apigee

SAML

Google Cloud

(c)Apigee 2017. All rights reserved

Security Assertion Markup Language (SAML)

- exchange authentication and authorization information in XML format

(c)Apigee 2017. All rights reserved

Security Assertion Markup Language (SAML)

- exchange authentication and authorization information in XML format
- security assertions between:
  - Identity Provider - generates SAML tokens
  - Service Provider - validates SAML tokens

(c)Apigee 2017. All rights reserved

Security Assertion Markup Language (SAML)

- exchange authentication and authorization information in XML format
- security assertions between:
  - Identity Provider - generates SAML tokens
  - Service Provider - validates SAML tokens
- Apigee Edge acts as Identity Provider and Service Provider

(c)Apigee 2017. All rights reserved

Security Assertion Markup Language (SAML)

- exchange authentication and authorization information in XML format
- security assertions between:
  - Identity Provider - generates SAML tokens
  - Service Provider - validates SAML tokens
- Apigee Edge acts as Identity Provider and Service Provider
- support SAML Core Specification Version 2.0 and WS-Security SAML Token Profile specification Version 1.0

(c)Apigee 2017. All rights reserved

GenerateSAMLAssertion policy

- outbound token generation

GenerateSAMLAssertion policy

- outbound token generation
- attach SAML assertions to outbound XML requests

(c)Apigee 2017. All rights reserved

GenerateSAMLAssertion policy

- outbound token generation
- attach SAML assertions to outbound XML requests
- for authentication and authorization of the backend services

(c)Apigee 2017. All rights reserved

GenerateSAMLAssertion policy

- outbound token generation
- attach SAML assertions to outbound XML requests
- for authentication and authorization of the backend services
- can only be attached to the TargetEndpoint request Flow

(c)Apigee 2017. All rights reserved

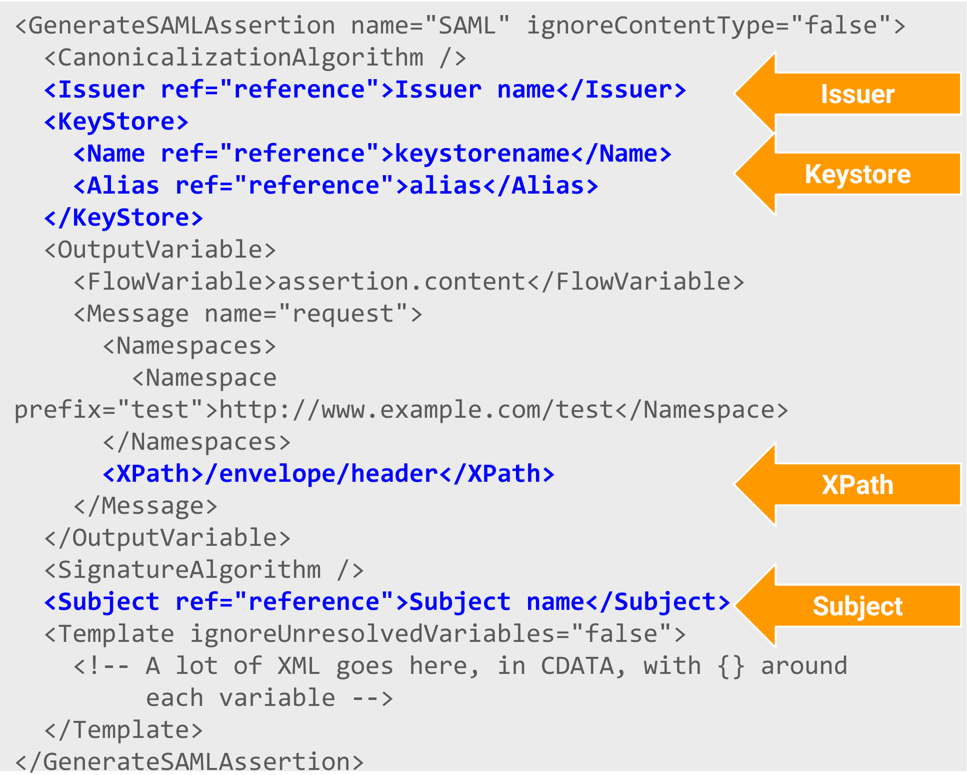
GenerateSAMLAssertion policy

- outbound token generation
- attach SAML assertions to outbound XML requests
- for authentication and authorization of the backend services
- can only be attached to the TargetEndpoint request Flow
- requires -
  - issuer
  - keystore
  - subject
  - xpath

apigee

(c)Apigee 2017. All rights reserved

GenerateSAMLAssertion policy



```
<GenerateSAMLAssertion name="SAML" ignoreContentType="false">
  <CanonicalizationAlgorithm />
  <Issuer ref="reference">Issuer name</Issuer>
  <KeyStore>
    <Name ref="reference">keystorename</Name>
    <Alias ref="reference">alias</Alias>
  </KeyStore>
  <OutputVariable>
    <FlowVariable>assertion.content</FlowVariable>
    <Message name="request">
      <Namespaces>
        <Namespace
prefix="test">http://www.example.com/test</Namespace>
      </Namespaces>
      <XPath>/envelope/header</XPath>
    </Message>
  </OutputVariable>
  <SignatureAlgorithm />
  <Subject ref="reference">Subject name</Subject>
  <Template ignoreUnresolvedVariables="false">
    <!-- A lot of XML goes here, in CDATA, with {} around
         each variable -->
  </Template>
</GenerateSAMLAssertion>
```

Issuer
Keystore
XPath
Subject

(c)Apigee 2017. All rights reserved

ValidateSAMLAssertion policy

- inbound authentication and authorization

(c)Apigee 2017. All rights reserved

ValidateSAMLAssertion policy

- inbound authentication and authorization
- validate SAML assertions to inbound SOAP requests.

  If valid, sets variables for further processing

ValidateSAMLAssertion policy

- inbound authentication and authorization
- validate SAML assertions to inbound SOAP requests.

  If valid, sets variables for further processing
- can only be attached to the ProxyEndpoint request

  Flow

(c)Apigee 2017. All rights reserved

ValidateSAMLAssertion policy

- inbound authentication and authorization
- validate SAML assertions to inbound SOAP requests. If valid, sets variables for further processing
- can only be attached to the ProxyEndpoint request Flow
- requires -
    - source
    - xpath
    - truststore

(c)Apigee 2017. All rights reserved

ValidateSAMLAssertion policy

```
<ValidateSAMLAssertion name="SAML" ignoreContentType="false">
  <Source name="request">
    <Namespaces>
      <Namespace
prefix='soap'>http://schemas.xmlsoap.org/soap/envelope/</Namesp
ace>
      <Namespace
prefix='wsse'>http://docs.oasis-open.org/wss/2004/01/oasis-2004
01-wss-wssecurity-secext-1.0.xsd</Namespace>
      <Namespace
prefix='saml'>urn:oasis:names:tc:SAML:2.0:assertion</Namespace>
    </Namespaces>

<XPath>/soap:Envelope/soap:Header/wsse:Security/saml:Assertion<
/XPath>
  </Source>
  <TrustStore>TrustStoreName</TrustStore>
  <RemoveAssertion>false</RemoveAssertion>
</ValidateSAMLAssertion>
```

Source

XPath

Truststore

Thank You

(c)Apigee 2017. All rights reserved

SAML for management server

- Edge Management Server for UI & API supports the following types of authentication
  - Basic Auth and Basic Auth with two-factor authentication
  - OAuth2
- Edge also supports SAML 2.0 as the authentication mechanism.
- You can generate OAuth2 tokens from SAML assertions returned by an identity provider.
- SAML supports a single sign-on (SSO) environment.
- SAML is supported as the authentication mechanism only for the Cloud version of Edge. It is not supported for Edge for the Private Cloud.

(c)Apigee 2017. All rights reserved