SAML authentication in AEM

Sham Hassan Chikkegowda
Customer Support Engineer

&

Timothee Maret
Sr. Software Developer

Janne Parviainen

Agenda

- SAML 2.0
  A quick overview
- AEM & SAML
  Supported features
- Configurations
  Settings in typical deployments
- Troubleshoot
  How to analyze deployment issues
- Changelog
  Improvements in AEM 6.2
- Q & A


Adobe
SAML 2.0
A quick overview
Bē
Janne Parviainen

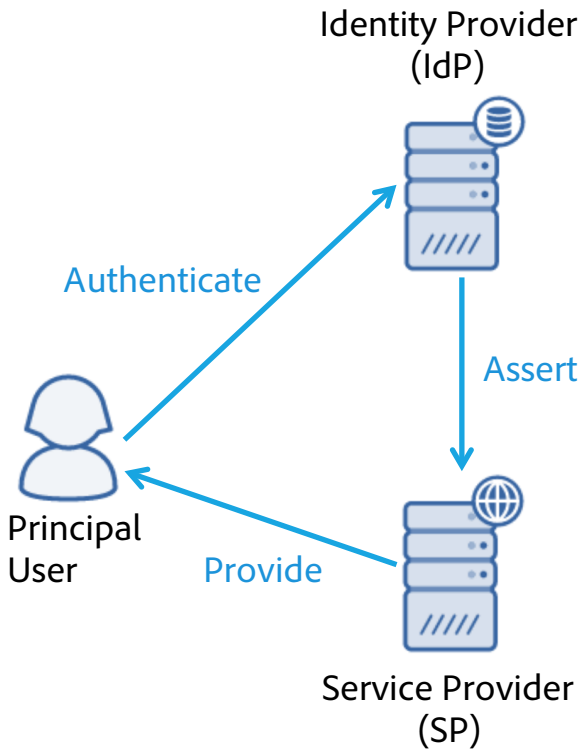
Overview of SAML 2.0

- Security Assertion Markup Language
- Open standard (OASIS) for Federated Identity implementations
- XML based Framework for exchanging authentication and authorization data across security domains
- Enables security use cases
  - Seamless cross domain browsing via Web Single Sign-On (SSO)
  - Attribute-Based Authorization
  - Securing Web Services

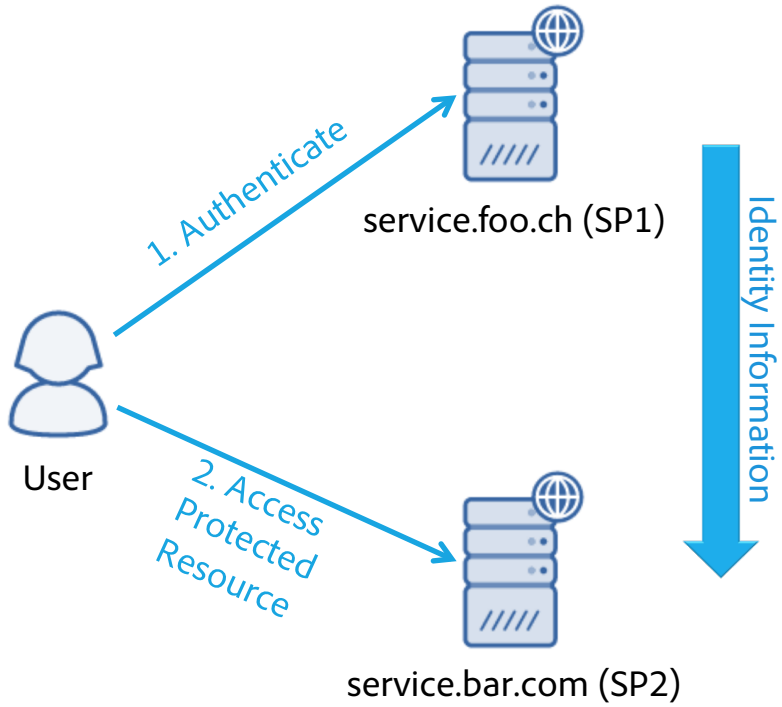
Source: [SAMLTech]

SAML Web SSO

Participants



Use case



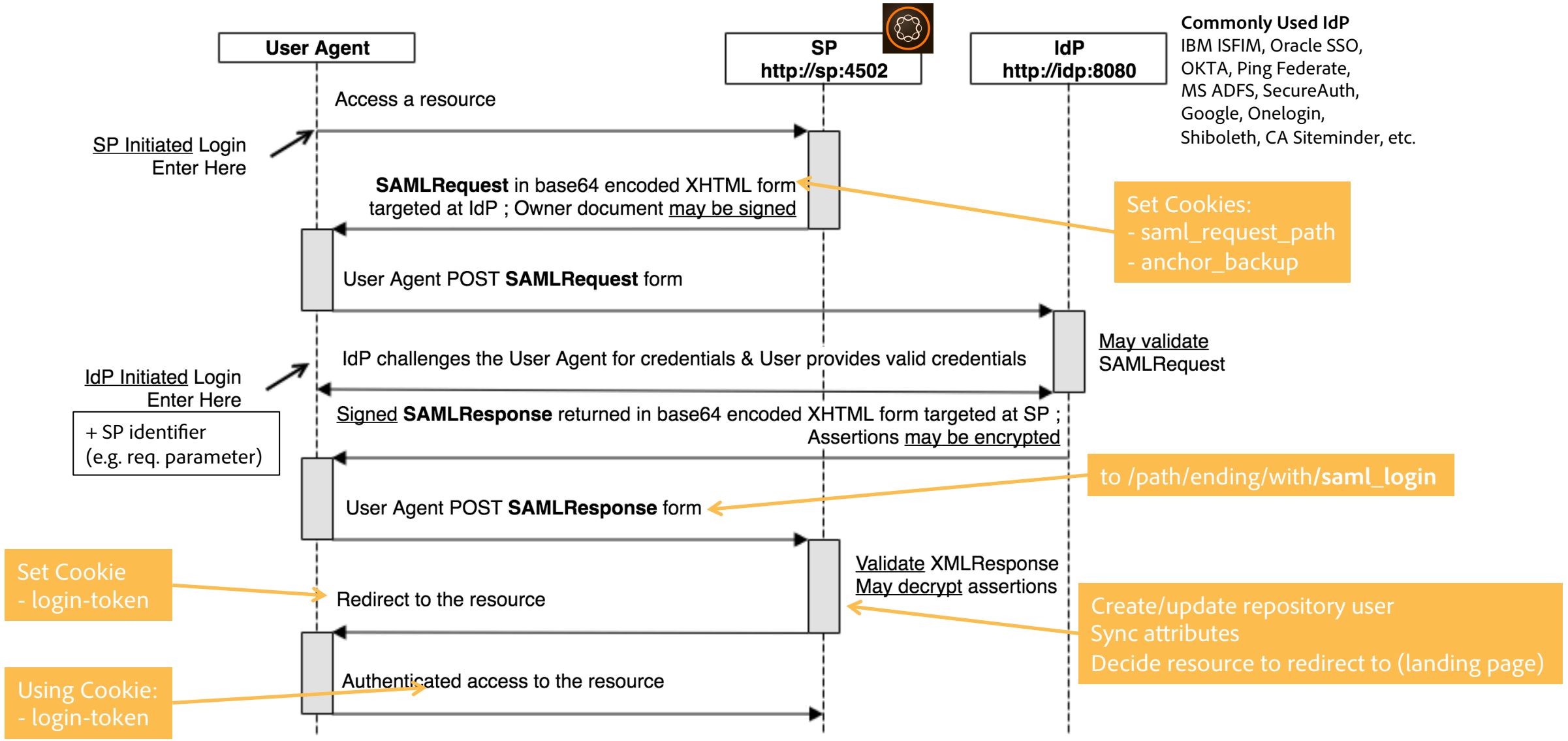
Source: [SAMLTech]


Adobe
AEM & SAML
Supported features
Bē
Janne Parviainen

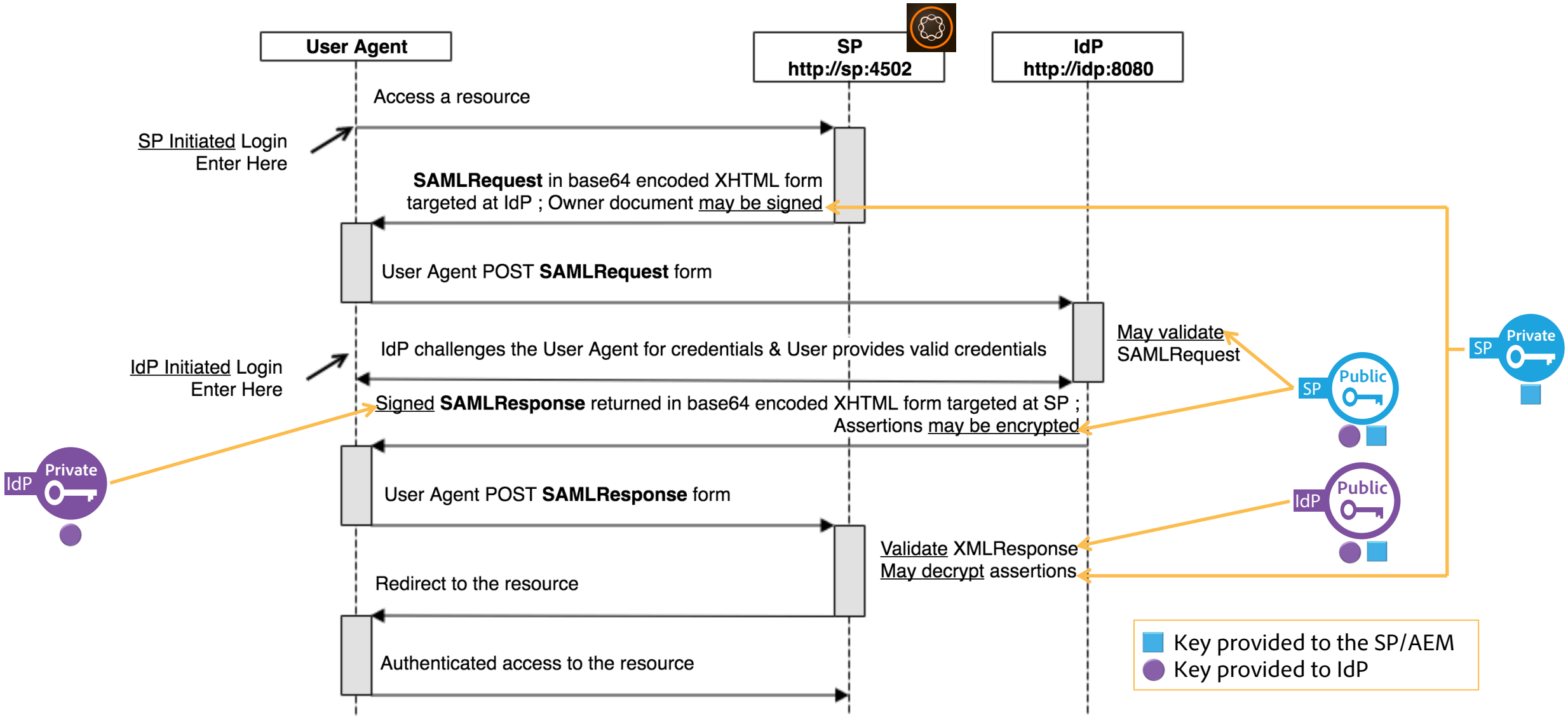
SAML features supported in AEM

SAML 2.0 standard	AEM authentication handler
Web Browser SSO Profile POST Binding SP & IdP initiated Single Sign-On (SSO)	Auto creation of users and assignment to groups
Single Logout Profile POST Binding SP & IdP initiated Single Log-Out (SLO)	Attribute synchronization
XML Signature	Multiple authentication handlers configurations
XML Encryption	Global and per request landing page
	Configurable clock drift compensation (HF 9985)

Web Browser SSO Profile



Security considerations (1/2)



Security considerations (2/2)

Security feature	Required	Description
Authentication & Integrity	Yes	Guarantees that the received assertions to have been emit by the trusted IdP and have not been modified Achieved using **XML Signature**
	No	Guarantee that the SAMLRequest has been emit by the trusted SP/AEM and the owner document has not been modified Achieved using **XML Signature**
Confidentiality	No	Assertions may contain sensitive data (e.g. PII data) which must only be read by the recipient Achieved • End to end using **XML Encryption** • Point to point using TLS (HTTPS)


Adobe
Configurations
Settings in typical deployments
Bē
Janne Parviainen

Security (1/4)

Authentication & Integrity

- Validating the origin and validating the integrity of the assertions (mandatory)

How

Key	Configuration
	Set the IdP certificate in the global TrustStore

SAML auth. handler property	Configuration
idpCertAlias	Set the alias of the IdP certificate in the global TrustStore

Security (2/4)

Confidentiality

- End-to-end confidentiality by encrypting the assertions (optional)

How

Key	Configuration
	Set the SP private key in the ‘authentication-service’ service user KeyStore
	Set the SP private key in the ‘authentication-service’ service user KeyStore

SAML auth. handler property	Configuration
useEncryption	Check if the authentication handler expects encrypted assertions
spPrivateKeyAlias	Set the alias of the SP certificate in the KeyStore
keyStorePassword	Set the password of the ‘authentication-service’ user KeyStore

Security (3/4)

Managing cryptographic keys

ⓘ Storing SP certificates and private key in the repository under the paths /etc/key/saml/[public|idp_cert|private] is no longer supported since the release com.adobe.granite.auth.saml-0.3.26 (DOC-8250, DOC-5509)

How

Set SP key pair in 'authentication-service' KeyStore

1. Browse /libs/granite/security/content/useradmin.html
2. Select the user 'authentication-service'
3. Create the KeyStore if needed
   Keep the KeyStore password for property keyStorePassword of SAML authentication handler configuration
4. Click on 'Manage KeyStore'
5. Upload the SP private key and public certificate
   Keep the private key alias for property spPrivateKeyAlias of SAML authentication handler configuration

Set IdP public key in global TrustStore

1. Browse /libs/granite/security/content/useradmin.html
2. Select any user
3. Create the global TrustStore if needed
4. Click on 'Manage TrustStore'
5. Upload IdP public certificate
   Keep the alias for property idpCertAlias of SAML authentication handler configuration

Private keys in PKCS12 or JKS format
Public keys in public certificate in PKCS#12, JKS or CER format

Security (4/4)

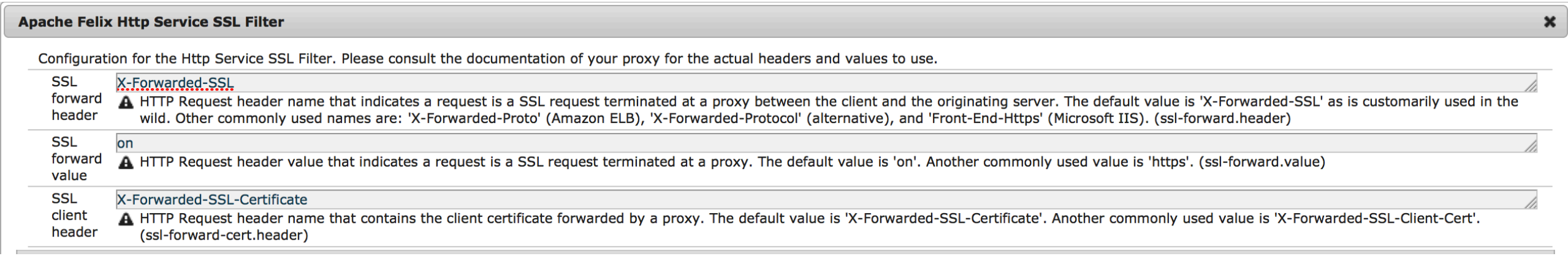
Deployment behind a dispatcher/LB

- ⓘ **Most deployments of SSL are terminated at the load balancer or at the dispatcher and communication to AEM instance happens over HTTP**

How

Make instances SSL context aware by configuring

http://host:port/system/console/configMgr/org.apache.felix.http.sslfilter.SslFilter



Auto creation of users

What

- AEM can automatically create non-existing AEM users on first login
- The user identifier and properties are derived from the assertions

How

SAML auth. handler property	Configuration
createUser	Check to enable the feature
userIDAttribute	Set the name of the attribute containing the user ID Leave empty to use the Subject:NameId attribute

Add user to groups

What

- AEM can automatically assign the user to the respective groups

How

SAML auth. handler property	Configuration
addGroupMemberships	Check to enable the feature
groupMembershipAttribute	Set the name of the attribute containing a list of AEM groups this user should be added to
defaultGroups	Set the list of default AEM groups users are added to after successful authentication ⓘ Attribute value is an array not a list of group names ⓘ Make sure neither default groups OR attribute containing AEM group is administrator ⓘ Prior to Granite-9432 SAML IdP would override any groups a user was added to manually on the AEM instance

Attributes synchronization

What

- AEM can store additional attributes from a SAML assertion in the repository (e.g. firstname, lastname, etc.)
- Synchronization happens during login

How

SAML auth. handler property	Configuration
synchronizeAttributes	Set the list of attribute from the SAML response to be stored at a path relative to the user node Example emailAddress=profile/email givenName=profile/givenName

Single Log-Out (SLO)

What

- AEM can close IdP and SP sessions upon logout
- IdP or SP Initiated SLO
- Attempt to logout all SP from the same session

How

SAML auth. handler property	Configuration
handleLogout	Check to enable the feature
logoutUrl	URL of the IdP where the SAML logout request should be sent to

- ⓘ Signin-out should be the same binding
- ⓘ Sensitive to clock drifts (HF 9985)

Landing page

What

- AEM supports specifying the path to redirect after successful login
- Narrow the focus on requested protected page

How

SAML auth. handler property	Configuration
defaultRedirectUrl	Set the default landing page path (only for IdP initiated login)

Cookie name	Value
saml_request_path	Use the cookie to define a request specific landing page path

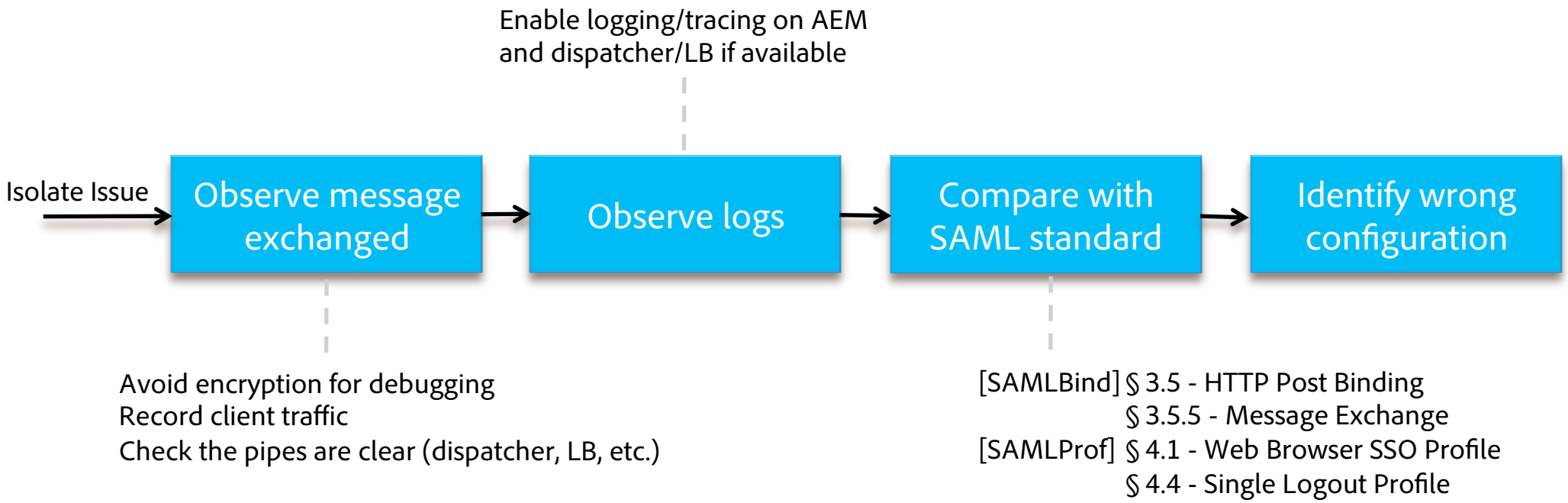
Order of priority

1. Cookie (saml_request_request)
2. SAML Authentication Handler redirect (defaultRedirectUrl)
3. Apache Sling default redirects


Adobe
Troubleshoot
How to analyze deployment issues
Bē
Janne Parviainen

Methodology

SAML deployments integrate multiple services supported by heterogeneous parties (companies, teams) connected with an open standard



Tools

On AEM

- Capture logs by enabling logging/tracing for the packages
  com.adobe.granite.auth.saml & **org.apache.sling.auth**

On client

- Record browsing session in HAR file
  https://help.tenderapp.com/kb/troubleshooting-your-tender-site/generating-an-har-file
- Observe SAML messages being transferred
  https://addons.mozilla.org/en-US/firefox/addon/saml-tracer

SAML 2.0

- Encrypting/decrypting, signing/validating, generating, SAML messages
  https://www.samltool.com/encrypt.php

Common mistakes

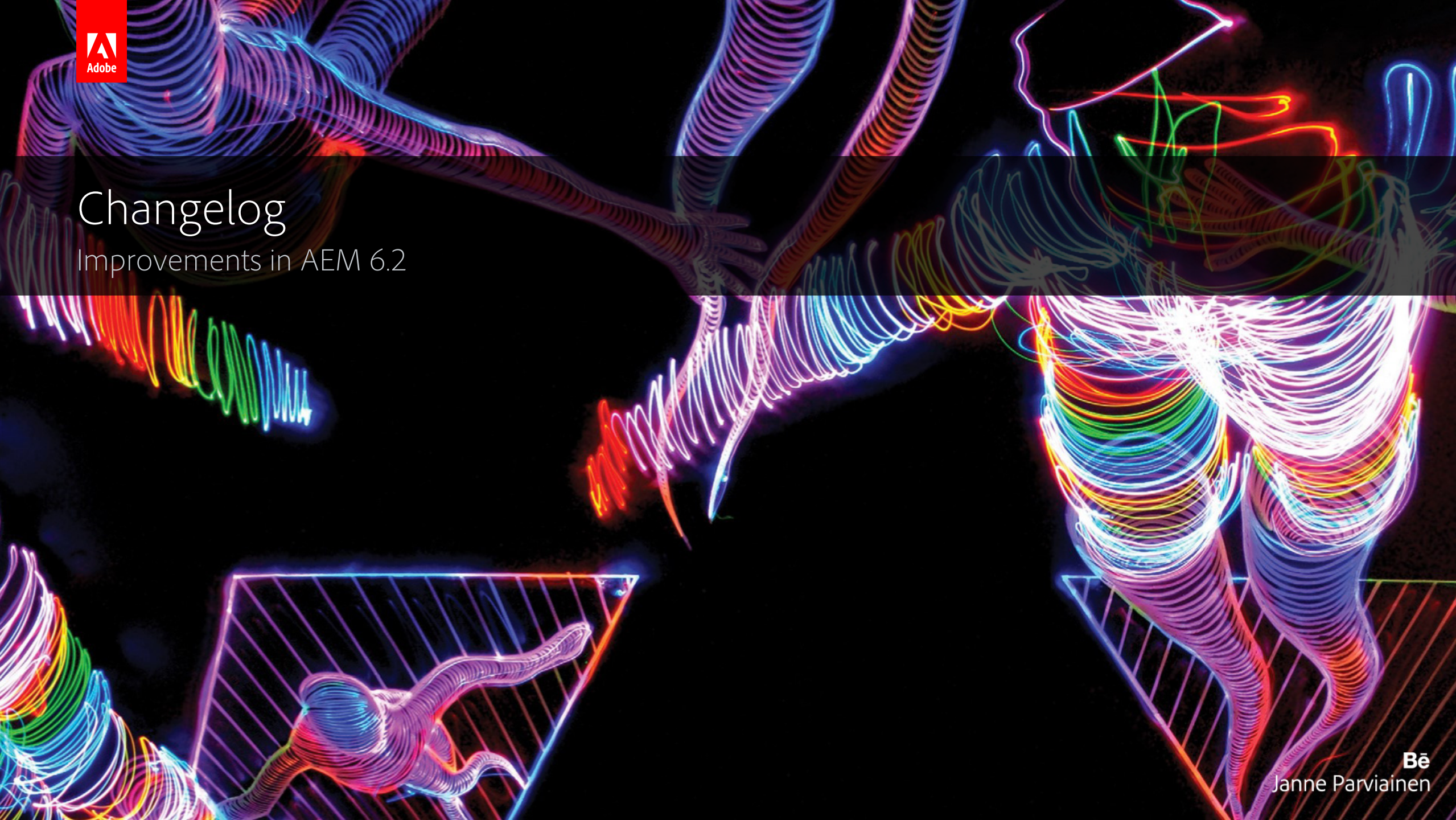
- Assertions not signed by the IdP
- Dispatcher/LB layer does not forward the saml_request_path cookie
- Missing/wrong session management with dispatcher enabling secure sessions
- IdP does not forward the saml_request_path cookie
- POST requests are cached at the dispatcher due to rewrite rules
- Consumption URL and entity id do not match
- HTTP SSL filter configuration does not retain the user in SSL protocol
- IdP does not support SLO (some don't, refer to IdP documentation)
- IdP server & AEM server not in sync with Internet time server (Configurable clock drift helps)

If allowAuthorized is set to '0' then add below session management section in dispatcher.any file

```
/sessionmanagement {
  /directory "<path>/.sessions"
  /encode "md5"
  /header "Cookie:login-token"
  /timeout "800"
}
```

Error & resolutions

Symptom	Common cause
HTTP ERROR: 403 Problem accessing /saml_login. Reason: Forbidden	The IdP hostname is not configured in Http Referer Filter
com.adobe.granite.auth.saml.model.Assertion Invalid Assertion: notOnOrAfter	Assertion not valid in time. IdP server & AEM server not in sync with Internet time server
com.adobe.granite.auth.saml.SamlAuthenticationHandler Private key of SP not provided: Cannot sign Authn request	It is a warning & can be ignored if not using encryption and the IdP accepts unsigned assertions
com.adobe.granite.auth.saml.util.SamlReader Failed validating signature	Signed SAML response signature not matching with IdP public certificate stored in AEM
javax.xml.crypto.dsig.XMLSignatureException: java.security.SignatureException: Signature length not correct: got 128 but was expecting 256	you are signing with a 1024-bit key but attempting to verify with a 2048-bit key
AccessDeniedException	One of the value of attribute containing a list of AEM groups is administrators


Adobe
Changelog
Improvements in AEM 6.2
Bē
Janne Parviainen

Improvements in AEM 6.2

- Release note
  https://docs.adobe.com/docs/en/aem/6-2/release-notes/wcm-platform.html

- SAML Handler should provide landing page in case of AEM side authentication errors
  GRANITE-8928

- SAML IdP Removes Users from Groups
  GRANITE-9432

- Configurable Clock drift compensation
  HF 11082, HF 9985

References

- SAML 2.0 Authentication Handler
  https://docs.adobe.com/docs/en/aem/6-2/administer/security/saml-2-0-authenticationhandler.html

- [SAMLProf] Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0
  https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

- [SAMLBind] Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0
  https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

- [SAMLTech] Security Assertion Markup Language (SAML) V2.0 Technical Overview
  https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

- SAML V2.0 Executive Overview
  https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf

Q & A

Adobe


Adobe