Certification Service

Error Code 43001

Problem
Failed to process request - certification profile attributes not found

Reason
This problem occurs when the certification profile does not find some or any of the attribute from the certification request or database.

Solution
Edit the specified profile using the ADSS Server Console and click the Update button so that all attributes can be stored in the database. Restart the certification service for the changes to take into effect.

Error Code 43002

Problem
Failed to process request - certificate alias is missing in the request

Reason
This problem occurs when the alias is missing for the CREATE, REVOKE, RECOVER, CHANGEPASSWORD, RENEW, DELETE requests.

Note that this error only occurs when the request is sent over the Ascertia's XML protocol. You do not need to specify the alias for the CREATE request over CMC protocol.

Solution
Following are the possible solutions to this problem:

- Provide the alias if it is a CREATE request
- While you can also provide the certificate in the request if it is other than CREATE request

---

Error Code 43003

Problem
Failed to process request - the request contains insufficient information

Reason
This problem occurs when any of the mandatory information is missing in any of the certification request types. e.g. old or new password is missing in the ChangePassword request.

Solution
Provide the missing information in the request in order to successfully process the request

---

Error Code 43004

Problem
Failed to process request - the request contains an invalid old password for PKCS#12/PFX

Reason
This error occurs when the incorrect old password is provided in the ChangePassword request.

Solution
Provide the correct old password while processing the ChangePassword request to change the password of the PFX/PKCS#12

Error Code 43005

Problem
Failed to verify PKCS#10 certificate a request

Reason
This error occurs when incorrect PKCS#10 is sent to ADSS Certification Service

Solution
|Provide the correct/valid PKCS#10 file in request to ADSS Certification Service

---

Error Code 43006

Problem
Failed to process request - certificate alias does not belong to the specified client

Reason
This error occurs when the user specifies an alias in the REVOKE, RENEW, REVOKE, CHANGEPASSWORD, or RECOVER request and that certificate is issued by another client.

Solution
Provide the correct client in above mentioned requests if you want to proceed with any action

---

Error Code 43007

Problem
Failed to process request - certificate does not belong to the specified client

Reason
This error occurs when the user puts the certificate in the REVOKE, RENEW, REVOKE, CHANGEPASSWORD, or RECOVER request and that certificate is issued by another client.

Solution
Provide the correct client in above mentioned requests if you want to proceed with any action

---

Error Code 43008

Problem
Failed to process request - a certificate with ACTIVE status cannot be deleted

Reason
If "ENABLE_VALID_CERTIFICATE_DELETION" is set to FALSE in [ADSS-Server-Installation-Dir.]/conf/system.properties file then you can not delete a certificate issued by the local CA but a certificate issued by external CA can be deleted regardless of this property.

Solution
Following are the possible solutions to this problem:

- Revoke the certificate instead of deleting if you do not wish to use this certificate anymore
- If you wish to remove this certificate from the ADSS Server then set the "ENABLE_VALID_CERTIFICATE_DELETION" property to TRUE in [ADSS-Server-Installation-Dir.]/conf/system.properties file and restart the ADSS Server Service instance from Windows Services Panel or UNIX daemon to take the changes into effect and then execute the DELETE request.

Error Code 43009

Problem
An internal error occurred while processing the request - see the certification service debug logs for details

Reason
This error occurs when any unseen event occurs while processing any type of certificate request.

Solution
Make sure that database and network are available and then retry with the request.

Error Code 43011

Problem
Failed to process request - requested certificate alias already exists

Reason
This error occurs while processing the certificate creation request if certificate alias provided in the request already exists in the ADSS Certification Service.

Solution
Provide a different certificate alias to identify each certificate uniquely.

Error Code 43012

Problem
Failed to delete certificate - see the certification service debug logs for details

Reason
This error occurs when the system fails to delete a certificate due any unseen affair. e.g. database became unavailable while deleting the certificate etc

Solution
Make sure that database and network is available and then retry to delete the certificate *(NR)*

Error Code 43013

Problem
An internal error occurred while authenticating/authorising the client request - see the certification service debug logs for details

Reason

This error occurs when the system is unable to authenticate the user request.

Solution
You need to make sure that:

- The Client name is correct
- Profile name is correct. It should be in the format adss:certification:profile:001 *(NR)*

Error Code 43014

Problem
Failed to process request - certification service license is expired

Reason
This error occurs when the license for the service is expired. Expiry based on two factors, either the specified transactions count in the license is reached or the contractual time is elapsed.

Solution
Ask Ascertia Ltd. for a renewed license at: sales@ascertia.com.

Error Code 43015

Problem
Failed to process request - certification service is stopped

Reason
This error occurs when certification service is stopped.

Solution
Start the certification service from Service Manager to entertain the certification service requests.
Note that if no certification profile exists in the system then service will not be started. You need to create a certification profile in order to start the service.

Error Code 43016

Problem
Failed to process request - certification service is not enabled in license

Reason
This error occurs when you send a certification request to the service and it is not licensed according to the contract.

Solution
If you wish to enable this service in the license then contact Ascertia Ltd. at: sales@ascertia.com

---

Error Code 43017

Problem
Failed to process request - a valid subject DN could not be composed

Reason
This error occurs when all attributes in Subject Distinguished Name field in certification profile is set overridable and the client does not provide any RDN in the request

Solution
Provide the subject DN in the certification request to get the certificate issued

---

Error Code 43018

Problem
Failed to revoke certificate - see the certification service debug logs for details

Reason
This error occurs when the system fails to revoke a certificate due to any unseen affair. e.g. database became unavailable while inserting the revocation information etc

Solution
Make sure that database and network is available and then retry to revoke the certificate *(NR)*

Error Code 43019

Problem
Failed to process request - the request must be signed

Reason

This error occurs when "Client request messages must be signed" checkbox is checked on the Certification Service > Service Manager page and client request is unsigned.

Solution
The solution to this problem is to send a signed certification request and the issuer of the signer certificate must be trusted in ADSS Server.

Error Code 43020 (NR)

Problem
Failed to verify certification request signature

Reason

Solution

Error Code 43021

Problem
Failed to process request - the request does not comply with Ascertia certification XML schema

Reason
This error occurs when user send the request to the certification and it is not according to the Ascertia's XML schema.

Solution
Make the request according to the schema. The schema for the certification service can be found at:
<ADSS-Server-Installation-Dir.>/service/schemas directory.

Error Code 43022

Problem
Failed to process request - certificate issued by an external CA cannot be revoked

Reason
This error occurs when the user tries to revoke a certificate that is issued by an external CA. External CA could be another instance of ADSS Server or Microsoft CA. You can not revoke a certificate in either case.

Solution
Send a direct revocation request to the ADSS Server or Microsoft CA because if front end ADSS Server revokes a certificate, it will not become the part of CRL.

Error Code 43023

Problem
Failed to process request - certificate is already revoked

Reason
This error occurs when the user tries to revoke and already revoked the certificate.

Solution
Do not revoke the certificate anymore

Error Code 43024

Problem
Failed to change PKCS#12/PFX password - see the certification service debug logs for details

Reason
This error occurs when system fails to change the password of a certificate due any unseen affair. e.g. database became unavailable while updating the record after changing the password of PFX etc.

Solution
Make sure that database and network is available and then retry to change the password the PFX *(NR)*

Error Code 43025 (needs to be tested with MS CA)

Problem
Failed to process request - certificate issued by an external CA cannot be renewed

Reason

Solution

Error Code 43026

Problem
Failed to process request - revoked certificate cannot be renewed

Reason
This error occurs when the user tries to renew a revoked certificate

Solution
Possible for this problem could be:

- Reinstate the certificate if it is revoked with holdInstructionCode and then try to renew
- Get a new certificate issued by the certification service

Error Code 43027

Problem
Failed to process request - PKCS#10 CSR does not comply with the certification profile

Reason
This error occurs when the client application is sending a PKCS#10 CSR and it not compliant with certification profile e.g.

- Key algorithm configured in the profile is different than the PKCS#10 algorithm. Also it is not marked as overridable.
- Key size configured in the profile is different than the PKCS#10 key size. Also it is not marked as overridable.
- Validity period configured in the profile is different than the PKCS#10 validity period. Also it is not marked as overridable.

Solution
Either send a PKCS#10 request according to the profile or mark the End-entity Key Type, End-entity Key Size and Validity Period overridable.

Error Code 43029 (not reproducible)

Problem
Failed to renew certificate the old key pair does not exist

Reason

Solution

Error Code 43030

Problem
Failed to save certificate in database - see the certification service debug logs for details

Reason
This error occurs when system fails to insert the record after certificate generation in database. e.g. database became unavailable while inserting the certificate etc

Solution
Make sure that database and network is available and then retry to generate the certificate *(NR)*

Error Code 43031

Problem
Failed to process request - certificate is already on hold

Reason
This error occurs when one tries to revoke a certificate with holdInstructionCode that is already revoked with holdInstructionCode.

Solution
If you want to revoke this certificate permanently then use some other revocation reason code and if you want to make it active then send revoke request with removeFromCRL revocation reason.

Error Code 43032

Problem
Failed to process request - certificate is not revoked

Reason
This error occurs when one tries to remove a certificate from the CRL with revocation reason "removeFromCRL" and the certificate is not in the CRL.

Solution
Nothing

Error Code 43033

Problem
Failed to process request - invalid revocation reason or hold instruction code

Reason
This error occurs when the user is specifying an invalid revocation or hold instruction code in the certification request

Solution
Provide correct revocation or hold instruction code in the revocation request. Follow the link for correct revocation and hold instruction codes: Revocation Reason Codes

---

Error Code 43034

Problem
Failed to process request - PKCS#12/PFX is not found in the database

Reason
This error occurs when PKCS#12 is not found in the database while renewing a certificate

Solution
This certificate cannot be renewed.

Error Code 43035

Problem
Failed to process request - the request does not contain PKCS#12/PFX password

Reason
This error occurs when you are renewing a certificate and "**Renew certificate using existing key pair**" option is selected in the profile

Solution
Following are the possible solutions to this problem:

- Provide the PFX is the request in order to renew the certificate or
- Renew a certificate with a new key pair by selecting the option " **Renew certificate using new key pair**" in the profile

---

Error Code 43036 (not reproducible)

Problem
Invalid or unsupported CMC request type

Reason

Solution

Error Code 43037

Problem
Failed to generate serial number for CMC certificate - see the certification service debug logs for details

Reason
This problem occurs when ADSS Server fails to generate serial number for a CMC request certificate due to any internal error.

Solution
Restart the ADSS Certification Service from Service Manager and then resend the request for certification generation.

Error Code 43038

Problem
Failed to process request - issuer DN in the request does not match with issuer DN found in the certificate

Reason
This error occurs when issuer DN specified in the CMC revocation request does not match with the issuer DN found in the target certificate.

Solution
Correct the issuer DN in the request.

Error Code 43039

Problem
Failed to process request - expired certificate cannot be revoked

Reason
This error occurs when the client tries to revoke an expired certificate

Solution
You can delete an expire certificate but can revoke it so send the DELETE request to the service if you do not want to keep within the system

---

Error Code 43040

Problem
Failed to process request - revoked certificate cannot be renewed

Reason
This error occurs when the user tries to renew a revoked certificate

Solution
Possible for this problem could be:

- Reinstate the certificate if it is revoked with holdInstructionCode and then try to renew
- Get a new certificate issued by the certification service

Error Code 43041

Problem
Failed to process request - Manage CAs module is not enabled in license

Reason
This error occurs when Manage CAs module that used to configure the CAs is not enabled in the license. If this module is not licensed then certification service cannot generate the certificate.

Solution
Ask Ascertia Ltd. for new license at sales@ascertia.com that have Manage CAs module enabled.

Error Code 43042

Problem
Failed to authorise request - given profile is not allowed to the client

Reason
This error occurs when profile given in the certification request is not assigned to the client specified in the request.

Solution
There are two possible solutions to this error:

- Use any of the profile that is assigned to the specified client
- Assign this profile to this client from Client Manager if deemed necessary

---

Error Code 43043

Problem
Failed to authenticate client - SSL client authentication certificate does not match with the configured client authentication certificate

Reason
This error occurs when the user is sending the certification request over SSL client authentication and that certificate is different from the one configured in the Client Manager module for the target client.

Solution
Following are the possible solutions to this problem:

- Use the correct SSL client authentication certificate that is configured in the Client Manager
- Send the request over plain HTTP protocol using 8777 port

Error Code 43045 (NR)

Problem
Invalid CMC enrolment request contents

Reason

Solution

Error Code 43046 (NR)

Problem
Invalid CMC revocation request contents

Reason

Solution

Error Code 43047 (NR)

Problem
Invalid PKCS#10 certificate signing request

Reason

Solution

Error Code 43048

Problem
Failed to process request - PKCS#10 CSR is missing in the request

Reason
This error occurs when certification profile is configured to accept PKCS#10 (**$pkcs10** is set in the **Subject Distinguished Name** field of certification profile) from the client application and client does not provide the PKCS#10 in the certification request. Follow the link for more details to set the Subject Distinguished Name: Certification Service > Certification Profile

Solution
Provide the PKCS#10 in the certification request to issue the certificate

---

Error Code 43049

Problem
Failed to process request - CA configured in the requested profile is inactive

Reason
This error occurs when the CA configured in the target certification profile is marked as inactive because an inactive CA cannot issue the certificates

Solution
Use a different profile in which an active CA is configured

Error Code 43050

Problem
Failed to authorise request - certification service is not allowed to this client

Reason
This error occurs when "**Allow this client to access the ADSS Certification Service**" in unchecked for the client specified in the request in Client Manager module

Solution
The solution to this problem is to check the above mentioned checkbox in Client Manager module, then restart the ADSS Certification Service for the changes to take into effect and then send the certification request.

Error Code 43051

Problem
Failed to process request - a certificate with NotYetValid status cannot be revoked

Reason
This error occurs when the user tries to revoke a certificate whose Valid From date is in future.

Solution
You need to wait for the certificate to get it validated.

Error Code 43052

Problem
Failed to process request - a certificate with NotYetValid status cannot be deleted

Reason
This error occurs when **ENABLE_VALID_CERTIFICATE_DELETION = FALSE** in [ADSS-Server-Dir.]/conf/system.properties file. It means that one cannot delete a valid certificate with status ACTIVE and NotYetValid. You can only delete the certificates with EXPIRE status

Solution
Following are the possible solutions for this problem:

- Set the property **ENABLE_VALID_CERTIFICATE_DELETION = TRUE** in [ADSS-Server-Dir.]/conf/system.properties file - restart the ADSS Server Service instance from the Windows Services Panel or UNIX daemon for the changes to take into effect and then send the DELETE request.
- You can either revoke the certificate

Error Code 43053

Problem
Failed to process request - certification service is not enabled in the system

Reason
This error occurs when property **ENABLE_SERVICE = FALSE** in [ADSS-Server-Dir.]/service/certification.properties file.

Solution
Set the property **ENABLE_SERVICE = TRUE** in [ADSS-Server-Dir.]/service/certification.properties file if you wish to enable this service.

Error Code 43054

Problem
Failed to process request - key size is not supported

Reason
This error occurs when key size provided in the certification request is not supported by the ADSS Server.

Solution
Following are the supported key sizes by ADSS Server:

- **RSA:** 1024, 2048, 3072, 4096
- **ECDSA:** 192, 224, 256, 384, 521

Error Code 43055

Problem
Failed to authorise request - certification profile is inactive

Reason
This error occurs when the profile specified in the request is marked inactive. This error could also occur if no profile is specified in the request but default profile in the target client is marked as inactive.

Solution
Use any of the active profile

Error Code 43056

Problem
Failed to authorise request - certification profile does not exist

Reason

This problem occurs when the certification profile specified in the request does not exist on ADSS Server.

Solution
Following are the possible resolutions for this problem:

- Verify that profile ID/name is not misspelled. Profile ID should be in the format "adss:certification:profile:000"
- Ask ADSS Server Console operator to create a new certification profile that you are using or
- Use any of the existing certification profile in the request

---

Error Code 43058

Problem
Failed to process request - subject DN in the request does not match subject DN pattern defined in certification profile

Reason
This error occurs when the checkbox "" is checked in the certification profile. When this checkbox is checked then service verifies that subject DN provided in the request matches the subject DN pattern defined in certification profile. Follow the link for more details about pattern matching: Certification Service > Certification Profile

Solution
Send the certification request according to the pattern defined in the target certification profile in order to get the certificate issued.

Error Code 43059

Problem
Failed to process request - subject DN is missing in the request

Reason
This error occurs when certification profile is configured to accept any subject DN (**$request** is set in the **Subject Distinguished Name** field of certification profile) from the client application and client does not provide the subject DN in request. Follow the link for more details to set the Subject Distinguished Name: Certification Service > Certification Profile

Solution
Provide the subject DN in the certification request to issue the certificate.

Error Code 43060

Problem
Failed to process request - default profile not configured and neither found in the request

Reason
This error occurs when no default certification profile is configured in the target client and neither provided through certification request.

Solution
Either configure a default profile against the target client or provide the profile ID/name in the certification request. Certification profile ID format is "adss:certification:profile:000"