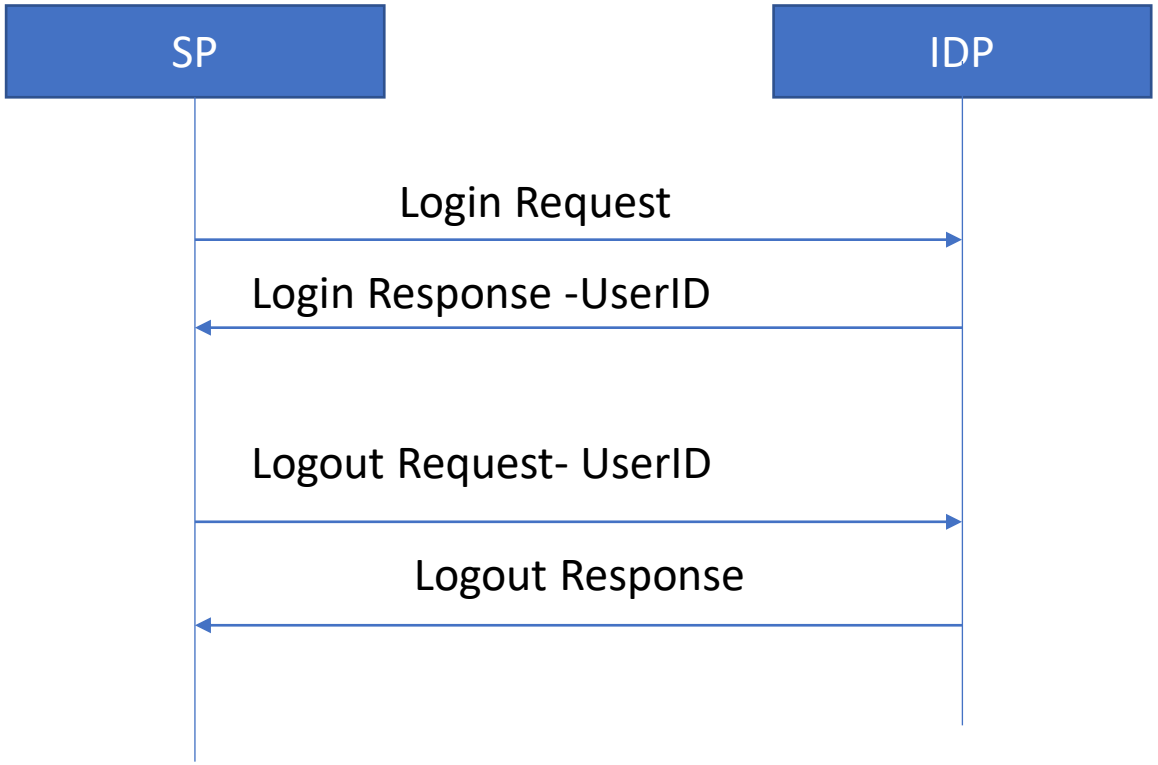
Go VE Become an Expert - SAML Authentication FAQ

Troubleshoot common issues that may come up when implementing SAML with Primo VE

Ex Libris
a ProQuest Company

SAML Authentication Theory

- SAML – An authentication messaging protocol
- SP – A service that requires authentication (Alma)
- IDP – A service that provides authentication (ADFS)



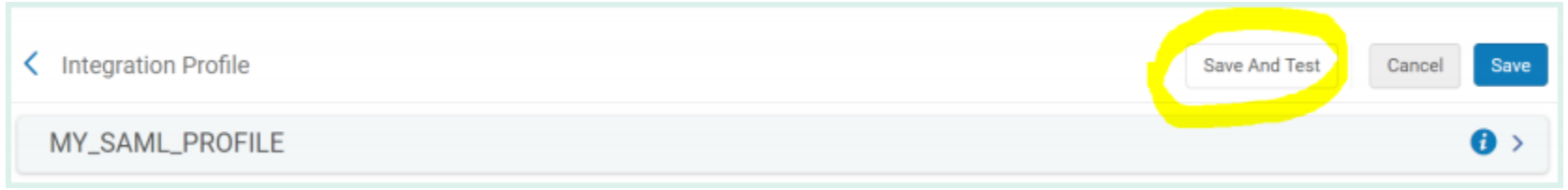
Requirements to set up SAML protocol

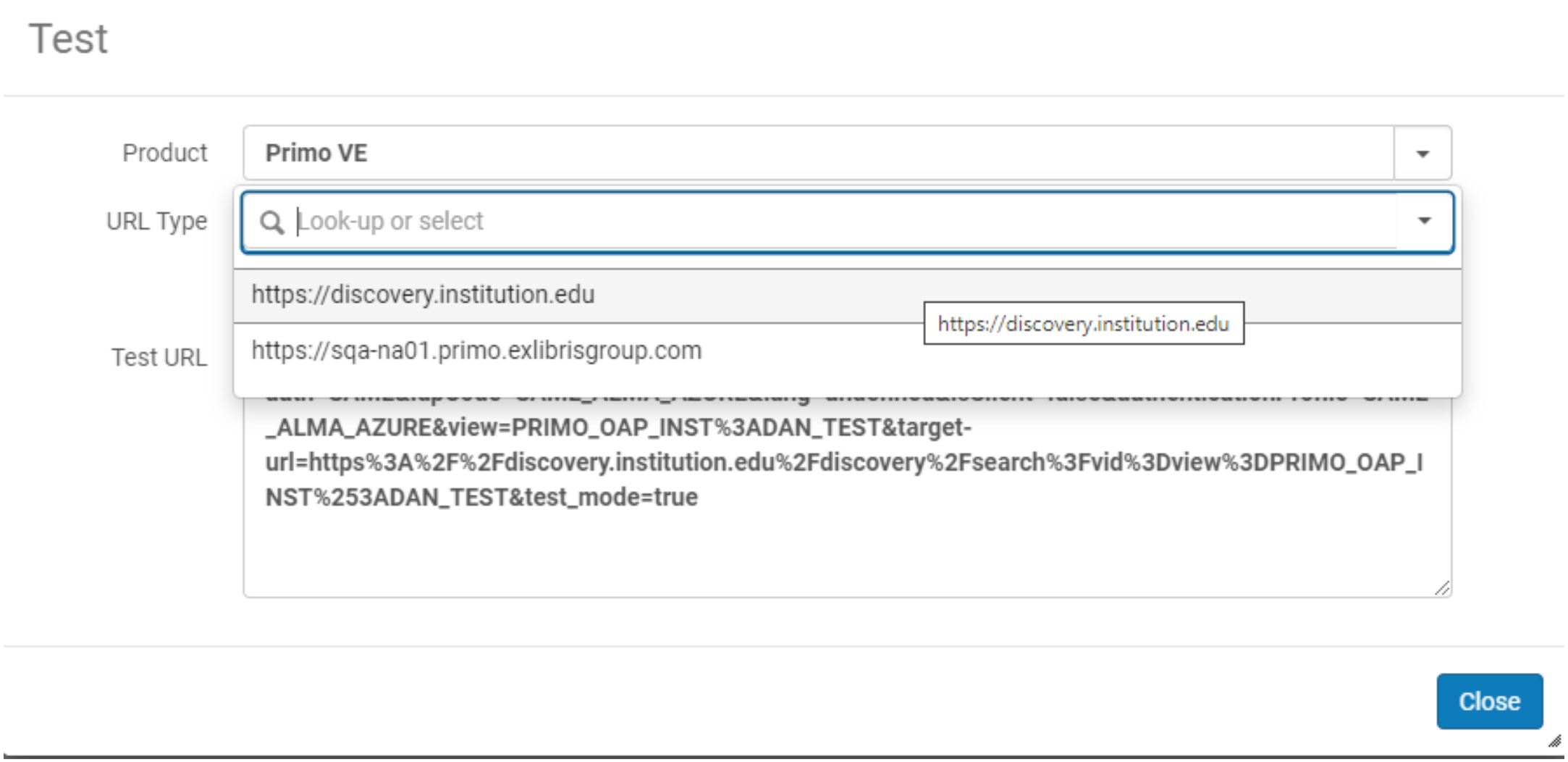
1) Configure the endpoints used by the SP and IDP
2) Secure the communication between the SP and the IDP using certificates
3) Communicate the identity of the user that is logging in to the SP (Alma)

Testing the integration profile

- How to create the SAML integration profile in Alma:
  - https://knowledge.exlibrisgroup.com/Primo/Product_Documentation/Go_VE/Getting_Started_with_Go_VE/Go_VE_Webinars_and_Training/020Go_VE_-_Become_an_Expert_Series/SAML_and_CAS_Authentication_Configuration

- "Test Integration Profile" Button
  - Available to everybody in May 2021 Release of Alma
  - Available on request by emailing: GO_VE@exlibrisgroup.com





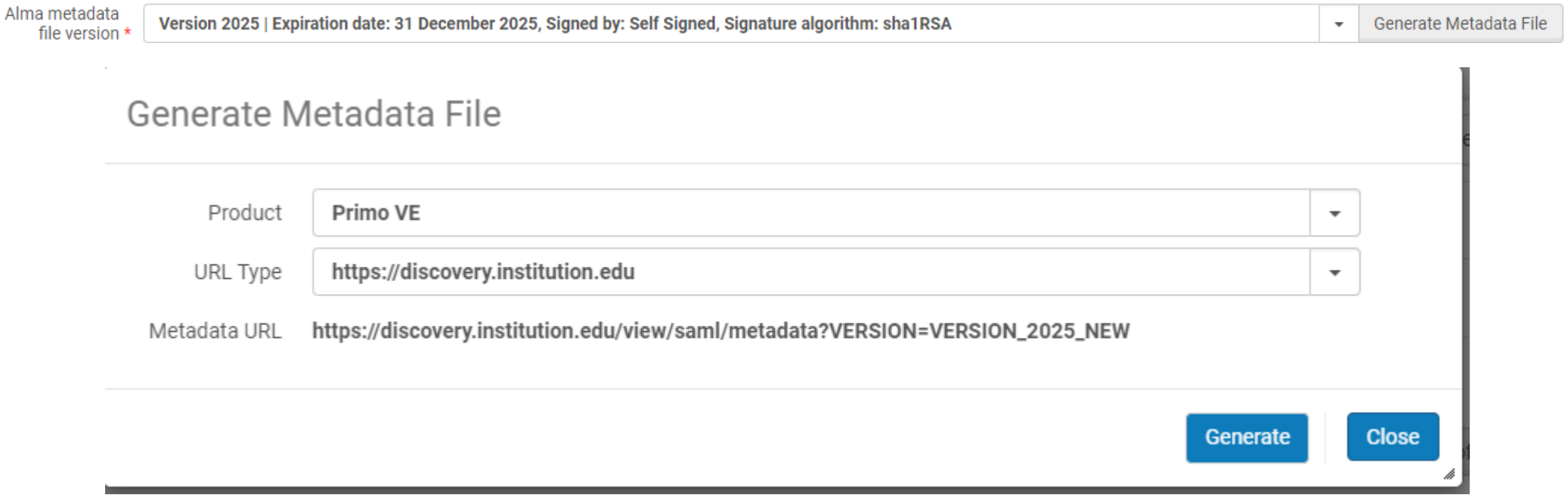
To Test using a custom DNS name that is currently in use by Primo Classic: https://knowledge.exlibrisgroup.com/@api/deki/files/87177/DNS_switch_simulation.docx?revision=2

Error on login request

- IDP does not recognize who is the SP and where to send LoginResponses to.

IDP Platform	Shibboleth	ADFS	AZURE
Error displayed	The application you have accessed is not registered for use with this service.	An error occurred. Contact your administrator for more information.	AADSTS700016: Application with identifier 'https://sqa-na01.primo.exlibrisgroup.com/mng/login' was not found in the directory 'b41de8….c'.

Generate SP metadata



Authentication stages

- Assertion Decryption check
- SAML message validations – entityid , saml2:Conditions
- Certificate validations (IDP Signing) – strict
- Signature check
- Attribute mapping
- SAML Response received (encrypted) – output
- Decrypted SAML Response - output

Assertion decryption error

- → [2020-10-20T02:45:41.550Z] login test: SAML - encrypted assertion was found.
- → [2020-10-20T02:45:41.559Z] login test: SAML failure 10: Assertion decryption failed. Error message: Failed to decrypt EncryptedData→ [2020-10-20T02:45:41.550Z] login test: SAML - encrypted assertion was found.
- → [2020-10-20T02:45:41.559Z] login test: SAML failure 10: Assertion decryption failed. Error message: Failed to decrypt EncryptedData
- → [2020-10-20T02:45:41.562Z] login test: Check if the 'Alma certificate version' parameter in the integration profile is consistent with the metadata file used by the customer.
- → [2020-10-20T02:45:41.564Z] login test: org.opensaml.xml.encryption.DecryptionException: Failed to decrypt EncryptedData
- → [2020-10-20T02:45:41.562Z] login test: Check if the 'Alma certificate version' parameter in the integration profile is consistent with the metadata file used by the customer.
- → [2020-10-20T02:45:41.564Z] login test: org.opensaml.xml.encryption.DecryptionException: Failed to decrypt EncryptedData

Solution:

- Regenerate Primo VE Metadata
- Upload the Primo VE Metadata to the IDP

SAML conditions error

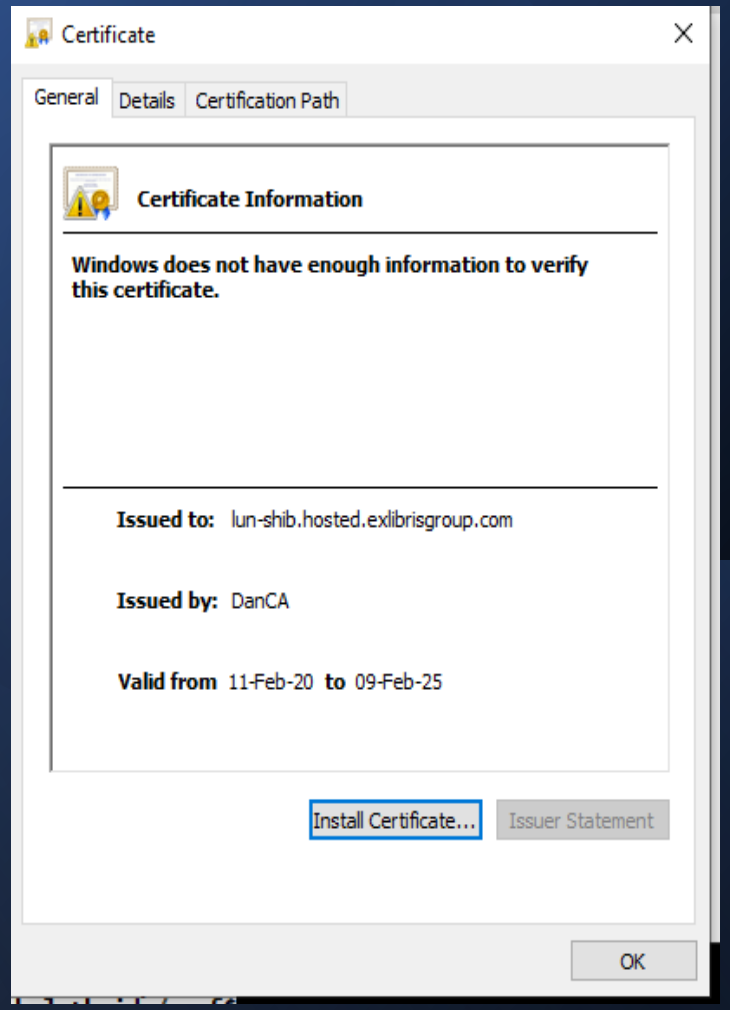
SAML failure: Conditions timestamp is still not valid after adding tolerance - current time is out of range. Assertion is valid only between 2017-11-08T14:00:32.000+02:00 and 2017-11-08T12:11:02.000Z . Current time is 2017-11-08T14:00:27.730+02:00

Solutions:

1. Check and resolve NTP issue on the IDP
2. Or configure the IDP to use a bigger window for this condition:

https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsrelyingpartytrust?view=win10-ps

IDP certificate validations error



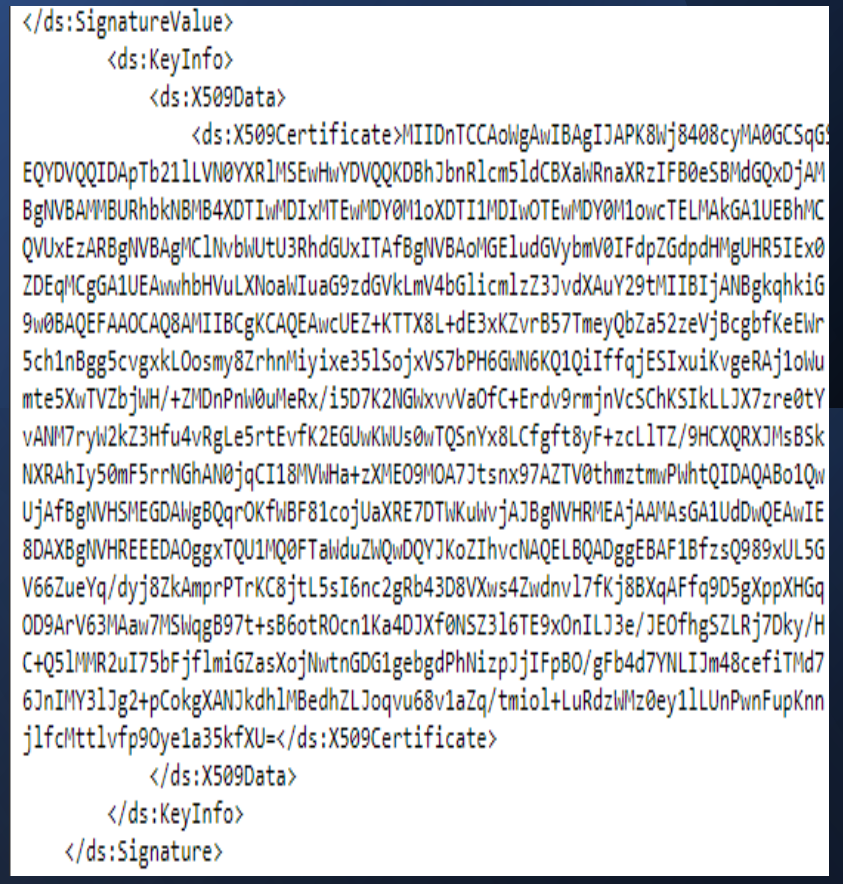
- → [2020-10-26T08:12:13.857Z] login test: SAML - signature is valid.
- → [2020-10-26T08:12:13.859Z] login test: SAML failure 20: Certificate is not valid. Error message: Path does not chain with any of the trust anchors
- → [2020-10-26T08:12:13.860Z] login test: java.security.cert.CertPathValidatorException: Path does not chain with any of the trust anchors
- → [2020-10-26T08:12:13.861Z] login test: SAML failure 20: Certificate is not valid. Cause: null
- → [2020-10-26T08:12:13.862Z] login test: SAML failure 20: Certificate is not valid. Reason: NO_TRUST_ANCHOR

Solution:
The IDP certificate uploaded to Alma was not input correctly.

Retrieve the IDP certificate from the SAML response, and if it is self-signed (subject and issuer are the same), add the certificate to the integration profile as free-text (with the certificate text surrounded by -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----)

If the certificate is signed by a CA, follow instructions to create a JKS here: https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst_idp/saml/chain_of_trust

Signature check failure



→ [2020-10-26T08:05:43.714Z] login test: java.security.cert.CertPathValidatorException: signature check failed

→ [2020-10-26T08:05:43.715Z] login test: SAML failure 20: Certificate is not valid. Cause: java.security.SignatureException: Signature does not match.

→ [2020-10-26T08:05:43.716Z] login test: SAML failure 20: Certificate is not valid. Reason: INVALID_SIGNATURE

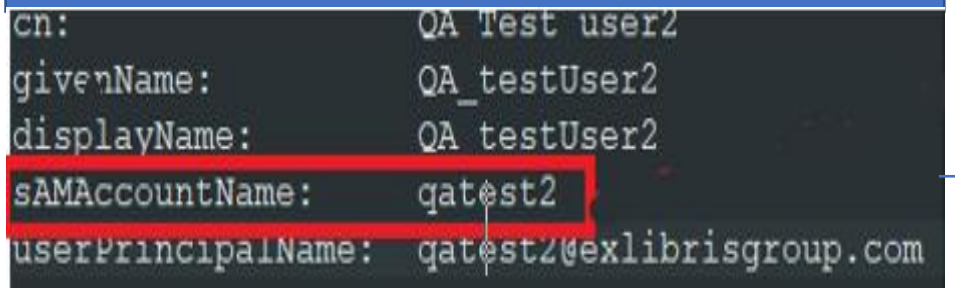
Cause:
The public key of the IDP certificate that was uploaded to Alma does not match the public key of the IDP certificate used in the SAML response

Solution:
Retrieve the certificate from the SAML response, and if it is self-signed (subject and issuer are the same), add the certificate to the integration profile as free-text (with the certificate text surrounded by -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----)

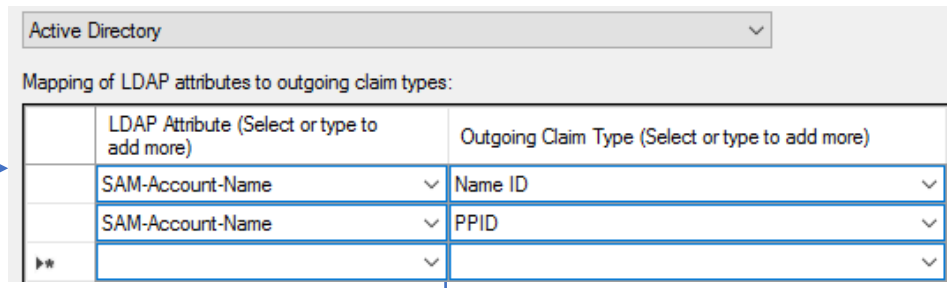
If the certificate is signed by a CA, follow instructions to create a JKS here.https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst_idp/saml/chain_of_trust

User identifier’s journey

Active Directory



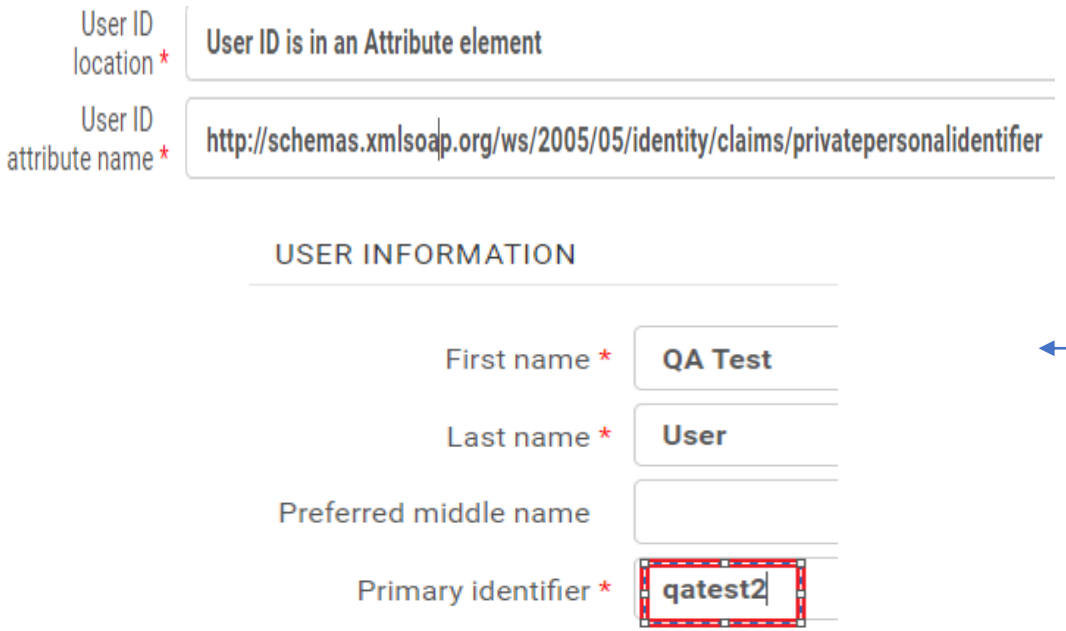
ADFS



SAML Response

```
<Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/privatepersonalidentifier">
      <AttributeValue>qatest2</AttributeValue>
    </Attribute>
  </AttributeStatement>
```

Alma



Attribute mapping error – wrong userId attribute name

→ [2020-10-27T03:26:50.179Z] login test: SAML - found attributes in response:

→ [2020-10-27T03:26:50.179Z] login test: SAML - telephoneNumber: +972-xxxxxxx

→ [2020-10-27T03:26:50.180Z] login test: SAML - mail: qatest2@test.test

→ [2020-10-27T03:26:50.181Z] login test: SAML - sAMAccountName: qatest2

→ [2020-10-27T03:26:50.181Z] login test: SAML - cn: qa test user2

→ [2020-10-27T03:26:50.183Z] login test: SAML failure 22: Cannot find 'User ID Attribute Name' value. User Id attribute name in SAML profile 'sAMAccountName'

Solution:

- Check decrypted SAML response for attributes being sent
- If the attribute that contains the AlmaId is found but has a different name, update the integration profile accordingly
- Otherwise the IDP administrator needs to release a new attribute with a value of the AlmaId

Attribute mapping error – user not found

→ [2020-10-27T03:26:50.179Z] login test: SAML - found attributes in response:

→ [2020-10-27T03:26:50.179Z] login test: SAML - telephoneNumber: +972-xxxxxxx

→ [2020-10-27T03:26:50.180Z] login test: SAML - mail: qatest2@test.test

→ [2020-10-27T03:26:50.181Z] login test: SAML - sAMAccountName:

→ [2020-10-27T03:26:50.181Z] login test: SAML - cn: qa test user2

→ [2021-03-15T08:42:45.730Z] login test: SAML - found primary identifier: qatest2
→ [2021-03-15T08:42:45.940Z] login test: SAML failure 24: User identifier ‘qatest2' is authenticated via SAML but user is not defined in Alma. Login failed.

Solution:

- Possibly just a matter of adding the user in Alma
- It is also possible that no identifiers in Alma are being returned in the SAML response for any user. In this case the IDP administrator needs to find the attribute in the ‘Active Directory’ that corresponds to the AlmaId and release a new SAML attribute with this value.

Thank You!

Go_VE@exlibrisgroup.com