Signing Service

Error Code 41001

Problem
Failed to process request - Signing service not enabled in license

Reason

This error occurs when you send a signing 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 41002

Problem
Failed to process request - Signing service license has 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
If you wish to enable this service in the license then contact Ascertia Ltd. at: sales@ascertia.com

---

Error Code 41003

Problem
Failed to process request - Signing service is stopped

Reason
This error occurs when signing service is stopped.

Solution

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Service Manager**
3. Start the signing service to entertain the signing service requests
4. If no signing profile exists in the system then service will not be started. You need to create a signing profile in order to start the service.

Error Code 41004

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

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

Solution

1. Check the signing service logs for more details from location: **[ADSS Server Installation Directory]/logs/signing/signing.log**
2. Make sure that database and network is available.
3. In case you did not find any clue then export the ADSS Server logs using Trace Logs Export Utility and send it to support@ascertia.com.

Error Code 41005

Problem
Failed to create signature

Reason
This error occurs when ADSS Server failed to generate a signature

Solution
Export the ADSS Server logs using Trace Logs Export Utility and send it to support@ascertia.com.

Error Code 41006

Problem
Failed to create visible signature

Reason
This error occurs when ADSS Server failed to generate visible PDF signature

Solution
Export the ADSS Server logs using Trace Logs Export Utility and send it to support@ascertia.com.

Error Code 41007

Problem
Failed to create invisible signature

Reason
This error occurs when ADSS Server failed to generate invisible PDF signature

Solution
Export the ADSS Server logs using Trace Logs Export Utility and send it to support@ascertia.com.

Error Code 41008

Problem
Failed to create PKCS#7 signature

Reason
This error occurs when ADSS Server failed to generate PKCS#7 signature

Solution
Export the ADSS Server logs using Trace Logs Export Utility and send it to support@ascertia.com.

Error Code 41009

Problem
Failed to get a timestamp to embed in the digital signature

Reason
This error occurs when the timestamp authority is not available

Solution

1. Launch the ADSS Server console:
2. Go to location: **Signing Service > Signing Profiles**
3. Edit your relevant profile and go to the **Signature Settings** page
4. Ensure that the timestamping authority configured or selected there
5. Navigate to location **Global Settings > Timestamping**
6. Select the relevant timestamping authority (which was referred in the signing profile) and click on the **Test TSA** button and check the results:
    a. If the system failed to connect with the timestamping authority then try to run the timestamping URL in any Web browser on the same server where ADSS Server is deployed.
        i. if you are not able to connect with the URL using Web browser then contact with your network manager for the solution.
        ii. If you are able to connect then confirm with your network manager whether there is any proxy server involved in the network etc. If a proxy server is involved in the network then follow these steps to enable the proxy settings for the ADSS Server
            1. Launch the ADSS Server console:
            2. Go to location: **Global Settings > Miscellaneous**
            3. Under the proxy settings section enable the check box Enable Proxy and configure the proxy credentials accordingly and restart the ADSS Server accordingly.
    b. If the received response status is other than **Granted** then contact with your timestamping service provider.
    c. If ADSS Server is unable to **verify TSA using local trust anchors** then navigate to **Trust Manager** screen and ensure that the complete certificate chain for the TSA authority is registered there
        i. If issuer chain is not registered then register the complete certificate chain and restart the ADSS Server accordingly
        ii. If issuer chain is registered then navigate to **CRL Monitor > CRL Details** screen and confirm that the latest CRLs for the relevant CAs are available there.

Error Code 41010

Problem
Failed to embed revocation information

Reason
This error occurs when ADSS Server failed to get the revocation information for the signer/ timestamping authority certificate chain

Solution

1. Launch the ADSS Server console
2. Navigate to **Trust Manager** screen and ensure that
    a. If the the issuer chain is not registered then register the complete certificate chain and restart the ADSS Server accordingly
    b. If the validation policy of the Issuer certificate chain is:

i. **Local CRL Cache** then navigate to CRL Monitor > CRL Details screen and confirm that the latest CRLs for the relevant CAs are available there
ii. **Configured OCSP Address** then ensure that configured OCSP address is accessible by clicking on the Test button
iii. **CDP / AIA** then ensure that you can access CDP / AIA path on any web browser on the same server where ADSS Server is deployed.

In case you are unable to resolve this issue then export the ADSS Server logs using Trace Logs Export Utility and send it to support@ascertia.com.

Error Code 41011

Problem
Failed to embed archive timestamp token

Reason
This error occurs when singing service is somehow unable to get the timestamp token from TSA service.

Error Code 41012

Problem
Failed to process request - PDF signing not enabled

Reason
This error occurs when PDF signature type is not enabled in the license in signing service module.

Solution

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

---

Error Code 41013

Problem
Failed to process request - embedded timestamped signature creation not enabled in license

Reason

This error occurs when embedded timestamped signature type is not enabled in the license in signing service module.

Solution

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

---

Error Code 41014

Problem
Failed to process request - long term signature creation is not enabled in license

Reason

This error occurs when long term signature type is not enabled in the license in signing service module.

Solution

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

---

Error Code 41016

Problem
Failed to embed revocation information

Reason

Solution

Error Code 41017

Problem
Failed to create XAdES-X type 2 signature

Reason

Solution

Error Code 41020

Problem
Failed to process request - there is no Originator Id in the request

Reason
This error occurs when in the signing request user didn't provide the Originator ID.

Solution

1. Launch the ADSS Server console:
2. Go to location: **Client Manager**
3. Ensure that your required **Client's Originator ID** is registered there
4. Provide the required **Client's Originator ID** in the request to resolve this error

---

Error Code 41021

Problem
Failed to process request - the user certificate chain is not in the request

Reason

Solution

Error Code 41022

Problem
Failed to process request - no signature found on the request

Reason
This error occurs when Client request messages must be signed and business application is sending an unsigned request to Signing Service.

Solution

1. Ensure that your business application is sending the signed requests to the signing service. Also ensure that the relevant request signing certificate must be registered against the same client originator ID in the Client Manager, for this:
    a. Launch the ADSS Server console
    b. Navigate to **Client Manager**
    c. Edit the required **Client's Originator ID**
    d. Ensure that relevant request signing certificate is registered against this client, if not then add the **Request Signing Certificate** a nd click on the **Save button**

2. If it is not required to send signed requests to signing service then follow these steps:
3. a. Launch the ADSS Server console
    b. Go to location: **Signing Service > Service Manager**
    c. **Disable** the checkbox **Client request messages must be signed**
    d. Click on the **Save** button
    e. Click on the **restart** button to have the changes take into effect

---

Error Code 41023

Problem
Failed to process request - the request structure is invalid

Reason

Solution

Error Code 41024

Problem
Failed to process request - signature verification failed

Reason

Solution

Error Code 41025

Problem
Failed to process request - referenced private key does not belong to the client

Reason
This error occurs when the private key does not belong to the client which used in request.

Solution

1. Launch the ADSS Server console:
2. Go to location: **Certification Service > X.509 Certificates > Issued Certificates**
3. Confirm that the certificate you are using in your request issued to which client
4. Then provide the same **Client's Originator ID** to avoid this error
5. If the certificate does not exist in the **Issued Certificates** list then generate the certificate against the required client to avoid this error

---

Error Code 41026

Problem
Failed to process request - the certificate chain referenced is not found

Reason
This error occurs when the signer certificate used in the request is in pending state

Solution#1

1. Launch the ADSS Server console:
2. Go to location: **Certification Service > X.509 Certificates > Issued Certificates**
3. Confirm the status of the certificate you are using in the request
4. Edit the profile under which certificate is issued
5. In the **Certificate Renewal Settings,** there are two options
    a. Renew certificate using existing key pair
        i. If you want to renew the certificate using existing key pair then **Save** the profile and send the renewal request to renew the certificate
        ii. After renewal now retry with the same request to avoid the error
    b. Renew certificate using a new key pair
        i. If you want to renew the certificate using new key pair then **Save** the profile and send the renewal request to renew the certificate
        ii. After renewal now retry with the same request to avoid the error.

Solution#2

1. Launch the ADSS Server console:
2. Go to location: **Certification Service > X.509 Certificates > Pending Requests**
3. Activate the required certificate as per possible ways i.e.
    a. Click the **Generate Certificate** button and generate the certificate to resolve the error
    b. Click the **Export CSR** button and certify from the any external CA or from **Manage CAs > Manual Certification** and download the certificate
    c. Navigate to **Certification Service > X.509 Certificates > Pending Requests** and click the **Import Certificate** and import that downloaded certificate
    d. By using the above methods certificate moves to the Issued Certificates tab
    e. Now try to send the request again to resolve the error

Solution#3

1. Launch the ADSS Server console:
2. Go to location: **Key Manager > Service Keys**
3. Edit the required service key and confirm the status of the certificate being used in the request
4. Select the certificate and click the **Renew Certificate** button
5. Now retry the with the same request to avoid the error

Error Code 41027

Problem
Failed to process request - the signer certificate has expired

Reason
This error occurs when the signer certificate used in the request is expired

Solution#1

1. Launch the ADSS Server console:
2. Go to location: **Certification Service > X.509 Certificates > Issued Certificates**
3. Confirm the status of the certificate you are using in the request
4. Edit the profile under which certificate is issued
5. In the **Certificate Renewal Settings** there is two options
    a. Renew certificate using existing key pair
        i. If you want to renew the certificate using existing key pair then **Save** the profile and send the renewal request to renew

the certificate
   ii. After renewal now retry with the same request to avoid the error
b. Renew certificate using new key pair
   i. If you want to renew the certificate using new key pair then **Save** the profile and send the renewal request to renew the certificate
   ii. After renewal now retry with the same request to avoid the error.

Solution#2

1. Go to location: **Key Manager > Service Keys**
2. Edit the required service key and confirm the status of the certificate being used in request
3. Select the certificate and click the **Renew Certificate** button
4. Now retry the with the same request to avoid the error

Error Code 41028

Problem
Failed to process request - the signer certificate is a CA certificate

Reason
This error occurs when the signing certificate used in the request is a CA certificate

Solution

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Edit the required Signing Profile and click on the **Advanced Settings** tab
4. In the **Certificate Details** box confirm that **Basic Constraints extension of signer certificate must show that signer is not CA** check-box is enabled
5. If enabled then unchecked the check-box, **Save** it and **restart** the signing service to resolve the error
6. If the user wants to send a signing request with the check-box of **Basic Constraints extension of signer certificate must show that signer is not CA** is enabled then confirm that
   a. The signing certificate doesn't contain the extensions of the CA certificate to avoid the error

---

Error Code 41029

Problem
Failed to process request - the request is not signed

Reason

This error occurs when the client request doesn't fulfil the requirements of the signed request

Solution#1

1. Launch the ADSS Server console
2. If the user didn't want to send a signed request then
3. Go to location: **Signing Service > Service Manager**
4. Unchecked the check-box of the **Client request messages must be signed** then save and restart the service
5. Now send the signing request again to avoid the error

Solution#2

1. If the user wants to send the signed request then
2. Go to location: **Client Manager**
3. Edit the required Client's Originator ID
4. Confirm that **Request Signing Certificate** is added and **Save** it.
5. Now check the signing request and provide the path of the Request Signing Certificate PFX and it's password to avoid the error

---

Error Code 41030

Problem
Failed to process request - document Id is not found in the request

Reason

Solution

Error Code 41031

Problem
Failed to process request - the signing profile is not appropriate for this file type

Reason
This error occurs when the user sends the signing request to inappropriate signing profile for that signature type

Solution

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Edit the profile and select the Signature Type according to your request type to resolve the error

---

Error Code 41032

Problem
Failed to sign document - a signed PDF cannot subsequently be certify signed

Reason
This error occurs when a user tries to certify signed on already signed PDF

Solution

1. Open the PDF in adobe reader and check whether the PDF is already signed or not.
2. If PDF is already signed and user try to sign the PDF again with enabling **Certify Signature Settings** in used **Signing Service > Signing Profiles**
3. As per **standard** user can't certify signed the already signed PDF
4. To avoid this error user need to send the unsigned PDF to certify signing.

Error Code 41033

Problem
Failed to sign document - PDF is already certify signed

Reason
This error occurs when a PDF document is already certify signed and user again try to sign the same document

Solution

1. Open the PDF in adobe reader and check whether the PDF is already certify signed or not.
2. If PDF is already certify signed and the user tries to sign the PDF again then as per **standard** user can't certify signed the already certify signed PDF
3. To avoid this error user need to send the unsigned PDF to certify signing.

Error Code 41034

Problem
Failed to authenticate signing request

Reason

Solution

Error Code 41035

Problem
Failed to process request - authorised signing is not enabled in license

Reason

This error occurs when authorised signing is not enabled in the license in signing service module.

Solution

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

---

Error Code 41036

Problem
Failed to validate authorisation control file

Reason
This error occurs when tempered authorisation control file is being used in the request

Solution

1. Check whether the **authorisation control file** is tempered or not
2. If authorisation control file is tempered then signed the valid authorisation control file again

3. Provide the new signed authorisation control file in the request to avoid the request

---

Error Code 41037

Problem
Failed to validate authorisation control file - file not found within request

Reason
This error occurs when the file path is not correct and the system cannot find the file specified in the request.

Solution

1. Check whether the authorisation control file path is provided in the request or not
2. If authorisation control file path is not provided then provide the path to avoid the error
3. if authorisation control file path is provided already then please provide the correct path to avoid this error

---

Error Code 41038

Problem
Failed to process request - signer certificate status revoked or unknown

Reason
This error occurs when the signer certificate is revoked by CA or it's revocation status is unknown

Solution

1. Launch the ADSS Server console
2. Go to location:**Certification Service > X.509 Certificates > Issued Certificates**
3. Check the status of the certificate under which revocation reason the certificate is revoked
    a. If the certificate is revoked with **certificateHold** then the user can reinstate the certificate to avoid the error
    b. If the certificate is revoked other than **certificateHold** then the user can't reinstate the certificate and to avoid the error get the new certificate.
4. If Certificate is not revoked and still user get the **unknown** status then navigate to **Trust Manager** screen and ensure that the complete certificate chain for the signing certificate is registered there
    a. If the issuer chain is not registered then register the complete certificate chain and restart the ADSS Server accordingly
    b. If the issuer chain is registered then navigate to **CRL Monitor > CRL Details** screen and confirm that the latest CRLs for the relevant CAs are available there.

Error Code 41039

Problem
Failed to process request - the profile is not allowed to the client

Reason
This error occurs when the signing request sent to that profile which is not registered to that client

Solution#1

1. Launch the ADSS Server console
2. Go to location: **Client Manager**
3. Edit the required **Client's Originator ID** and click on the **Signing Service** tab
4. Confirm that the signing profile using in the signing request is selected in the **Selected Signing Profiles** box
5. If not then move the signing profile from **Available Signing Profiles** to **Selected Signing Profiles** to resolve the error

Solution#2

1. Launch the ADSS Server console
2. Go to location: **Client Manager**
3. Matched the name of the required **Client's Originator ID** which used in the request
4. If the **Client's Originator ID** doesn't match with **Client's Originator ID** used in the request then used the correct one to resolve the error

---

Error Code 41040

Problem
Failed to authorise request - signing certificate alias is not one of the allowed set of certificate aliases

Reason
This error occurs when the signing certificate alias is not allowed set of certificate aliases in the client manager

Solution#1

1. Launch the ADSS Server console
2. Go to location: **Client Manager**
3. Edit the required **Client's Originator ID** and click on the **Signing Service** tab

4. Confirm that the signing certificate alias used in the signing request is selected in the **Selected Document Signing keys** box
5. If not then move the signing certificate alias from **Available Document Signing keys** to **Selected Document Signing keys** to resolve the error

Solution#2

1. Launch the ADSS Server console
2. Go to location: **Client Manager**
3. Matched the name of the required **Client's Originator ID** under which signing certificate alias is allowed and used in the request
4. If the **Client's Originator ID** doesn't match with **Client's Originator ID** used in the request then used the correct one to resolve the error

---

Error Code 41041

Problem
Failed to authorise request - default signing certificate alias not found in request or profile

Reason
This error occurs when the default signing certificate alias is not found in the request or in the signing profile

Solution#1

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Edit the required **Signing Profile** and **General** tab is shown
4. Confirm that in the **Default Signing Certificate** box default signing certificate is selected if not then select available/required certificate and save the profile
5. Restart the Signing Service from the **Service Manager**
6. Now send the signing request again to resolve the error

Solution#2

1. Provide the required signing certificate alias in the signing request to avoid the error

---

Error Code 41043

Problem
Failed to match data hash with signed hash

Reason
******* discuss with developer*****

Solution

Error Code 41044

Problem
Failed to assemble signature within the document

Reason

Solution

Error Code 41045

Problem
Failed to create empty signature field

Reason

Solution

Error Code 41046

Problem
Failed to create a file signature

Reason

Solution

Error Code 41047

Problem
Failed to parse PDF document

Reason

Solution

Error Code 41048

Problem
Failed to create signing response

Reason

Solution

Error Code 41049

Problem
Failed to compute the hash

Reason

Solution

Error Code 41050

Problem
Failed to create CAdES-T signature

Reason

Solution

Error Code 41051

Problem
Failed to process request - private key referenced is not found

Reason

Solution

Error Code 41052

Problem
Failed to process request - document hash was not provided in the request

Reason

Solution

Error Code 41053

Problem
Failed to create XAdES-T signature

Reason

Solution

Error Code 41054

Problem
Failed to create CMS signature

Reason

Solution

Error Code 41055

Problem
Failed to create CAdES-BES signature

Reason

Solution

Error Code 41056

Problem
Failed to create S/MIME signature

Reason

Solution

Error Code 41057

Problem
XAdES detached signatures are not supported

Reason

Solution

Error Code 41058

Problem
Failed to create XADES-BES signature

Reason

Solution

Error Code 41059

Problem
Failed to create CAdES-X-L signature

Reason

Solution

Error Code 41060

Problem
Failed to create XAdES-X-L signature

Reason

Solution

Error Code 41061

Problem
Failed to create CAdES-A signature

Reason

Solution

Error Code 41062

Problem
Failed to create XAdES-A signature

Reason

Solution

Error Code 41063

Problem
Failed to process request - a certify signed PDF with no changes allowed cannot be signed

Reason
This error occurs when the user tried to sign a certify signed PDF which is already a certify signed PDF with no changes allowed

Solution

1. Open the PDF in adobe reader and check whether the PDF is already certify signed or not.
2. If PDF is already certify signed PDF with no changes allowed and user try to sign the PDF again then as per **standard** user can't sign the already certify signed PDF with no changes allowed
3. To avoid this error user need to send the unsigned PDF to sign

---

Error Code 41064

Problem
Failed to process request - signing field information is not available

Reason

Solution

Error Code 41068

Problem
Failed to process request - signer certificate does not contains required extensions

Reason
This error occurs when a signer certificate does not contain required extensions as per criteria

Solution

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Edit the required Signing Profile and click on the **Advanced Settings** tab
4. In the **Certificate Details** box confirm that **Key Usage extensions of signer's certificate must have following flags:** check box is enabled with **AND** radio button selected
    a. If yes then add the both **Digital Signature** and **Non Repudiation** extensions in the certificate key usages to resolve the error
    b. If **AND** radio button is selected then select the **OR** radio button to resolve the error

---

Error Code 41069

Problem
Failed to process request - processing of this signature type is not enabled in license

Reason
This error occurs when authorised signing is not enabled in the license in signing service module.

Solution

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

---

Error Code 41070

Problem
Failed to process request - signature grace period is not yet elapsed

Reason

Solution

Error Code 41071

Problem
Failed to create PAdES-BES signature - see the signing service debug logs for details

Reason

Solution

Error Code 41072

Problem
Failed to create XAdES-X type 1 signature

Reason

Solution

Error Code 41073

Problem
Failed to process request - input file is either unsigned or contains an archive timestamped signature

Reason

Solution

Error Code 41074

Problem
Failed to create PDF signature - PDF document already contains PAdES-LTV document timestamp signature

Reason

Solution

Error Code 41075

Problem
Failed to authorise client request - signing service not allowed

Reason
This error occurs when the signing service is not allowed to client provided in the signing request

Solution

1. Launch the ADSS Server console
2. Go to location: **Client Manager**
3. Edit the required **Client's Originator ID** and click on the **Signing Service** tab
4. In the **Signing Service Settings** box enable the **Allow this client to access the ADSS Signing Service** check box
5. Move the required signing profiles from **Available Signing Profiles** to **Selected Signing Profiles** and select the default signing profile
6. Now again send the signing request using the same **Client's Originator ID** to resolve the error

---

Error Code 41076

Problem
Failed to create PDF signature - signature dictionary size is smaller than required

Reason
This error occurs when the signatre dictionary size is smaller than the required

Solution

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Edit the required **Signing Profile** and click on the **Advanced Settings** tab
4. In the **PDF Signature Dictionary Settings** box increase the value of the **PDF Signature Space Allocation:** to resolve the issue

---

Error Code 41077

Problem
Failed to process request - no key alias available from request and profile

Reason

This error occurs when the default signing certificate alias is not found in the request or in the signing profile

Solution#1

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Edit the required **Signing Profile** and **General** tab is shown
4. Confirm that in the **Default Signing Certificate** box default signing certificate is selected if not then select available/required certificate and save the profile
5. Restart the Signing Service from the **Service Manager**
6. Now send the signing request again to resolve the error

Solution#2

1. Provide the required signing key alias in the signing request to avoid the error

---

Error Code 41078

Problem
Failed to process request - invalid input document format

Reason

Solution

Error Code 41079

Problem
Failed to process request - embedded data in signature time stamp is invalid

Reason

Solution

Error Code 41080

Problem
Failed to process request - embedded data in time-stamp is invalid

Reason

Solution

Error Code 41081

Problem
Failed to process request - embedded data in the signature is invalid

Reason

Solution

Error Code 41082

Problem
Failed to process request - signing time not present in the signature

Reason

Solution

Error Code 41083

Problem

Failed to process request - signing service not enabled in the system

Reason

This error occurs when you send a signing request to the service and it is not enabled in ADSS Server Console Server Manager

Solution

1. Launch the ADSS Server console
2. Go to location: **Server Manager**
3. Click the service instance in **ADSS Server Instance** column and Click the Enable button in front of the Signing Service to enable the service in the system

---

Error Code 41084

Problem
Failed to process request - signing field not found in the PDF document

Reason

This error occurs when a user tries to sign a PDF which is already a certify signed PDF document

Solution

1. Open the PDF in adobe reader and check whether the PDF is already certify signed other than with **no changes allowed**
2. If PDF is already certify signed other than with **no changes allowed** and user try to sign the already certify signed PDF then this error occurs
3. To avoid this error user needs to send the unsigned PDF to sign.

Error Code 41085

Problem
Failed to process request - signing certificate cannot be used for document or notary or email signing

Reason

Solution

Error Code 41086

Problem
Failed to authorise request - signing profile is inactive

Reason
This error occurs user sends signing request and signing profile is marked inactive in the signing service

Solution

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Edit the required signing profile and marked the **Inactive** profile to **Active** to resolve the issue

---

Error Code 41087

Problem
Failed to authorise request - signing profile does not exist or marked inactive

Reason
This error occurs when a user sends signing request and signing profile does not exist in the signing service

Solution

1. Launch the ADSS Server console
2. Go to location: **Signing Service > Signing Profiles**
3. Confirm that the signing profile used in the request already exists or not
    a. If not then create the new signing profile with the required name and send the signing request again to resolve the error
    b. If signing profile used in a request already exists then match the name both in request and ADSS Server console

---

Error Code 41088

Problem
Failed to process request - input document is encrypted

Reason

Solution

Error Code 41089

Problem
Failed to process request - signed document can not be encrypted

Reason

Solution

Error Code 41090

Problem
Failed to process request - authorised signature not supported on http interface

Reason

Solution

Error Code 41091

Problem
Failed to process request - invalid password

Reason
This error occurs when an incorrect password is provided in the request

Solution

1. To resolve this error, the user needs to send the valid password in the signing request to avoid the errors

---

Error Code 41092

Problem
Failed to process request - password not provided in the request

Reason
This error occurs when the password is not provided in the request

Solution

1. To resolve this error, the user needs to provide the password in the signing request to avoid the errors

---

Error Code 41093

Problem
Failed to process request - key cannot be used for document signing

Reason

Solution

Error Code 41094

Problem
Failed to process request - only PDF documents can be timestamped

Reason

Solution

Error Code 41095

Problem
Failed to process request - revocation information unavailable for existing document timestamp(s)

Reason

Solution

Error Code 41096

Problem
Failed to process request - unable to create document timestamp

Reason

Solution

Error Code 41097

Problem
Failed to process request - user authentication failed against the directory

Reason

Solution

Error Code 41098

Problem
Failed to process request - PDF document cannot be timestamped, the document has user signature(s)

Reason

Solution

Error Code 41099

Problem
Failed to process request - signature line not found in the office document

Reason
This error occurs when the signature line is not found in the office document

Solution

1. To resolve this issue error create/add the signature line in the provided office document in the signing request

---

Error Code 41100

Problem
Failed to process request - input document is an invalid PDF

Reason

Solution

Error Code 41101

Problem
Failed to process request - unable to convert input document into PDF

Reason

Solution

Error Code 41102

Problem
Failed to process request - some mandatory request parameter(s) are missing

Reason

Solution

Error Code 41103

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

Reason
This error occurs when the signing profile is not provided in the request and also no default profile is configured in the client manager

Solution#1

1. Launch the ADSS Server console
2. Go to location: **Client Manager**
3. Edit the required **Client's Originator ID** and click on the **Signing Service** tab
4. In the **Signing Service Settings** box select any profile from the **Default Signing Profile:** drop-down list, Save it and **Restart** the signing service at location **Signing Service > Service Manager**

Solution#2

1. The other solution to resolve this error, provide the required signing profile in the request

---

Error Code 41104

Problem
Failed to process request - the signer certificate is in pending state

Reason

Solution

Error Code 41105

Problem
Failed to process request - the document format must be a valid OID

Reason

Solution

Error Code 41106

Problem
Failed to validate authorisation control file - originator ID is missing

Reason

This error occurs when in the authorisation control file user didn't provide the Originator ID.

Solution

1. To resolve this error, the user needs to create authorisation control file with all the mandatory attributes including **Client Originator ID** be fore sending the signing request.

Error Code 41107

Problem
Failed to validate authorisation control file - originator ID does not match with the originator ID in the request

Reason
This error occurs when the Originator ID provided in the request doesn't match with the Originator ID provided in the authorisation control file

Solution

1. User created an authorisation control file with all the mandatory attributes including **Client Originator ID**
2. When the user used signed authorisation control file for signing using the different **Client Originator ID** instead of the one used in authorisation control file then this error comes
3. To resolve the error used the signed authorisation control file for that client only which is being used in the authorisation control file

---

Error Code 41108

Problem
Failed to validate authorisation control file - valid from date is missing

Reason

This error occurs when valid to date is mention but valid from date is missing in the authorisation control file

Solution

1. User created an authorisation control file with all the mandatory attributes including **Validity Period** and in that **<ValidFrom>** tag is missing
2. When the user used signed authorisation control file for signing then this error comes
3. To resolve the error user needs to add **<ValidFrom>** tag in authorisation control file before signing the authorisation control file

---

Error Code 41109

Problem
Failed to validate authorisation control file - valid period is in future

Reason
This error occurs when the validity period used in the authorisation control file is in future dates

Solution

1. User created an authorisation control file with all the mandatory attributes including **Validity Period** and in **<ValidFrom>** to **<ValidTo>** is a future date
2. When the user used signed authorisation control file for signing then this error occurs
3. To resolve this error, the user needs to provide a valid time/date in the **Validity Period** tag in authorisation control file before signing the authorisation control file

---

Error Code 41110

Problem
Failed to validate authorisation control file - valid from date is not according to XSD date format

Reason
This error occurs when valid from date used in authorisation control file is not according to XSD date format

Solution

1. User created an authorisation control file with all the mandatory attributes including **Validity Period** and in that **<ValidFrom>** tag format is not according to XSD date format
2. When the user used signed authorisation control file for signing then this error occurs
3. To resolve the error user needs to provide the **<ValidFrom>** tag format according to XSD date format in authorisation control file before signing the authorisation control file

---

Error Code 41111

Problem
Failed to validate authorisation control file - valid to date is missing

Reason
This error occurs when valid from date is mention but valid to date is missing in the authorisation control file

Solution

1. User created an authorisation control file with all the mandatory attributes including **Validity Period** and in that **<ValidTo>** tag is missing
2. When the user used signed authorisation control file for signing then this error occurs
3. To resolve the error user needs to add **<ValidTo>** tag in authorisation control file before signing the authorisation control file

---

Error Code 41112

Problem
Failed to validate authorisation control file - validity period has elapsed

Reason
This error occurs when the validity period used in the autorisation control file has elapsed

Solution

1. User created an authorisation control file with all the mandatory attributes including **Validity Period** and in **<ValidFrom>** to **<ValidTo>** is past date
2. When the user used signed authorisation control file for signing then this error occurs
3. To resolve this error, the user needs to provide a valid time/date in the **Validity Period** tag in authorisation control file before signing the authorisation control file

---

Error Code 41113

Problem

Failed to validate authorisation control file - valid to date is not according to XSD date format

Reason
This error occurs when the date format used in valid to date is not according to XSD date format

Solution

1. User created an authorisation control file with all the mandatory attributes including **Validity Period** and in that **<ValidTo>** tag format is not according to XSD date format
2. When user used signed authorisation control file for signing then this error occurs
3. To resolve the error user needs to provide the **<ValidTo>** tag format according to XSD date format in authorisation control file before signing the authorisation control file

---

Error Code 41114

Problem
Failed to validate authorisation control file - authorisation profile is inactive

Reason
This error occurs when the authorisation profile is marked as inactive

Solution

1. Launch the ADSS Server console
2. Go to location: **Global Settings > Authorisation Profiles**
3. Edit the required authorisation profile and marked the **Inactive** profile to **Active** to resolve the issue

---

Error Code 41115

Problem
Failed to validate authorisation control file - request does not contain minimum required authoriser signatures

Reason
This error occurs when authorisation control file is signed with the signers that are not authorised to sign the document

Solution

1. Launch the ADSS Server console
2. Go to location: **Global Settings > Authorisation Profiles**
3. Edit the required authorisation profile and confirm that which **Authoriser Certificates** are added in the **Authorisers Details box**
4. Confirm that which **Number of authorities for approval (M of N schemes):** is set to authorisation of sign the document
5. Now sign the document with the authorised certificate to resolve the error

---

Error Code 41116

Problem
Failed to validate authorisation control file - one or more signatures could not be verified

Reason
This error occurs when one or more signatures are required to verify the authorisation control file

Solution

1. When user used the signed authorisation control file for signing and the signature of the autorised signer is corrupted or doesn't match with the authorised signer
2. To resolve the error used the signer certificate which is linked with the authorised certificate whose signature is added in the authorisation control file.

Error Code 41117

Problem
Failed to validate authorisation control file - hashes do not match with the hashes of the documents

Reason
This error occurs when the hash of the document provided in the authorisation control file doesn't match with the hash of the document provided in the request

Solution

1. To resolve this error, provide the hash in the authorisation control file of the document that is being used in the request. Or provide the document, whose hash is being used in the authorisation control file

---

Error Code 41118

Problem
Failed to validate authorisation control file - document digest or validity period must be available

Reason
This error occurs when the document digest or validity period is not available in the authorisation control file

Solution

1. User created an authorisation control file without all the mandatory attributes including **<ValidityPeriod>** and **<DocumentDigest>**
2. When user used signed authorisation control file for signing then this error occurs
3. To resolve the error, user needs to provide the one of the mandatory attribute from **<ValidityPeriod>** or **<DocumentDigest>** in authorisation control file before signing the authorisation control file

---

Error Code 41119

Problem
Failed to process request - invalid OTP provided in the request

Reason
This error occurs when invalid OTP provided in the request

Solution

1. To resolve this error, provide the valid OTP received on the user mobile in the signing request

---

Error Code 41120

Problem
Failed to process request - crypto profile requires two factor authentication to access the referenced private key

Reason

Solution

Error Code 41121

Problem
Failed to validate authorisation control file - certificate ID is missing

Reason

This error occurs when the certificate ID is not provided in the authorisation control file

Solution

1. User created an authorisation control file without the mandatory attributes **<CertificateID>**
2. When the user used signed authorisation control file for signing then this error occurs
3. To resolve the error, user needs to provide the mandatory attribute **<CertificateID>** in authorisation control file before signing the authorisation control file

---

Error Code 41122

Problem
Failed to validate authorisation control file - certificate ID does not match with the certificate ID in the request

Reason

This error occurs when the certificate ID provided in the request doesn't match with the certificate ID provided in the authorisation control file

Solution

- To resolve the error, user needs to provide the same certificate alias for signing request that is being used in the certificate ID of the authorisation control file before signing the authorisation control file

---

Error Code 41123

Problem
Failed to process request - the signing certificate is marked inactive

Reason

This error occurs when the signing request failed due to any reason, after the no. of configured failure times the signer certificate is marked as

inactive

Solution

1. Launch the ADSS Server console
2. Go to location: **Certification Service > X.509 Certificates > Issued Certificates**
3. Select the required certificate and click on **Reinstate** button to **Active** the **Inactive** certificate
4. If the user doesn't want to make the certificate manually **Active** then wait for the configure time of the threshold to **Activate** the certificate
5. If the user doesn't want to make the certificate Inactive on the failure of signing request then do the following steps
    a. Go to location: **Global Settings > Advanced Settings**
    b. Select the **Property Type: Signing**
    c. **USER_ACTIVATION_THRESHOLD** property defines the time period in minutes for which the signer status remains INACTIVE. Once this period is elapsed, the signer status is automatically marked as ACTIVE**.**
    d. **USER_AUTHENTICATION_FAILURE_LIMIT** defines the number of failed authentications after which the signer status is automatically marked as INACTIVE. Default value is set to **ZERO** for unlimited failed authentications allowed

---

Error Code 41124

Problem
Failed to validate authorisation control file - authorisation control file is not a valid XML file

Reason
This error occurs when authorisation control file is not a valid XML file

Solution

1. To resolve this error, provide the valid authorisation control file xml

---

Error Code 41125

Problem
Failed to process request - Two factor authentication not enabled in license

Reason

This error occurs when Two factor authentication is not enabled in license

Solution

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

---