

# Details of the event with ID 53 of the source Microsoft-Windows-CertificationAuthority

Uwe Gradenegger / September 2020 / Events, Certification Authority / Event display, Extended key usage (EKU), Hardware Security Module (HSM), NTE\_BAD\_DATA, SafeNet, Certificate Template

Event Source:	Microsoft-Windows-CertificationAuthority
Event ID:	53 (0x35)
Event log:	Application
Event type:	Warning
Symbolic Name:	MSG_DN_CERT_DENIED_WITH_INFO
Event text (English):	Active Directory Certificate Services denied request %1 because %2. The request was for %3. Additional information: %4
Event text (German):	The request %1 was rejected because %2. The request was for %3. More information: %4

## Parameter

The parameters contained in the event text are filled with the following fields:

- %1: RequestId (win:UnicodeString)
- %2: Reason (win:UnicodeString)
- %3: SubjectName (win:UnicodeString)
- %4: AdditionalInformation (win:UnicodeString)

## Example events

Active Directory Certificate Services denied request 146 because The public key does not meet the minimum size required by the specified certificate template. 0x80094811 (-2146875375 CERTSRV\_E\_KEY\_LENGTH). The request was for CN=TestNDESCert. Additional information: Denied by Policy Module

The [TameMyCerts](#) Policy module for the Microsoft Certification Authority is available on [GitHub](#) available (Current version: [1.6.1045.1129](#) / [Manual](#) / [Changelog](#)).

The [PSCertificateEnrollment](#) PowerShell module is set to [GitHub](#) and in the [PowerShell Gallery](#) available (Current version: 1.0.9 / [Changelog](#)).

## SEARCH

## PKI EVENTS

- [Active Directory](#)
- [Autoenrollment](#)
- [Online responder \(OCSP\)](#)
- [Online responder \(OCSP, Audit\)](#)
- [Network Device Registration Service \(NDES\)](#)
- [Remote Desktop Session Host \(RDP\)](#)
- [Certificate Enrollment Policy Web Service \(CEP\)](#)
- [Certificate Enrollment Web Service \(CES\)](#)
- [Certification Authority](#)
- [Certification Authority \(Audit\)](#)

## RECENT POSTS

- [New ESC15 vulnerability discovered in Active Directory Certificate Services - easy-to-implement countermeasures](#)  
October 2024
- [How the TameMyCerts Policy Module for Active Directory Certificate Services \(ADCS\) can repair incoming certificate](#)

GeneralDetails

Active Directory Certificate Services denied request 146 because The public key does not meet the minimum size required by the specified certificate template. 0x80094811 (-2146875375 CERTSRV\_E\_KEY\_LENGTH). The request was for CN=TestNDESCert. Additional information: Denied by Policy Module

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:24.08.2020 18:05:20

Task Category:None

Keywords:

Computer:CA02.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 168 because The permissions on the certificate template do not allow the current user to enroll for this type of certificate. 0x80094012 (-2146877422 CERTSRV\_E\_TEMPLATE\_DENIED). The request was for INTRA\WEB01\$. Additional information: Denied by Policy Module

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 168 because The permissions on the certificate template do not allow the current user to enroll for this type of certificate. 0x80094012 (-2146877422 CERTSRV\_E\_TEMPLATE\_DENIED). The request was for INTRA\WEB01\$. Additional information: Denied by Policy Module

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:15.09.2020 11:24:14

Task Category:None

Keywords:

Computer:CA02.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 799 because An internal error occurred. 0x80090020 (-2146893792 NTE\_FAIL). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

- How the TameMyCerts Policy Module for Active Directory Certificate Services (ADCS) can help establish digital signature processes in the company  
July 2024
- How the TameMyCerts Policy Module for Active Directory Certificate Services (ADCS) can help secure scenarios with Microsoft Intune and other Mobile Device Management (MDM) systems  
July 2024
- How the TameMyCerts Policy Module for Active Directory Certificate Services (ADCS) can detect and prevent attacks against the ESC6 and ESC7 attack vectors  
July 2024

### CATEGORIES

- Active Directory (70)
- Code signature (6)
- Events (390)
- Function test (5)
- Basics (23)
- High availability (4)
- Internet Information Services (IIS) (14)
- Online Certificate Status Protocol (OCSP) (54)
- Penetration Testing (10)
- Network Device Registration Service (NDES) (109)
- Security (96)
- Backup and restore (8)
- Smartcard (14)
- Software development (2)
- TameMyCerts (7)
- Test environment (2)
- Troubleshooting (181)
- Windows operating system (14)
- Certificate usage (285)
- Certificate Enrollment Web Services (84)
- Certification Authority (288)
- Certification Authority Cluster (2)
- Certification Authority Database (20)
- Certification Authority Installation (12)
- Certification Authority Maintenance (7)
- Certification Authority Web Enrollment (CAWE) (18)

### TAGS

- Apple MacintoshAuditing
- Exhibition guideline
- AutoscrolltestCodinginf

English

GeneralDetails

Active Directory Certificate Services denied request 875 because An internal error occurred. 0x80090020 (-2146893792 NTE\_FAIL). The request was for Additional information: Error Constructing or Publishing Certificate

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:02.09.2020 16:12:48

Task Category:None

Keywords:None

Computer:

Copy

Close

Active Directory Certificate Services denied request 798 because Invalid Signature. 0x80090006 (-2146893818 NTE\_BAD\_SIGNATURE). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 869 because Invalid Signature. 0x80090006 (-2146893818 NTE\_BAD\_SIGNATURE). The request was for Additional information: Error Constructing or Publishing Certificate

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:02.09.2020 16:12:12

Task Category:None

Keywords:

Computer:

Copy

Close

Active Directory Certificate Services denied request 797 because The security token does not have storage space available for an additional container. 0x80090023 (-2146893789 NTE\_TOKEN\_KEYSET\_STORAGE\_FULL). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

certreqcertutilChromium

CryptoAPI

Cryptographic Service Provider (CSP)

CT\_FLAG\_SUBJECT\_ALT\_REQUIRE\_DOMAIN

Delegation (Kerberos)

Domain controller (DC)

Elliptic curves

Enrollment Agent

Enroll on Behalf of (EOBO)

Event display

Extended key usage (EKU)ESC1

ESC6Exit moduleFirewall

Group Managed Service Account (gMSA)

Group Policy

Hardware Security Module (HSM)

HTTP error 500

HTTP over SSL (HTTPS)

In-Place Upgrade

Internet Information Services (IIS)

Kerberos

Key Storage Provider (KSP)

Microsoft EdgeMicrosoft Intune

Microsoft OutlookMigration

Mobile Device Management (MDM)

MS-WSTEPMS-XCEP

Network Policy Server (NPS)

NTAuthCertificatesPKCS#1

PKCS#7Policy module

Private Key Archiving

PSCertificateEnrollment

Registration Authority (RA)

RegistryRemote Desktop (RDP)

RFC 2818RFC 5280

RPC\_S\_SERVER\_UNAVAILABLE

SafeNetSeBatchLogonRight

Secure/Multipurpose Internet Mail Extensions (S/MIME)

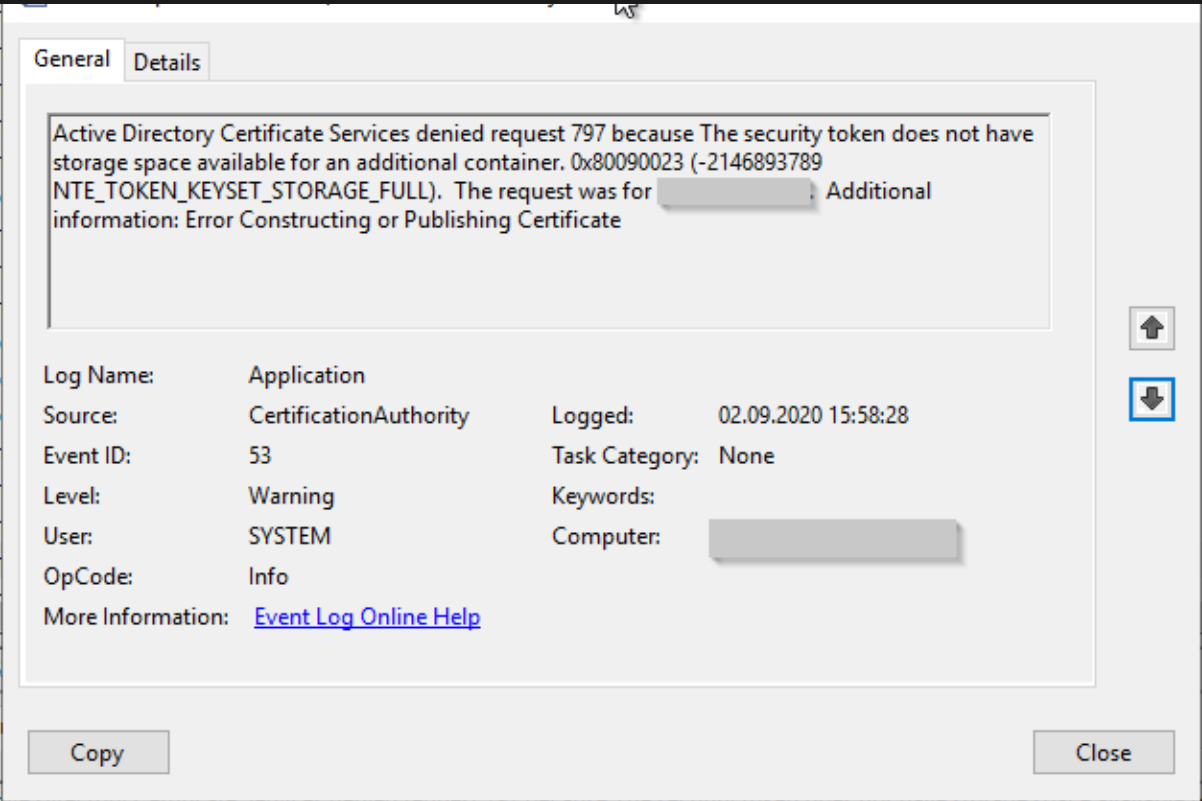
Secure Sockets Layer (SSL)

Service Principal Name (SPN)

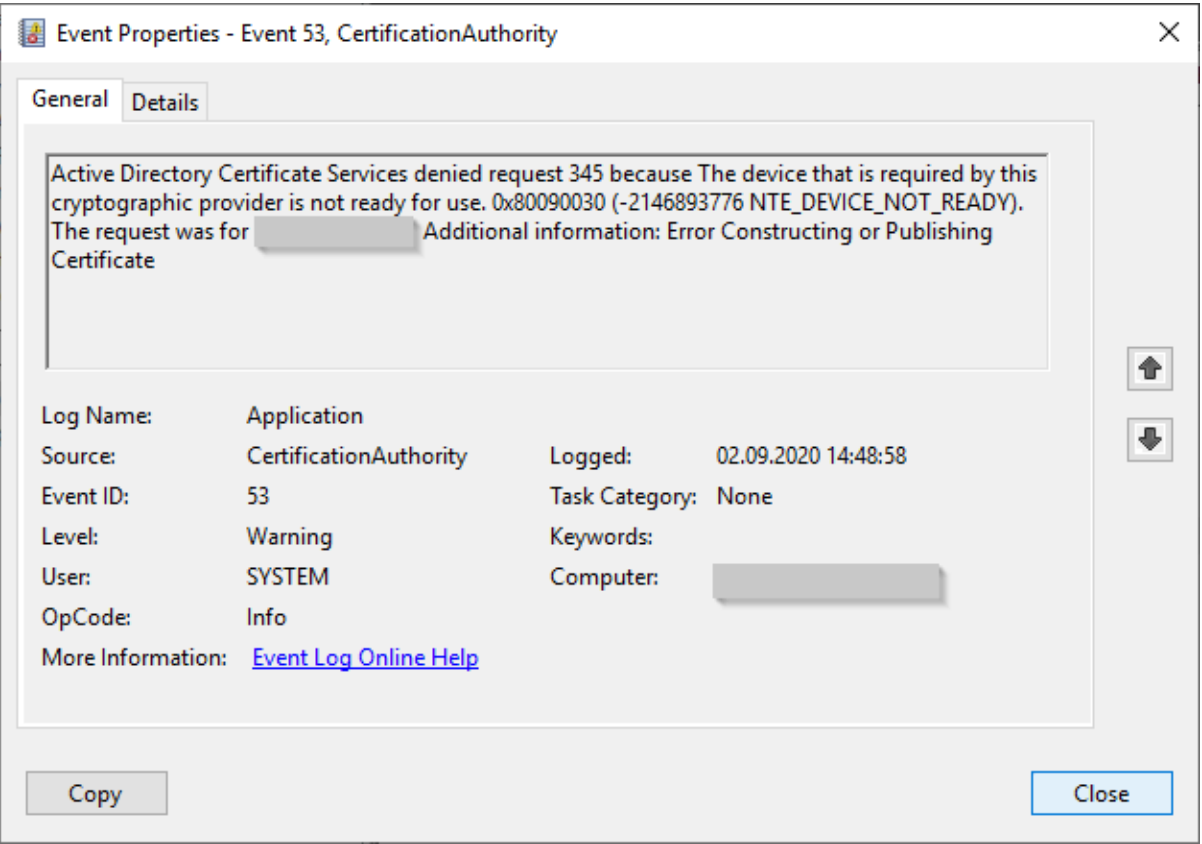
SeServiceLogonRight

Safety hardening

English



Active Directory Certificate Services denied request 795 because The device that is required by this cryptographic provider is not ready for use. 0x80090030 (-2146893776 NTE\_DEVICE\_NOT\_READY). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate



Active Directory Certificate Services denied request 788 because Incorrect password. 0x80090033 (-2146893773 NTE\_INCORRECT\_PASSWORD). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

- (CDP)
- Subject Alternative Name (SAN)
- TameMyCerts Policy Module
- TPM Key Attestation
- Trusted Platform Module (TPM)
- Windows Hello for Business
- Windows Powershell
- Certificate Enrollment Guideline
- Certificate Enrollment Policy Web Service (CEP)
- Certificate Enrollment Web Service (CES)
- Certificate Revocation List (CRL)
- Certificate Template
- Certification Authority Certificate

ARCHIVE

- October 2024
- July 2024
- January 2024
- November 2023
- July 2023
- May 2023
- April 2023
- January 2023
- December 2022
- November 2022
- October 2022
- September 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- November 2021
- October 2021
- September 2021
- August 2021
- July 2021
- June 2021
- May 2021
- April 2021
- March 2021
- February 2021
- January 2021
- December 2020
- November 2020
- October 2020
- September 2020
- August 2020
- July 2020
- June 2020
- May 2020
- April 2020
- March 2020
- February 2020

GeneralDetails

Active Directory Certificate Services denied request 876 because Incorrect password. 0x80090033 (-2146893773 NTE\_INCORRECT\_PASSWORD). The request was for Additional information: Error Constructing or Publishing Certificate

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:02.09.2020 16:12:48

Task Category:None

Keywords:

Computer:

Copy

Close

Active Directory Certificate Services denied request 782 because The signature of the certificate cannot be verified. 0x80096004 (-2146869244 TRUST\_E\_CERT\_SIGNATURE). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 782 because The signature of the certificate cannot be verified. 0x80096004 (-2146869244 TRUST\_E\_CERT\_SIGNATURE). The request was for Additional information: Error Constructing or Publishing Certificate

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:02.09.2020 15:57:48

Task Category:None

Keywords:

Computer:

Copy

Close

Active Directory Certificate Services denied request 777 because The parameter is incorrect. 0x80090027 (-2146893785 NTE\_INVALID\_PARAMETER). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

META

- [Uwe Gradenegger](#)
- [Entries feed](#)
- [Comments feed](#)
- [WordPress.org](#)



GeneralDetails

Active Directory Certificate Services denied request 777 because The parameter is incorrect. 0x80090027 (-2146893785 NTE\_INVALID\_PARAMETER). The request was for [REDACTED]  
Additional information: Error Constructing or Publishing Certificate

↑

↓

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:02.09.2020 15:57:25

Task Category:None

Keywords:

Computer:[REDACTED]

Copy

Close

Active Directory Certificate Services denied request 356 because An attempt was made to open a Certification Authority database session, but there are already too many active sessions. The server may need to be configured to allow additional sessions. 0x8009400f (-2146877425 CERTSRV\_E\_NO\_DB\_SESSIONS). The request was for INTRA\CLIENT1\$. Additional information: Denied by Policy Module

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 356 because An attempt was made to open a Certification Authority database session, but there are already too many active sessions. The server may need to be configured to allow additional sessions. 0x8009400f (-2146877425 CERTSRV\_E\_NO\_DB\_SESSIONS). The request was for [REDACTED]  
Additional information: Denied by Policy Module

↑

↓

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:02.09.2020 14:49:07

Task Category:None


Keywords:

Computer:[REDACTED]

Copy

Close

Active Directory Certificate Services denied request 838 because Bad Length. 0x80090004 (-2146893820 NTE\_BAD\_LEN). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

 English

Page 6 of 23

GeneralDetails

Active Directory Certificate Services denied request 838 because Bad Length. 0x80090004 (-2146893820 NTE\_BAD\_LEN). The request was for Additional information: Error Constructing or Publishing Certificate

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:02.09.2020 16:08:22

Task Category:None

Keywords:

Computer:

Copy

Close

Active Directory Certificate Services denied request 34 because The certificate has invalid policy. 0x800b0113 (-2146762477 CERT\_E\_INVALID\_POLICY). The request was for INTRA\CLIENT4\$. Additional information: Error Constructing or Publishing Certificate Invalid Issuance Policies: 1.3.6.1.4.1.311.21.31

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 34 because The certificate has invalid policy. 0x800b0113 (-2146762477 CERT\_E\_INVALID\_POLICY). The request was for INTRA\CLIENT4\$. Additional information: Error Constructing or Publishing Certificate Invalid Issuance Policies: 1.3.6.1.4.1.311.21.31

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:30.06.2021 19:26:13

Task Category:None

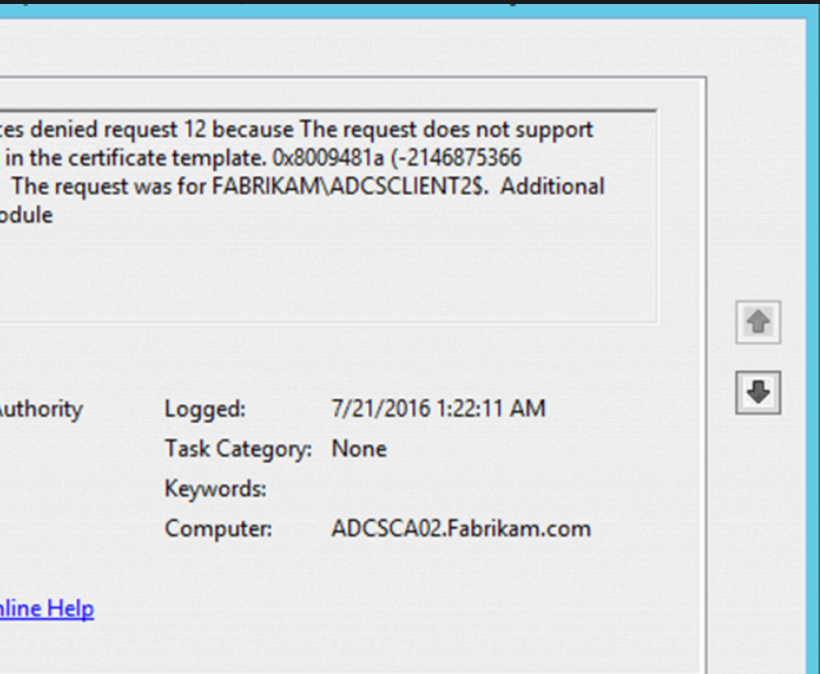
Keywords:None

Computer:ECA02.intra.adcslabor.de

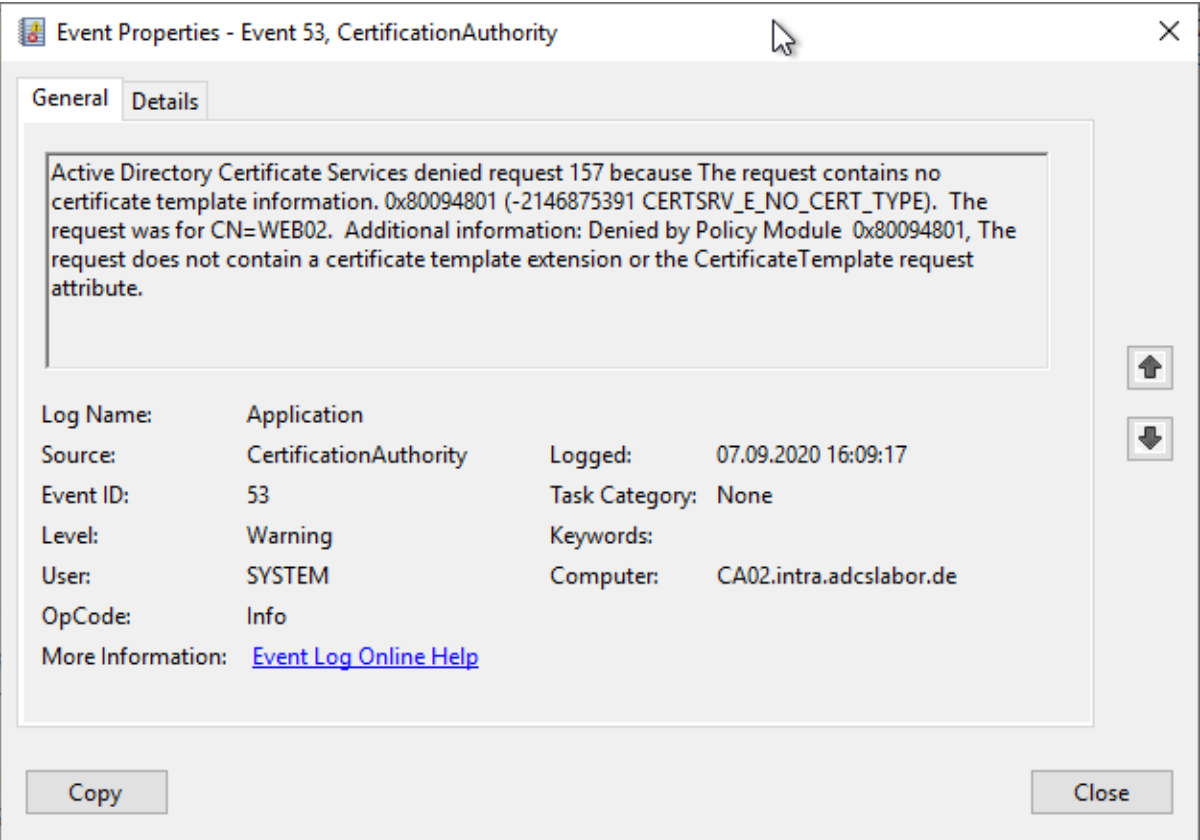
Copy

Close

Active Directory Certificate Services denied request 12 because The request does not support private key attestation as defined in the certificate template. 0x8009481a (-2146875366 CERTSRV\_E\_KEY\_ATTESTATION). The request was for INTRA\CLIENT01\$. Additional information: Denied by Policy Module



Active Directory Certificate Services denied request 157 because The request contains no certificate template information. 0x80094801 (-2146875391 CERTSRV\_E\_NO\_CERT\_TYPE). The request was for CN=WEB02. Additional information: Denied by Policy Module 0x80094801, The request does not contain a certificate template extension or the CertificateTemplate request attribute.



Active Directory Certificate Services denied request 152 because The requested certificate template is not supported by this CA. 0x80094800 (-2146875392 CERTSRV\_E\_UNSUPPORTED\_CERT\_TYPE). The request was for O=ADCS Labor, CN=www.adcslabor.de. Additional information: Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: 1.3.6.1.4.1.311.21.8.6301991.2938543.412570.1725121.735828.231.14577106.8832112(ADCS Lab Web Server).



GeneralDetails

Active Directory Certificate Services denied request 152 because The requested certificate template is not supported by this CA. 0x80094800 (-2146875392 CERTSRV\_E\_UNSUPPORTED\_CERT\_TYPE). The request was for O=ADCS Labor, CN=www.adcslabor.de. Additional information: Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: 1.3.6.1.4.1.311.21.8.6301991.2938543.412570.1725121.735828.231.14577106.8832112(ADCS Labor Web Server).

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:26.08.2020 09:45:12

Task Category:None

Keywords:

Computer:CA02.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 165405 because The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC\_S\_SERVER\_UNAVAILABLE). The request was for INTRA\DC01\$. Additional information: Denied by Policy Module

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 165405 because The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC\_S\_SERVER\_UNAVAILABLE). The request was for INTRA\DC01\$. Additional information: Denied by Policy Module

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:20.02.2020 10:12:08

Task Category:None

Keywords:

Computer:CA03.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 57 because The certification authority's certificate contains invalid data. 0x80094005 (-2146877435 CERTSRV\_E\_INVALID\_CA\_CERTIFICATE). The request was for CN=Invalid Path Length CA. Additional information: Denied by Policy Module

English

Page 9 of 23

GeneralDetails

Active Directory Certificate Services denied request 57 because The certification authority's certificate contains invalid data. 0x80094005 (-2146877435 CERTSRV\_E\_INVALID\_CA\_CERTIFICATE). The request was for CN=Invalid Path Length CA. Additional information: Denied by Policy Module

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:11.05.2020 13:14:18

Task Category:None

Keywords:

Computer:CA02.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 8 because The certificate template renewal period is longer than the certificate validity period. The template should be reconfigured or the CA certificate renewed. 0x80094814 (-2146875372 CERTSRV\_E\_CERT\_TYPE\_OVERLAP). The request was for CN=Rudi Ratlos. Additional information: Denied by Policy Module Renewing a certificate with the ADCSLaborBenutzer2 Certificate Template failed because the renewal overlap period is longer than the certificate validity period.

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 8 because The certificate template renewal period is longer than the certificate validity period. The template should be reconfigured or the CA certificate renewed. 0x80094814 (-2146875372 CERTSRV\_E\_CERT\_TYPE\_OVERLAP). The request was for CN=Rudi Ratlos. Additional information: Denied by Policy Module Renewing a certificate with the ADCSLaborBenutzer2 Certificate Template failed because the renewal overlap period is longer than the certificate validity period.

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:26.10.2020 10:01:34

Task Category:None

Keywords:

Computer:CA04.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 699 because The request is missing a required private key for archival by the server. 0x80094804 (-2146875388 CERTSRV\_E\_ARCHIVED\_KEY\_REQUIRED). The request was for CN=Testuser, E=testuser@adcslabor.de. Additional information: Denied by Policy Module

GeneralDetails

Active Directory Certificate Services denied request 699 because The request is missing a required private key for archival by the server. 0x80094804 (-2146875388 CERTSRV\_E\_ARCHIVED\_KEY\_REQUIRED). The request was for CN=Testuser, E=testuser@adcslabor.de. Additional information: Denied by Policy Module

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:06.12.2020 14:52:55

Task Category:None

Keywords:

Computer:CA02.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 110791 because One or more signatures did not include the required application or issuance policies. The request is missing one or more required valid signatures. 0x8009480b (-2146875381 CERTSRV\_E\_SIGNATURE\_REJECTED). The request was for CN=www.bla.de. Additional information: Denied by Policy Module 0x8009480b, The ADCSLaborWebServer Certificate Template requires 1 signatures, but only 0 were accepted.

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 110791 because One or more signatures did not include the required application or issuance policies. The request is missing one or more required valid signatures. 0x8009480b (-2146875381 CERTSRV\_E\_SIGNATURE\_REJECTED). The request was for CN=www.bla.de. Additional information: Denied by Policy Module 0x8009480b, The ADCSLaborWebServer Certificate Template requires 1 signatures, but only 0 were accepted.

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:29.01.2021 11:30:57

Task Category:None

Keywords:

Computer:CA02.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 110823 because The request is missing required signature policy information. 0x80094809 (-2146875383 CERTSRV\_E\_SIGNATURE\_POLICY\_REQUIRED). The request was for CN=Peter Pan. Additional information: Denied by Policy Module

GeneralDetails

Active Directory Certificate Services denied request 110823 because The request is missing required signature policy information. 0x80094809 (-2146875383 CERTSRV\_E\_SIGNATURE\_POLICY\_REQUIRED). The request was for CN=Peter Pan. Additional information: Denied by Policy Module

↑

↓

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:17.02.2021 10:16:17

Task Category:None

Keywords:

Computer:CA02.intra.adcslabor.de

Copy

Close

Active Directory Certificate Services denied request 12345 because Write lock failed due to outstanding write lock 0xc800044e (ESE: -1102 JET\_errWriteConflict). The request was for INTRA\rudi. Additional information: Denied by Policy Module Resubmitted by INTRA\Administrator

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request because Write lock failed due to outstanding write lock 0xc800044e (ESE: -1102 JET\_errWriteConflict). The request was for . Additional information: Denied by Policy Module Resubmitted by

↑

↓

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:

Task Category:None

Keywords:

Computer:

Copy

Close

Active Directory Certificate Services denied request 525317 because The specified time is invalid. 0x8007076d (WIN32: 1901 ERROR\_INVALID\_TIME). The request was for CN=somewebsite.intra.adcslabor.de. Additional information: Denied by Policy Module

GeneralDetails

Active Directory Certificate Services denied request 525317 because The specified time is invalid. 0x8007076d (WIN32: 1901 ERROR\_INVALID\_TIME). The request was for CN=somewebsite.intra.adclabor.de. Additional information: Denied by Policy Module

↑

↓

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:24.02.2022 11:19:39

Task Category:None

Keywords:

Computer:CA02.intra.adclabor.de

Copy

Close

Active Directory Certificate Services denied request 821 because The DNS name is unavailable and cannot be added to the Subject Alternate name. 0x8009480f (-2146875377 CERTSRV\_E\_SUBJECT\_DNS\_REQUIRED). The request was for CN=pki.adclabor.de. Additional information: Denied by Policy Module Resubmitted by INTRA\Administrator.

Active Directory Certificate Services denied request 12345 because The specified server cannot perform the requested operation. 0x8007003a (WIN32: 58 ERROR\_BAD\_NET\_RESP). The request was for INTRA\rudi. Additional information: Denied by Policy Module 0x8007003a, The Active Directory containing the Certification Authority could not be contacted.

Active Directory Certificate Services denied request 1234 because An internal consistency check failed. 0x8009002d (-2146893779 NTE\_INTERNAL\_ERROR). The request was for INTRA\CLIENT01\$. Additional information: Error Constructing or Publishing Certificate

Active Directory Certificate Services denied request 12345 because Bad Data. 0x80090005 (-2146893819 NTE\_BAD\_DATA). The request was for CN=Rudi Ratlos. Additional information: Error Constructing or Publishing Certificate Resubmitted by INTRA\Administrator

Event Properties - Event 53, CertificationAuthority

GeneralDetails

Active Directory Certificate Services denied request 1150499 because Bad Data. 0x80090005 (-2146893819 NTE\_BAD\_DATA). The request was for CN= . Additional information: Error Constructing or Publishing Certificate

↑

↓

Log Name:Application

Source:CertificationAuthority

Event ID:53

Level:Warning

User:SYSTEM

OpCode:Info

More Information:[Event Log Online Help](#)

Logged:

Task Category:None

Keywords:

Computer:

Copy

Close



Active Directory Certificate Services denied request 12345 because The Email name is unavailable and cannot be added to the Subject or Subject Alternate name. 0x80094812 (-2146875374 CERTSRV\_E\_SUBJECT\_EMAIL\_REQUIRED). The request was for INTRA\rudi. Additional information: Denied by Policy Module

Active Directory Certificate Services denied request 7040 because The parameter is incorrect. 0x80070057 (WIN32: 87 ERROR\_INVALID\_PARAMETER). CN=WEB01.intra.adcslabor.de. Additional information: Denied by Policy Module

Active Directory Certificate Services denied request 12345 because The request contains conflicting template information. 0x80094802 (-2146875390 CERTSRV\_E\_TEMPLATE\_CONFLICT). The request was for CN=test.adcslabor.de. Additional information: Denied by Policy Module 0x80094802, The request specifies conflicting certificate templates: 1.3.6.1.4.1.311.21.8.6301991.2938543.412570.1725121.735828.231.4136173.932265 5(ADCSLaborWebServer)/ADCSLaborWebServer.

Active Directory Certificate Services denied request 1049 because The user name or password is incorrect. 0x8007052e (WIN32: 1326 ERROR\_LOGON\_FAILURE). The request was for INTRA\WEB02\$. Additional information: Denied by Policy Module 0x8007052e, Active Directory Certificate Services could not connect to the global catalog server. CN=WEB02,OU=Server,OU=ADCSLabor Computer,DC=intra,DC=adcslabor,DC=de

## Description

### Hinweis

Do you know **TameMyCerts**? TameMyCerts is an add-on for the Microsoft certification authority (Active Directory Certificate Services). It extends the function of the certification authority and enables the [Application of regulations](#) to realize the secure automation of certificate issuance. TameMyCerts is unique in the Microsoft ecosystem, has already proven itself in countless companies around the world and is available under a free license. It can [downloaded via GitHub](#) and can be used free of charge. Professional maintenance is also offered.

Error codes that are usually part of normal Certification Authority operation:

- The public key does not meet the minimum size required by the specified certificate template. 0x80094811 (-2146875375 CERTSRV\_E\_KEY\_LENGTH).
- The permissions on the certificate template do not allow the current user to enroll for this type of certificate. 0x80094012 (-2146877422 CERTSRV\_E\_TEMPLATE\_DENIED).
- The request contains no certificate template information. 0x80094801 (-2146875391 CERTSRV\_E\_NO\_CERT\_TYPE).
- The requested certificate template is not supported by this CA. 0x80094800 (-2146875392 CERTSRV\_E\_UNSUPPORTED\_CERT\_TYPE).
- The request contains conflicting template information. 0x80094802 (-2146875390 CERTSRV\_E\_TEMPLATE\_CONFLICT).
- The request is missing a required private key for archival by the server. 0x80094804 (-2146875388 CERTSRV\_E\_ARCHIVED\_KEY\_REQUIRED).
- The DNS name is unavailable and cannot be added to the Subject Alternate name. 0x8009480f (-2146875377 CERTSRV\_E\_SUBJECT\_DNS\_REQUIRED)

- The certificate has invalid policy. 0x800b0113 (-2146762477 CERT\_E\_INVALID\_POLICY).
- The request does not support private key attestation as defined in the certificate template. 0x8009481a (-2146875366 CERTSRV\_E\_KEY\_ATTESTATION).
- The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC\_SERVER\_UNAVAILABLE).
- The certificate template renewal period is longer than the certificate validity period. The template should be reconfigured or the CA certificate renewed. 0x80094814 (-2146875372 CERTSRV\_E\_CERT\_TYPE\_OVERLAP).

Error codes that may indicate Active Directory, network, or certificate template misconfiguration:

- The EMail name is unavailable and cannot be added to the Subject or Subject Alternate name. 0x80094812 (-2146875374 CERTSRV\_E\_SUBJECT\_EMAIL\_REQUIRED).
- The request is missing required signature policy information. 0x80094809 (-2146875383 CERTSRV\_E\_SIGNATURE\_POLICY\_REQUIRED).
- The specified server cannot perform the requested operation. 0x8007003a (WIN32: 58 ERROR\_BAD\_NET\_RESP).
- Incorrect password. 0x80090033 (-2146893773 NTE\_INCORRECT\_PASSWORD).
- The user name or password is incorrect. 0x8007052e (WIN32: 1326 ERROR\_LOGON\_FAILURE).

Error codes that may indicate a malfunction of the certification authority:

- The certification authority's certificate contains invalid data. 0x80094005 (-2146877435 CERTSRV\_E\_INVALID\_CA\_CERTIFICATE).
- An internal error occurred. 0x80090020 (-2146893792 NTE\_FAIL).
- Invalid Signature. 0x80090006 (-2146893818 NTE\_BAD\_SIGNATURE).
- The security token does not have storage space available for an additional container. 0x80090023 (-2146893789 NTE\_TOKEN\_KEYSET\_STORAGE\_FULL).
- The device that is required by this cryptographic provider is not ready for use. 0x80090030 (-2146893776 NTE\_DEVICE\_NOT\_READY)
- The signature of the certificate cannot be verified. 0x80096004 (-2146869244 TRUST\_E\_CERT\_SIGNATURE).
- The parameter is incorrect. 0x80090027 (-2146893785 NTE\_INVALID\_PARAMETER).
- An attempt was made to open a Certification Authority database session, but there are already too many active sessions. The server may need to be configured to allow additional sessions. 0x8009400f (-2146877425 CERTSRV\_E\_NO\_DB\_SESSIONS).
- Bad Length. 0x80090004 (-2146893820 NTE\_BAD\_LEN).
- Bad Data. 0x80090005 (-2146893819 NTE\_BAD\_DATA).

Often the cause is a malfunction of the hardware security module.

## Error code NTE\_BAD\_DATA

If a SafeNet Hardware Security Module (HSM) is used, this error can occur if the network connection to the HSM is lost and the certification authority can no longer access the private key.

[\(-2146893819 NTE\\_BAD\\_DATA\)."](#)),,

In the same context, events no. [86](#), [88](#) and [130](#) occur.

## Error code CERTSRV\_E\_TEMPLATE\_CONFLICT

Occurs if the submitted certificate request includes a Certificate Template Information extension that designates a certificate template for issuance, but [a different certificate template is selected when submitting the certificate request](#).

## Error code CERTSRV\_E\_TEMPLATE\_DENIED

Occurs when the requesting user or computer is not authorized to request a certificate for this certificate template.

This can also occur with autoenrollment or application through the Microsoft Management Console (MMC) if the authorization to apply is through a security group and the applying user or computer has not yet re-logged in since being added to the group (for computers, this requires a reboot).

The reason is that the client-side authorization check is done using a directory query, but the actual authentication is done using a Kerberos ticket, in which the group membership is not yet mapped.

## Error code CERTSRV\_E\_NO\_CERT\_TYPE

This error occurs, [when a certificate request has been sent to the certification authority](#) but no specification about the desired certificate template was made.

The certificate template is mandatory information. It must be specified either via an attribute within the certificate request or during submission.

When submitting the certificate request using certreq.exe, the desired certificate request can be specified with the -attrib argument:

```
certreq -attrib "CertificateTemplate:{name-of-the-certificate-template}" -
submit {certificate-request}.req
```

## Error code CERTSRV\_E\_UNSUPPORTED\_CERT\_TYPE

This error occurs when a certificate request was sent to the certification authority, [which contains an attribute for the certificate template or which was specified when the certificate request was submitted](#), but this is either incorrect (e.g. typing error) or the desired certificate template was not published on this certification authority (e.g. because the certificate request was sent to the wrong certification authority).

Also occurs when the certificate authority does not have read permission on a published certificate template. By default, the certificate authority obtains read permission through the Authenticated Users entry in the certificate template's security settings.

Subject Name

Issuance Requirements

General

Compatibility

Request Handling

Cryptography

Key Attestation

Superseded Templates

Extensions

Security

Server

Group or user names:

Administrator (Administrator@intra.adcslabor.de)

Authenticated Users

Domain Admins (INTRA\Domain Admins)

Domain Users (INTRA\Domain Users)

Enterprise Admins (INTRA\Enterprise Admins)

Add...

Remove

Permissions for Authenticated Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

OK

Cancel

Apply

Help

## Error code CERTSRV\_\_E\_\_KEY\_\_LENGTH

This error occurs if the key length within the certificate request is smaller than the minimum size defined in the certificate template. This can occur especially with manually generated certificate requests.

The solution is to select an appropriate key size as early as the application stage and thus when generating the key pair. Alternatively, the key size can be reduced in the certificate template. Please note, [that the key algorithm used is not verified by the certification authority's policy module](#)i.e., a certificate template with a low key length that accepts both RSA and ECC keys is technically feasible.

## Error code CERTSRV\_\_E\_\_KEY\_\_ATTESTATION

This error occurs when [Trusted Platform Module \(TPM\) Key Attestation](#) is configured, and a certificate request is received for which either no corresponding endorsement key or no certification authority certificate corresponding to the endorsement certificate is stored on the certification authority. See also article "[Configuring the Trusted Platform Module \(TPM\) Key Attestation](#)",.

## Error code RPC\_\_S\_\_SERVER\_\_UNAVAILABLE

This error occurs when a certificate is requested for a domain controller, the certificate template contains the flag [CT\\_FLAG\\_SUBJECT\\_ALT\\_REQUIRE\\_DOMAIN\\_DNS](#) and the certificate authority cannot connect to the domain controller via RPC named pipes. See article "[Requesting a certificate for domain controller fails with error message "The RPC server is unavailable. 0x800706ba \(WIN32: 1722 RPC\\_SERVER\\_UNAVAILABLE\)"](#)",.

## Error code CERT\_\_E\_\_INVALID\_\_POLICY

Extended Key Usage (EKU) or an Issuance Policy that is not permitted for the certification authority - i.e. that the requested policy OID is not present in the certification authority certificate and thus may not be issued by it.

This can occur in the following cases, among others:

- The certificate template used is required for the registration of a [Extended Key Usage \(EKU\)](#) configured in the issued certificate, [However, the certification authority is restricted to certain Extended Key Usages](#) and does not include the desired EKU.
- The certificate template used is configured to include a certificate policy OID in the issued certificate, but the certification authority certificate does not include it.
- The certificate template used is for [Trusted Platform \(TPM\) Key Attestation](#) and the option "Include issuance policies for enforced attestation types" is configured, but the certification authority certificate does not include it. See article "[Include the issuance policies for Trusted Platform \(TPM\) Key Attestation in a certification authority certificate.](#)" as well as "[Frequently Used Extended Key Usages and Issuance Policies](#)",,

## Error code CERTSRV\_\_E\_\_INVALID\_\_CA\_\_CERTIFICATE

Basically, this error occurs when the certification authority certificate has a certificate policy (Issuance Policy) or restriction (Application Policy) or a path length constraint that conflicts with the requested certificate. Examples may include:

- The certification authority certificate has a path length constraint and a subordinate certification authority certificate is requested
- The certificate policy (issuance policy) on a root certification authority was changed when the certification authority certificate was renewed

See article "[Certificate authority certificate request fails with error message "The certification authority's certificate contains invalid data. 0x80094005 \(-2146877435 CERTSRV\\_\\_E\\_\\_INVALID\\_\\_CA\\_\\_CERTIFICATE\)"](#)",,

## Error code NTE\_\_INTERNAL\_\_ERROR

Occurs, among other things, when there is a problem accessing a private key of the certification authority (e.g. in case of problems with a hardware security module, (especially if the Cavium Key Storage Provider of the [AWS CloudHSM](#) is used).

See also Events [100](#) and [130](#).

## Error code CERTSRV\_\_E\_\_SUBJECT\_\_EMAIL\_\_REQUIRED

Occurs when the underlying certificate template is configured to write an email address in the subject of the issued certificate, but the requesting user account does not have an email address stored in Active Directory.

This can occur with administrative accounts, among others, as they often do not have a configured email address. If there is a certificate template that has configured



[AutoEnrollment process](#)) tries to apply for a certificate, which will fail and thus (depending on the number of accounts affected) result in a [enormous growth of the Certification Authority database](#) can lead.

## Error code CERTSRV\_E\_NO\_DB\_SESSIONS

Occurs when there are too many concurrent connections to the certificate authority database - usually because a very large number of certificate requests are being processed.

See article "[Certificate or revocation list issuance fails with error code CERTSRV\\_E\\_NO\\_DB\\_SESSIONS](#)".

May also indicate a Denial of Service (DoS) attack.

## Error code JET\_errWriteConflict

Occurs when there are too many concurrent connections to the certificate authority database - usually because a very large number of certificate requests are being processed.

See also error code CERTSRV\_E\_NO\_DB\_SESSIONS.

For more information see article "[Certificate or revocation list issuance fails with error code CERTSRV\\_E\\_NO\\_DB\\_SESSIONS](#)".

May also indicate a Denial of Service (DoS) attack.

## Error code CERTSRV\_E\_CERT\_TYPE\_OVERLAP

Occurs when the timely renewal of the certification authority certificate was missed. Towards the end of the validity of the certification authority certificate, the issued certificates are truncated in their validity periods (see [Event no. 97](#)) and finally certificates are requested which would be valid for a shorter period than the renewal period configured in the certificate template (if this would exceed the remaining validity of the certification authority certificate).

## Error code CERTSRV\_E\_SIGNATURE\_REJECTED

Occurs when a certificate template requires a signature (Issuance Requirements tab) and this signature cannot be verified, for example...

- if the certification authority that issued the signature certificate is not approved for Extended Key Usage or Issuance Policy for this purpose (e.g. due to constraints in the certification authority certificate)
- if the certification authority that issued the signature certificate does not have a trust status on the issuing certification authority

issued by another certification authority. It will be accepted as long as it is classified as trustworthy.

## Error code CERTSRV\_E\_SIGNATURE\_POLICY\_REQUIRED

Occurs when the certificate template requires the certificate request to have a certificate enrollment agent signature, but the submitted certificate request does not contain one.

See also article "[Certificate request fails with error message "The request is missing required signature policy information. 0x80094809 \(-2146875383 CERTSRV\\_E\\_SIGNATURE\\_POLICY\\_REQUIRED\)".](#)".

## Error code CERTSRV\_E\_SUBJECT\_DNS\_REQUIRED

Occurs when a certificate template (usually for computer certificates) is configured to form the Subject Distinguished Name or the Subject Alternative Name from the Active Directory and to enter the DNS name of the requester in the issued certificate. The error message states that the **requesting** account does not have a DNS name (the [dNSHostName](#) attribute on the Active Directory object is not populated).

Also occurs when an administrator manually submits a certificate request against such a certificate template (a user account usually does not have a dNSHostName attribute).

## Error code CERT\_E\_INVALID\_POLICY

Attempts have been made to issue a certificate that would have [Restrictions on the Extended Key Usage of the Certification Authority Certificate](#) (Qualified Subordination, also Extended Key Usage Constraints) is violated.

The certification authority certificate contains a list of allowed Extended Key Usages that the reported Extended Key Usage does not contain. The enhanced key usages are taken from the certificate template and overwrite any attributes in the certificate request.

## Error code ERROR\_INVALID\_TIME

Occurs when the EDITF\_ATTRIBUTEENDDATE flag is enabled on the certification authority to [To be able to issue certificates with a shortened validity period](#), and an invalid date was requested in the certificate request.

## Safety assessment


Begriffsdefinition

The security assessment is based on the three dimensions of confidentiality, integrity and availability.

be an indication that availability is impaired.

The error code CERT\_E\_INVALID\_POLICY may indicate an attack attempt and should possibly be alerted.



## Microsoft rating

Microsoft evaluates this event in the [Securing Public Key Infrastructure \(PKI\)](#)  Whitepaper with a severity score of "Low".

## Related links:

- [Overview of Windows events generated by the certification authority](#)
- [Overview of audit events generated by the Certification Authority](#)
- [\(Mass\) deletion of entries in the certification authority database \(certificates, requirements, revocation lists\)](#)
- [Send a manually created certificate request to a certification authority](#)

## External sources

- [Event ID 53 - AD CS Certificate Request \(Enrollment\) Processing](#) (Microsoft)
- [Securing Public Key Infrastructure \(PKI\)](#)  (Microsoft)
- [A Certification Authority can't use a certificate template](#)  (Microsoft)

---

## 16 thoughts on “Details zum Ereignis mit ID 53 der Quelle Microsoft-Windows-CertificationAuthority”

---

Pingback: [Issuing of certificates or revocation lists fails with error code CERTSRV\\_E\\_NO\\_DB\\_SESSIONS](#) - Uwe Gradenegger

---

Pingback: [Certificate authority certificate request fails with error message "The certification authority's certificate contains invalid data. 0x80094005 \(-2146877435 CERTSRV\\_E\\_INVALID\\_CA\\_CERTIFICATE\)"](#) - Uwe Gradenegger

---

Pingback: [Requesting a certificate for domain controller fails with error message "The RPC server is unavailable. 0x800706ba \(WIN32: 1722 RPC\\_SERVER\\_UNAVAILABLE\)"](#) - Uwe Gradenegger

---

Pingback: [Details about the event with ID 13 of the source Microsoft-Windows-CertificateServicesClient-CertEnroll](#) - Uwe Gradenegger

Pingback: [Certificate request fails with error message "The requested certificate template is not supported by this CA. 0x80094800 \(-2146875392 CERTSRV\\_E\\_UNSUPPORTED\\_CERT\\_TYPE\)." - Uwe Gradenegger](#)

---

Pingback: [Certificate request fails with error message "The request is missing required signature policy information. 0x80094809 \(-2146875383 CERTSRV\\_E\\_SIGNATURE\\_POLICY\\_REQUIRED\)" - Uwe Gradenegger](#)

---

Pingback: [Certificate request fails with error message "Bad Data. 0x80090005 \(-2146893819 NTE\\_BAD\\_DATA\)." - Uwe Gradenegger](#)

---

Pingback: [Details about the event with ID 57 of the source Microsoft-Windows-CertificationAuthority - Uwe Gradenegger](#)

---

Pingback: [Troubleshooting for automatic certificate request \(autoenrollment\) via RPC/DCOM - Uwe Gradenegger](#)

---

Pingback: [Configuring the Trusted Platform Module \(TPM\) Key Attestation - Uwe Gradenegger](#)

---

Pingback: [Performing a functional test for a Certification Authority - Uwe Gradenegger](#)

---

Pingback: [A policy module to tame them: Presentation of the TameMyCerts Policy Module for the Microsoft Certification Authority - Uwe Gradenegger](#)

---

Pingback: [About the option "Build this from Active Directory information" for certificate templates - Uwe Gradenegger](#)

---

Pingback: [Details about the event with ID 100 of the source Microsoft-Windows-CertificationAuthority - Uwe Gradenegger](#)

---

Pingback: [Details about the event with ID 130 of the source Microsoft-Windows-CertificationAuthority - Uwe Gradenegger](#)

---

Pingback: [Certificate request fails with error message "The certificate request could not be submitted to the certification authority. Error: The RPC server is unavailable. 0x800706ba \(WIN32: 1722 RPC\\_S\\_SERVER\\_UNAVAILABLE\)" - Uw](#)

---

Comments are closed.

PREVIOUS

## Details of the event with ID 52 of the source Microsoft-Windows-CertificationAuthority

NEXT

## Details of the event with ID 63 of the source Microsoft-Windows-CertificationAuthority

Copyright Uwe Gradenegger. All rights reserved. Information without guarantee. / Privacy policy