lokal bereits abgebildet wurde, kann mit folgenden Kommandozeilenbefehlen überprüft werden.

Für den Benutzerkontext:

```
gpresult /R /Scope:User
```

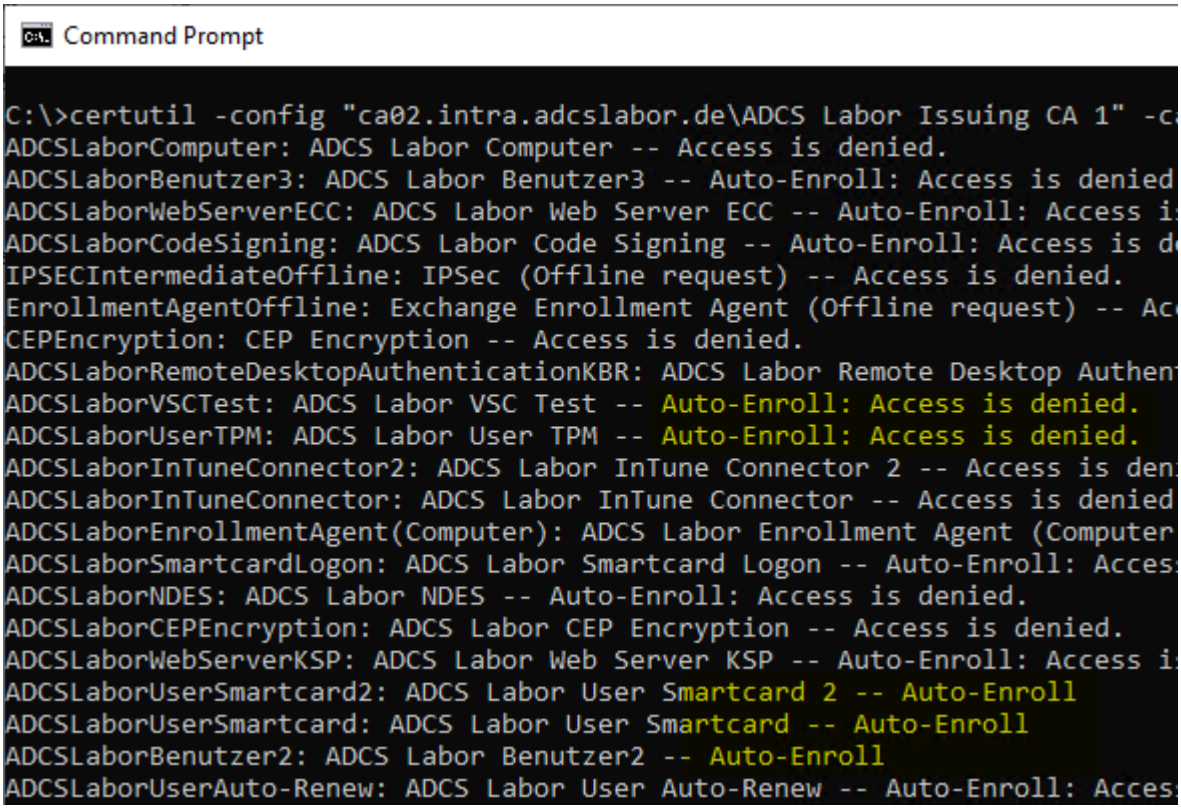
Für den Computerkontext:

```
gpresult /R /Scope:Computer
```

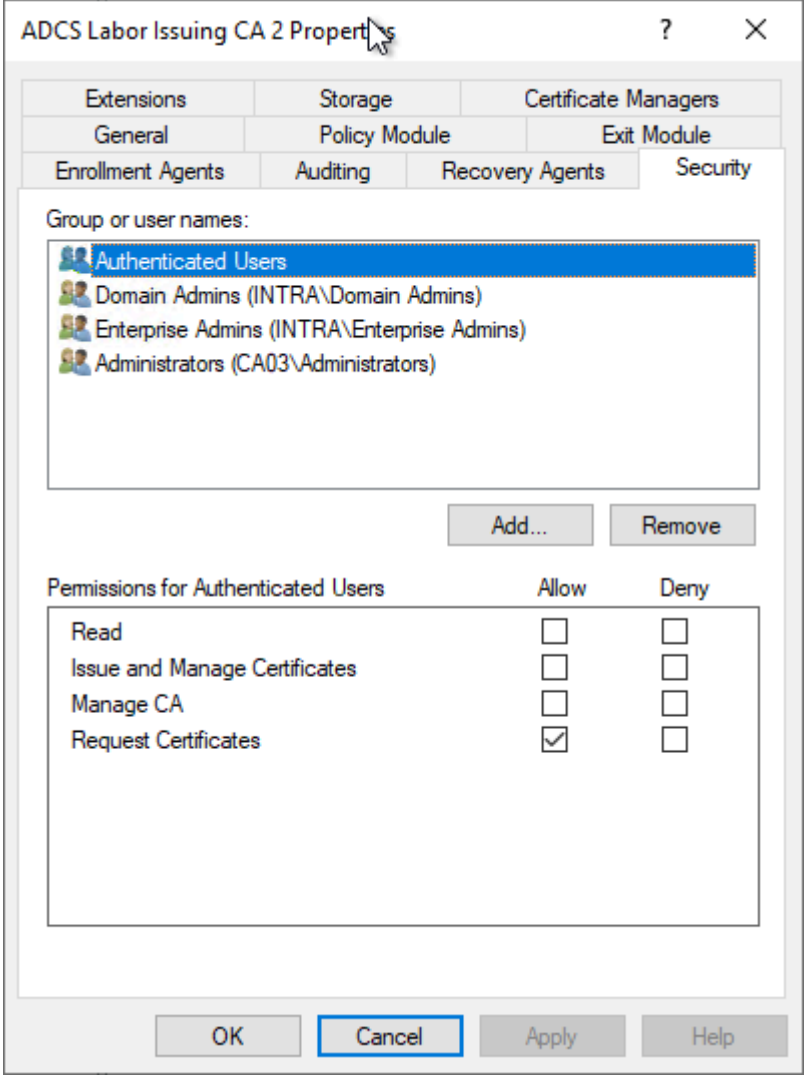


Die Berechtigungen für die Zertifikatbeantragung können auch mit folgendem Kommandozeilenbefehl überprüft werden:

```
certutil -config "Hostname-der-CA\Common-Name-der-CA" -catemplates
```



Die Berechtigung zur Beantragung von Zertifikaten auf der Zertifizierungsstelle wird in der Standardeinstellung über einen entsprechenden Eintrag für "Authenticated Users" sichergestellt.



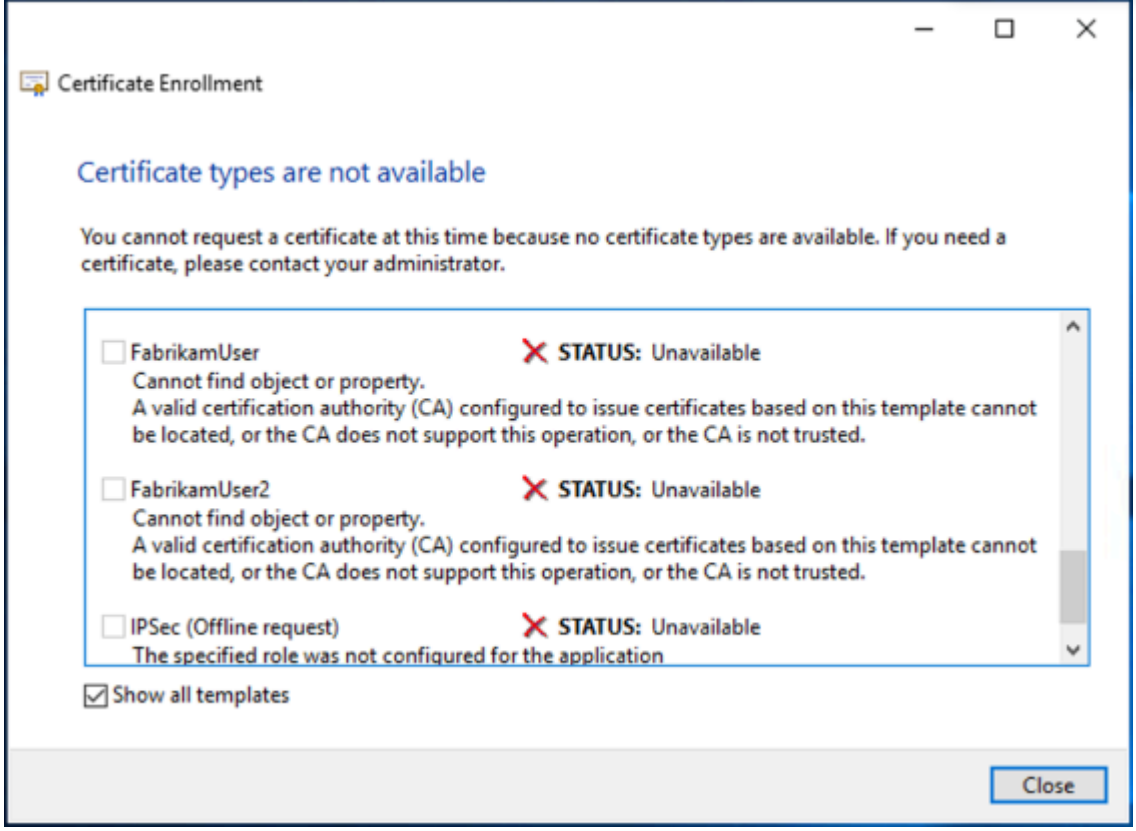
Diese Information wird ins Active Directory synchronisiert. Entsprechend können sich Clients bereits vor Antragstellung über ihre Berechtigungen informieren. Sind sie nicht berechtigt, wird auch kein Zertifikatantrag gestellt.

Typische Ursachen für fehlende Berechtigungen auf der Zertifizierungsstelle sind in folgenden Artikeln beschrieben:

- Eine Active Directory integrierte Zertifizierungsstelle (Enterprise Certification Authority) in den Wartungsmodus versetzen
- Die Beantragung eines Zertifikats schlägt fehl mit der Fehlermeldung "A valid certification authority (CA) configured to issue certificates based on this template cannot be located, or the CA does not support this operation, or the CA is not trusted."

Details: Kann der Client die Vertrauenskette zur Zertifizierungsstelle herstellen?

Versucht man, das Zertifikat über die Microsoft Management Konsole zu beantragen (certmgr.msc für den Benutzerkontext sowie certlm.msc für den Computerkontext), und die Zertifikatvorlage wird zwar angezeigt, aber ist nicht auswählbar mit der Fehlermeldung "A valid certification authority (CA) configured to issue certificates based on this template cannot be located, or the CA does not support this operation, or the CA is not trusted.", ist es möglich, dass der Client die entsprechende ausstellende Zertifizierungsstelle nicht kennt, d.h. die Vertrauenskette nicht herstellen kann.



In diesem Fall sollte folgendes überprüft werden:

- Ist die Stammzertifizierungsstelle (engl. "Root CA") im entsprechenden Speicher für vertrauenswürdige Stammzertifizierungsstellen hinterlegt?
- Sind (sofern vorhanden) alle Zwischenzertifizierungsstellen im Speicher für Zwischenzertifizierungsstellen-Zertifikate hinterlegt? (Dieser Speicher wird auf Domänen-Clients automatisch aus dem "AIA" Objekt des Public Key Services Containers im Active Directory befüllt. Entsprechend sollte überprüft werden, ob die Zertifikate auch dort hinterlegt sind)

Siehe hierzu auch:

- Die Beantragung eines Zertifikats schlägt fehl mit der Fehlermeldung "A valid certification authority (CA) configured to issue certificates based on this template cannot be located, or the CA does not support this operation, or the CA is not trusted."

Details: Kann der Client ein Schlüsselpaar erzeugen?

Das Schlüsselpaar kann nicht erzeugt werden, z.B. weil der Cryptographic Service Provider bzw. Key Storage Provider nicht vorhanden ist oder nicht funktioniert (würde auf dem Client das Ereignis Nr. 57 auslösen).

Ob ein bestimmter Key Storage Provider auf dem Client benutzbar ist, kann mit folgendem Befehl überprüft werden.

```
certutil -csp "Microsoft Platform Crypto Provider" -csptest
```

Im Erfolgsfall würde folgende Meldung generiert:

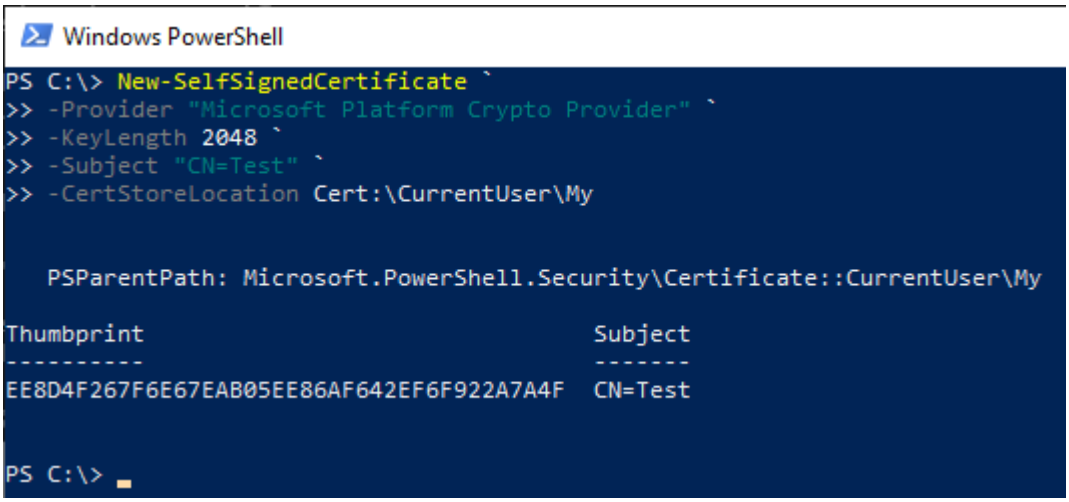
```
CertUtil: -csptest-Befehl wurde erfolgreich ausgeführt.
```

Im Fehlerfall würde eine mit folgener vergleichbare Meldung generiert:

```
CertUtil: -csptest command FAILED: 0x80090030 (-2146893776 NTE_DEVICE_NOT_READY)
CertUtil: The device that is required by this cryptographic provider is not ready for use.
```

Es ist auch möglich, mit der Windows PowerShell ein selbstsigniertes Zertifikat unter Verwendung des entsprechenden Key Storage Provider zu erzeugen:

```
New-SelfSignedCertificate `
-Provider "Microsoft Platform Crypto Provider" `
-KeyLength 2048 `
-Subject "CN=Test" `
-CertStoreLocation Cert:\CurrentUser\My
```



> Siehe auch Artikel ''Die Beantragung eines Zertifikats ist nicht möglich, da die Zertifikatvorlage nicht angezeigt wird. Die Fehlermeldung lautet ''Can not find a valid CSP in the local machine.''''.

Die Zertifikatanforderung wird gestellt, kommt aber nicht an der Zertifizierungsstelle an

Wird die Zertifikatanforderung zwar gestellt, kommt aber nicht bei der Zertifizierungsstelle an, sollten folgende Punkte beleuchtet werden:

- Ist die Zertifizierungsstelle erreichbar und kann sich an dieser authentifiziert weden?
- Kann ein Zertifikat von der betreffenden Zertifikatvorlage manuell angefordert werden?

Ist die Zertifizierungsstelle erreichbar und kann sich an dieser authentifiziert werden?

Fehler, die aufgrund eines Problems mit der Netzwerkverbindung oder der Authentifizierung an der RPC/DCOM Schnittstelle auftreten können, verursachen den Fehlercode RPC_S_SERVER_UNAVAILABLE.

> Siehe hierzu Artikel "Die Beantragung eines Zertifikats schlägt fehl mit Fehlermeldung "The certificate request could not be submitted to the certification authority. Error: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)"".

Beim Zertifikatregistrierungs-Webdienst (CES) gibt der Client den gleichen Fehlercode aus, wenn der Serverdienst läuft, aber keine Verbindung zur Zertifizierungsstelle herstellen kann. Kann der Serverdienst jedoch erst gar nicht starten, weil die Zertifizierungsstelle zu diesem Zeitpunkt nicht erreichbar ist, wird der Fehlercode WS_E_ENDPOINT_FAILURE sein, der sich aber wiederum in den meisten Fällen im Backend auf RPC_S_SERVER_UNAVAILABLE herunterbrechen lässt.

Mit der folgenden Befehlsabfolge in der Windows PowerShell kann einfach die gesamte Kette bis zur Zertifizierungsstelle (über RPC/DCOM) validiert werden.

```
$ConfigString = "{Hostname-der-Zertifizierungstelle}\{Common-Name-der-
Zertifizierungsstelle}"
$CertRequest = New-Object -ComObject CertificateAuthority.Request
$CertRequest.GetCAProperty($ConfigString, 0x6, 0, 4, 0)
```

Der Befehl sollte bei Erfolg den Common Name der Zertifizierungsstelle zurückmelden.

Für den Computerkontext muss zunächst in den diesen gewechselt werden (NT-AUTHORITY\SYSTEM). Dies kann beispielsweise per psexec erfolgen:

```
psexec -s -i powershell.exe
```

Anschließend kann der vorige Befehl im Kontext des Computerkontos ausgeführt werden.

Details: Kann ein Zertifikat von der betreffenden Zertifikatvorlage manuell angefordert werden?

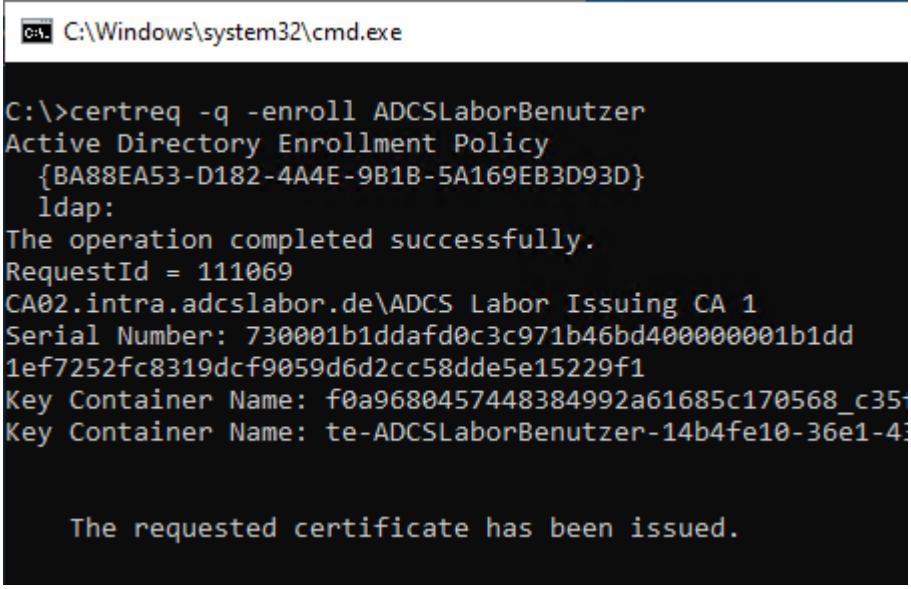
Die Zertifikatbeantragung für eine bestimmte Zertifikatvorlage kann mit folgendem Befehl manuell (also ohne Autoenrollment) ausgelöst werden.

Für den Benutzerkontext:

```
certreq -q -enroll "Name-der-Zertifikatvorlage"
```

Für den Computerkontext:

```
certreq -q -machine -enroll "Name-der-Zertifikatvorlage"
```



> Ein Aufruf des Befehls ohne den -q Parameter öffnet einen GUI Dialog. In einer Remote-Shell-Verbindung führt dies dazu, dass der Prozess stehen bleibt.

Schlägt die Zertifikatbeantragung mit Fehlercode "CERTSRV_E_UNSUPPORTED_CERT_TYPE" fehl, siehe Artikel "Die Beantragung eines Zertifikats schlägt fehl mit Fehlermeldung "The requested certificate template is not supported by this CA. 0x80094800 (-2146875392 CERTSRV_E_UNSUPPORTED_CERT_TYPE).""".

Weitere mögliche Ursachen

- Die Zertifizierungsstelle kann eine benötigte Verbindung nicht herstellen (im Falle von Domänencontroller-Zertifikaten). Siehe hierzu Artikel "Die Beantragung eines Zertifikats für Domänencontroller schlägt fehl mit Fehlermeldung "The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)".
- Die Sicherheitsberechtigungen des Betriebssystems der Zertifizierungsstelle erlauben keine Zertifikatbeantragung. Siehe hierzu Artikel "Die Beantragung eines Zertifikats schlägt fehl mit Fehlermeldung "The request is not supported. 0x80070032 (WIN32: 50 ERROR_NOT_SUPPORTED)""".

Die Zertifikatanforderung wird gestellt, kommt auch an der Zertifizierungsstelle an, wird dort allerdings abgelehnt

Kommt die Zertifikatanforderung an der Zertifizierungsstelle an, wird dort allerdings abgelehnt, wird diese das Ereignis Nr. 53 protokollieren. Mögliche Ursachen und deren Lösung sind im entsprechenden Artikel beschrieben.

Protokollierungsebene für Autoenrollment auf dem Client erhöhen

Um ein Problem weiter einzugrenzen, kann es hilfreich sein, die Protokollierungsebene für Autoenrollment auf dem Client zu erhöhen (siehe hierzu auch Artikel "Protokollierung für die automatische Zertifikatbeantragung (Autoenrollment) aktivieren").

Mit folgendem Kommandozeilenbefehl kann die Protokollierung für den Benutzer- als auch den Systemkontext aktiviert werden (Es werden alle Ereignisse der Typen "Error", "Warning" und "Information" ausgegeben):

```
certutil -setreg Enroll\LogLevel 4
```

> Die Änderungen werden direkt ohne Neuanmeldung bzw. Neustart aktiv.

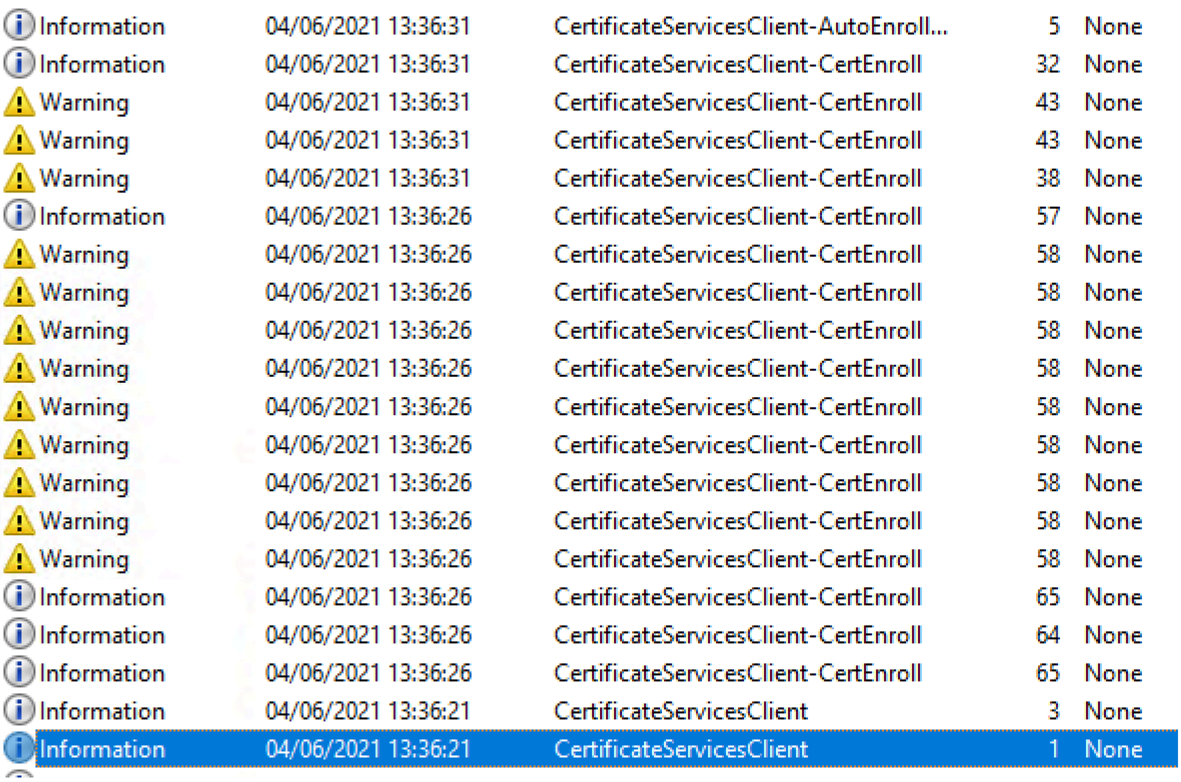
Anschließend kann eine Zertifikatbeantragung ausgelöst werden. Entsprechende Ereignisse sollten sich nun im Anwendungs-Ereignisprotokoll finden.

Aufbau einer üblichen Ereignis-Sequenz

Eine übliche Sequenz sieht wie folgt aus:

Quelle	Nummer	Ereignistext
Microsoft-Windows-CertificateServicesClient-AutoEnrollment	2	Automatic certificate enrollment for %1 started.
Microsoft-Windows-CertificateServicesClient-AutoEnrollment	4	Automatic certificate enrollment for %1 invoked the enrollment API.
Microsoft-Windows-CertificateServicesClient	1	Certificate Services Client has been started successfully.
Microsoft-Windows-CertificateServicesClient	3	Certificate Services Client has detected network connectivity.
Microsoft-Windows-CertificateServicesClient-CertEnroll	65	Certificate enrollment for %1 is successfully authenticated by policy server %2 using authentication mechanism %5 (Credential: %4). Policy Id: %3
Microsoft-Windows-CertificateServicesClient-CertEnroll	64	Certificate enrollment for %1 successfully load policy from policy server %2
(ggfs. weitere)		

Quelle	Nummer	Ereignistext
Microsoft-Windows-CertificateServicesClient-AutoEnrollment	5	Automatic certificate enrollment for %1 returned from the enrollment API.
Microsoft-Windows-CertificateServicesClient-AutoEnrollment	3	Automatic certificate enrollment for %1 completed.
Microsoft-Windows-CertificateServicesClient	2	Certificate Services Client has been stopped.



Information	04/06/2021 13:36:31	CertificateServicesClient-AutoEnroll...	5	None
Information	04/06/2021 13:36:31	CertificateServicesClient-CertEnroll	32	None
Warning	04/06/2021 13:36:31	CertificateServicesClient-CertEnroll	43	None
Warning	04/06/2021 13:36:31	CertificateServicesClient-CertEnroll	43	None
Warning	04/06/2021 13:36:31	CertificateServicesClient-CertEnroll	38	None
Information	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	57	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Warning	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	58	None
Information	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	65	None
Information	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	64	None
Information	04/06/2021 13:36:26	CertificateServicesClient-CertEnroll	65	None
Information	04/06/2021 13:36:21	CertificateServicesClient	3	None
Information	04/06/2021 13:36:21	CertificateServicesClient	1	None

Abfrage der Ereignisse

Mit folgendem Windows PowerShell Befehl können die Ereignisse ausgelesen werden:

```
Get-WinEvent -FilterHashtable @{
Logname='Application'
ProviderName=@('Microsoft-Windows-CertificateServicesClient-AutoEnrollment','Microsoft-Windows-CertificateServicesClient','Microsoft-Windows-CertificateServicesClient-CertEnroll')
StartTime=(Get-Date -Hour 0 -Minute 0 -Second 0)
} | Sort-Object -Property TimeCreated -Descending
```

Hierbei werden folgende Kriterien angewendet:

- Quelle: Ereignisse der betreffenden drei Kategorien
- Zeitraum: Die Ereignisse des heutigen Tages

- Sortierung: Absteigend nach Datum

```
PS C:\Users\rudi.INTRA\Desktop> Get-WinEvent -FilterHashtable @{
>>   Logname='Application'
>>   ProviderName=@('Microsoft-Windows-CertificateServicesClient-AutoEnrollment','Microsoft-Windows-CertificateS
>>   StartTime=(Get-Date).AddMinutes(-5)
>> } | Sort-Object -Property TimeCreated -Descending


   ProviderName: Microsoft-Windows-CertificateServicesClient-CertEnroll

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
6/4/2021 4:27:02 PM             58 Warning          The "HMAC(0x8009)" algorithm for the "Microsoft Base Cryptog
6/4/2021 4:27:02 PM             58 Warning          The "MAC(0x8005)" algorithm for the "Microsoft Base Cryptogr
6/4/2021 4:27:02 PM             58 Warning          The "SSL3 SHAMD5(0x8008)" algorithm for the "Microsoft Base
6/4/2021 4:27:02 PM             57 Information      The "Microsoft Platform Crypto Provider" provider was not lo
6/4/2021 4:27:02 PM             58 Warning          The "CYLINK MEK(0x660c)" algorithm for the "Microsoft Base D
6/4/2021 4:27:01 PM             58 Warning          The "ECDSA_numsP384t1(0x10)" algorithm for the "Microsoft So
6/4/2021 4:27:01 PM             58 Warning          The "ECDSA_numsP256t1(0x10)" algorithm for the "Microsoft So
6/4/2021 4:27:01 PM             58 Warning          The "ECDSA_numsP512t1(0x10)" algorithm for the "Microsoft So
6/4/2021 4:27:01 PM             58 Warning          The "ECDSA_curve25519(0x10)" algorithm for the "Microsoft So
6/4/2021 4:27:01 PM             58 Warning          The "ECDH_curve25519(0x18)" algorithm for the "Microsoft Sof
6/4/2021 4:27:01 PM             58 Warning          The "ECDH_numsP256t1(0x18)" algorithm for the "Microsoft Sof
6/4/2021 4:27:01 PM             58 Warning          The "AES-GMAC(0x2)" algorithm for the "BCrypt" provider was
6/4/2021 4:27:01 PM             58 Warning          The "AES-CMAC(0x2)" algorithm for the "BCrypt" provider was
6/4/2021 4:27:01 PM             58 Warning          The "ECDH_numsP512t1(0x18)" algorithm for the "Microsoft Sof
6/4/2021 4:27:01 PM             58 Warning          The "ECDH_numsP384t1(0x18)" algorithm for the "Microsoft Sof
6/4/2021 4:27:01 PM             58 Warning          The "DESX(0x1)" algorithm for the "BCrypt" provider was not
6/4/2021 4:27:01 PM             58 Warning          The "XTS-AES(0x1)" algorithm for the "BCrypt" provider was n
6/4/2021 4:27:01 PM             58 Warning          The "3DES_112(0x1)" algorithm for the "BCrypt" provider was
6/4/2021 4:27:01 PM             65 Information      Certificate enrollment for INTRA\rudi is successfully auther
6/4/2021 4:27:01 PM             64 Information      Certificate enrollment for INTRA\rudi successfully load poli
6/4/2021 4:27:01 PM             65 Information      Certificate enrollment for INTRA\rudi is successfully auther


   ProviderName: Microsoft-Windows-CertificateServicesClient

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
6/4/2021 4:27:01 PM              3 Information      Certificate Services Client has detected network connectivit


   ProviderName: Microsoft-Windows-CertificateServicesClient-AutoEnrollment

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
6/4/2021 4:27:01 PM              4 Information      Automatic certificate enrollment for INTRA\rudi invoked the
6/4/2021 4:27:01 PM              2 Information      Automatic certificate enrollment for INTRA\rudi started.


   ProviderName: Microsoft-Windows-CertificateServicesClient

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
6/4/2021 4:27:01 PM              1 Information      Certificate Services Client has been started successfully.
```

Ereignisse in eine Datei speichern

Die Ereignisse können auch einfach im CSV-Format abgespeichert werden, um die Analyse abseits des fehlerhaften Systems vorzunehmen:

```
... | Select-Object -Property TimeCreated,Id,LevelDisplayName,Message | Export-Csv -Path
.\$($env:Computername)_ClientEvents.csv -Encoding Unicode -NoTypeInformation
```

> Ein Export in eine .evt oder .evtx Datei ist nach Filterung nicht mehr möglich.

Weiterführende Links:

- Grundlagen: Cryptographic Service Provider (CSP) und Key Storage Provider (KSP)
- Benötigte Firewallregeln für Active Directory Certificate Services
- Details zum Ereignis mit ID 53 der Quelle Microsoft-Windows-CertificationAuthority
- Grundlagen manuelle und automatische Zertifikatbeantragung über Lightweight Directory Access Protocol (LDAP) und Remote Procedure Call / Distributed Common Object Model (RPC/DCOM)

Externe Quellen

- Troubleshooting Autoenrollment (Microsoft)
- How to troubleshoot Certificate Enrollment in the MMC Certificate Snap-in (Microsoft)
- Active Directory Certificate Services (AD CS) Troubleshooting: Certificate Autoenrollment (Microsoft)
- Configure Certificate Autoenrollment (Microsoft)
- Troubleshooting Certificate Enrollment (Microsoft, Archivlink)
- Update computer group membership without a reboot (shellandco.net)
- How to Refresh AD Groups Membership without Reboot/Logoff? (Windows OS Hub)
- certutil (Microsoft)