



Identity Federation key components

Click to edit subtitle

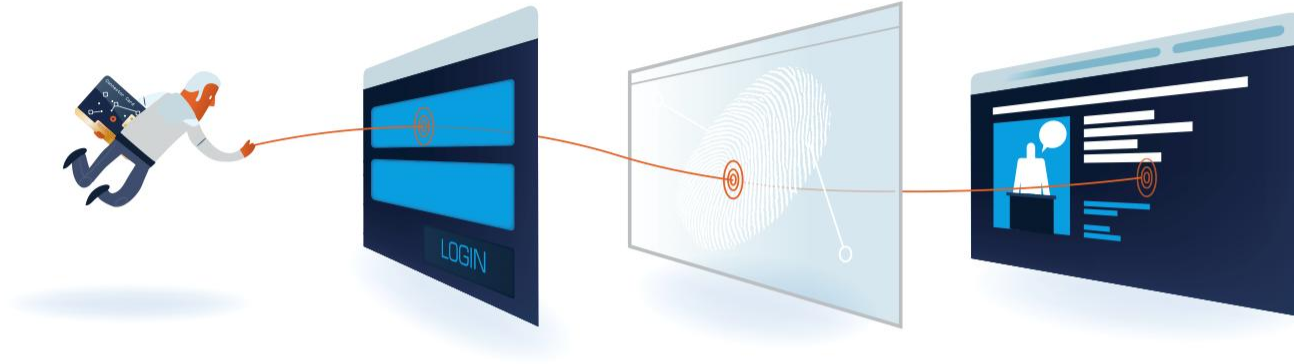
eduGAIN Training Team

GÉANT GN5-2

eduGAIN training for ngREN
April 2025

<Click to edit label> Public (PU) / Project Participants Sensitive (SEN)

Learning Objectives



01

What is SAML protocol?



02

The central role of SAML Metadata components



03

Attribute release concepts explained through examples



What is Security Assertion Markup Language (SAML)?

```

</ds:RSAKeyValue>
</ds:KeyValue>
<ds:X509Data>
  <ds:X509Certificate> MIIDDzCCAfcCFDrJjXj5buopQY/s+nY6EZszJFEnMA0GCSqGSIb3DQEBCwUAMEQxCzAJBgNVBAYT AklUMRYwFAYDVQQKDA1JREVNIEdBULIqQUFJMR0wGwYDVQQDDBRJREVNIEdGFkY:
  cJAEFw0yMTExMTkxMTEyMDFaFw0yNDExMTgxMTEyMDFaMEQxCzAJBgNVBAYTAKLUMRYwFAYDVQQK DA1JREVNIEdBULIqQUFJMR0wGwYDVQQDDBRJREVNIEdGFkYXRhIFNpZ25lcjCCASIwDQYJKoZI
  hvCNAQEBBQADggEPADCCAQoCggEBAMay3N21fswu3AE6hqCPUVjvCyol50KTHs9CXDIFyAoigP+Y SdloLSGwx6n6ks9aBbJqlzRBIEd3CpByvX7GmBuITL3ElhxMY40Cv/ULok1GbDmQMhPScU6J1f9b
  526R9Ks+BbYZYmBRX9gqmpX1R867IES4z+JhXnXr5K8HTPjfaDGh2x0RL6msXjwwDJgaJC0pBCct LvCWcmUp0ucpl8VHGjFAAI5Eb6pwQEEPj1yqW52ggM+AHNFY6bAC9RX7Qv8MonQZwXpNNBNL+Ucn
  GLVBXtBftd4zq7XxPNN9F/El3YJGa0Vvk8cCEJt5SfTerHaAyh8f/BfEs6CwucCSsCAWEAATAN BgkqhkiG9w0BAQsFAAOCAQEAne0JrkKQpkdyAKkLho4YNXHdKGex6KyEBPG0p/Ymg062LtwPpdC
  kmFoEaiZkn2NcfvTuP0Jyex4o0M0PDJqeq6EK0dGEXMr3Jd/e/hZLsm03HsvdCou3kn eA7k0tViMu9nLwORPGHeKuLd9H5I6EmCuDqgHq+EN2ooLB54xsAYK75LmgiW+CBoZCG/EPVGjmTR
  yoebeKNpAx0xIwpPF17jq4t2EB0ZNjoEODip2Wy0na38p+ws3H0VoD5WVkrSvLv DzedkmCm7UJ9HZYkxnmK6YVh4oghgBWfjRhqTLU6GGppIIJoqDYN8sayaRJHcw== </ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" creationInstant="2024-05-23T12:14:40.000Z" location="http://www.idem.garr.it/">
  <mdrpi:PublicationInfo>
    <mdrpi:RegistrationInfo registrationAuthority="http://www.idem.garr.it/" registrationPolicy="http://www.idem.garr.it/raw/ide-mrps-1.0.md" registrationTime="2024-05-23T11:00:00Z">
      <mdrpi:RegistrationPolicy xml:lang="en">https://www.idem.garr.it/raw/ide-mrps-1.0.md</mdrpi:RegistrationPolicy>
    </mdrpi:RegistrationInfo>
  </mdrpi:PublicationInfo>
</md:Extensions>
<EntityDescriptor xmlns:alg="urn:oasis:names:tc:SAML:metadata:alg:supp" xmlns:disc="http://www.w3.org/2000/09/xmldsig#" xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:
protocol" xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-init" xmlns:names="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdui="urn:oasis:names:tc:SAML:
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:shibmd="urn:mace:shibboleth:1.0:nameIdentifier" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
entityID="https://xploreuat.ieee.org/shibboleth-sp">
  <Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://www.idem.garr.it/" registrationPolicy="http://www.idem.garr.it/raw/ide-mrps-1.0.md" registrationTime="2024-05-23T11:00:00Z">
      <mdrpi:RegistrationPolicy xml:lang="en">https://www.idem.garr.it/raw/ide-mrps-1.0.md</mdrpi:RegistrationPolicy>
    </mdrpi:RegistrationInfo>
  </Extensions>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:2.0:protocol>
    <KeyDescriptor>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate> MIIcCuDCAaACCQDAKCYv5apLLTANBgkqhkiG9w0BAQsFADAeMRwwGgYDVQQDEXNp ZWVleHBsb3JlLmllZWUub3JmLm44XDTIyMDExMDExNzE2MTUx
          OVowHjEcMBoGA1UEAxMTaWVlZXhwbG9yZS5pZWVlLm9yZzCCASIwDQYJKoZIhvcN AQEBBQADggEPADCCAQoCggEBAMx0u0ovELST5WX50XZSDq/LpTRAzLmVSuNYTktO
          WNWfHf0XHN+8Lw4Z3UQUQeaoU00gJ88j0saLUXKEbTxDtTlVo0Csu4i8hks0ft Ym9OMPfghi1IaFMcGRErWx+GWPxaXkdMasIwwdcmL9iutVnIi5Rj0azihz0Wb4ZC
          Hlpw02czYAQL9XSweRm7gu32g4d2pVF/ls7IR2unI2UM5Rxp0UN/l8M8BjVaTj7X SQ9eyrVIUmK7fiYskdphLoD30xmQUXoj0gn9CaPsJSX4qNmjdDB3b5tPstlwMI+
          Zu4L/jMSdq6EmWz1ABR+eJZesoWvma/qMX0a5TilpZrSMnECAWEAATANBgkqhkiG 9w0BAQsFAAOCAQEAyBW9t7Ere0Tq2Ut18iD4RBcMVW2oyNG34lqmyzwA4NM35PlV
          sz4/Dwn2AXx4+oBd/27/Tq10f3S687KN0GxNKSEi3CGxArRG7CUuI0b7sY35JTBZ P+hIqpUpkhQP+Ppxpel1s0qkcpctqSdAm/w+MPczm4wXgPFJseWldvGvsQj++4Wn
          k0/GS1+3s/nolflrf8G60uDLgb/W6L8j4n6s6kqg/z1/E0+/Qy84otrPR9wcX25 GskE9LxyINZAYTU48VheqjuDd3gSy04axMYxttvcGa3c1qMkSr44Q9f9oTyApRT9 py2oI9VKC04U/S7EGIDloDFP03V0UN
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://xploreuat.ieee.org/Shibboleth/Shibboleth_sso/SAML2/POST" index="

```

What is SAML beyond a lot of XML?

What is Security Assertion Markup Language (SAML)?

- SAML 2.0 is the de facto standard for academic Identity Federations
- SAML 2.0 Web Browser Single Sign On Profile
- SAML2int Interoperable SAML 2.0 Profile





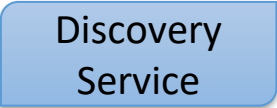
SAML Components

- **SAML Metadata** - an XML document representing SAML Entities

SAML Metadata Specification

- **SAML Metadata Consumer**
- **SAML Metadata Producer**

SAML Metadata Consumers/Producers

At the institution level	
	<ul style="list-style-type: none">• A SAML authority that authenticates users against a user repository• Retrieves information for the users in the form of attributes• Transfers the authentication event along with the attributes to a SAML Service Provider
	<ul style="list-style-type: none">• A SAML consumer that acts as a middleware in order to protect Web Applications• Consumes SAML messages from the Identity Provider and deduces authentication events and attributes
	<ul style="list-style-type: none">• The Discovery Service service, also known as "Where Are You From (WAYF)" service, lets the user choose his home institution from a list and then redirects the user to the login page of the selected institution for authentication.

SAML Metadata Consumers/Producers

At the NREN level	
Federation Registry	The system component that helps Federation Operators to register and manage entities. It could be used for collecting, processing and republishing federation metadata.
Central Discovery Service (optional)	A central Discovery Service, operated by Federation Operators to support and help their institutions to deploy services without having to deploy a discovery service at their level.

Federation Metadata

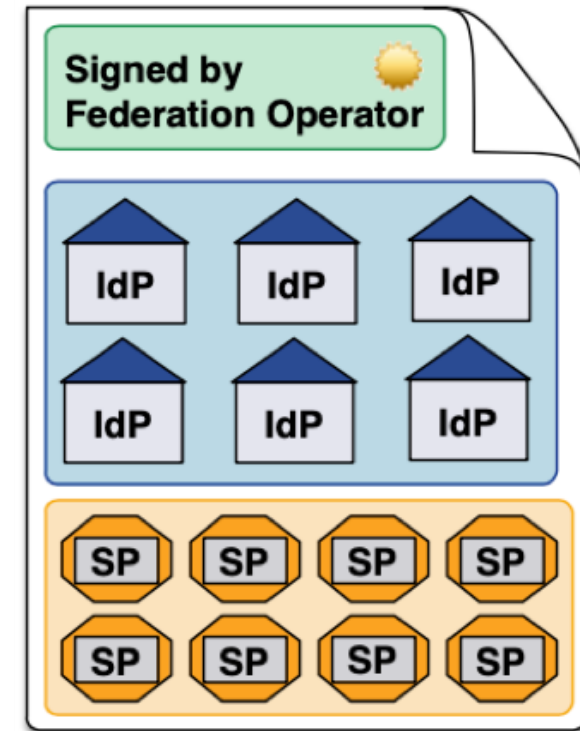
- The **federation Metadata** provides the technical trust in the federation
 - XML Documents defined by the SAML 2.0 standards
 - Generated by the Federation operators
 - Cryptographically signed by the Federations operators
 - Optionally transported over the internet using SSL
 - Contains technical information on all participating entities

Add Trust to Metadata

- **Consumers** of metadata must be sure that the metadata was really created by Federation Operator
- Therefore, **metadata must be secured**
- Two methods to secure metadata:
 - A. Recommended:** Add an **XML signature** on metadata and publish public signing key Metadata can be served via http in this case.
 - B.** Serve plain metadata via a **secure HTTPS URL**.
Make web server use a certificate issued by a well-known CA

Federation Metadata Structure

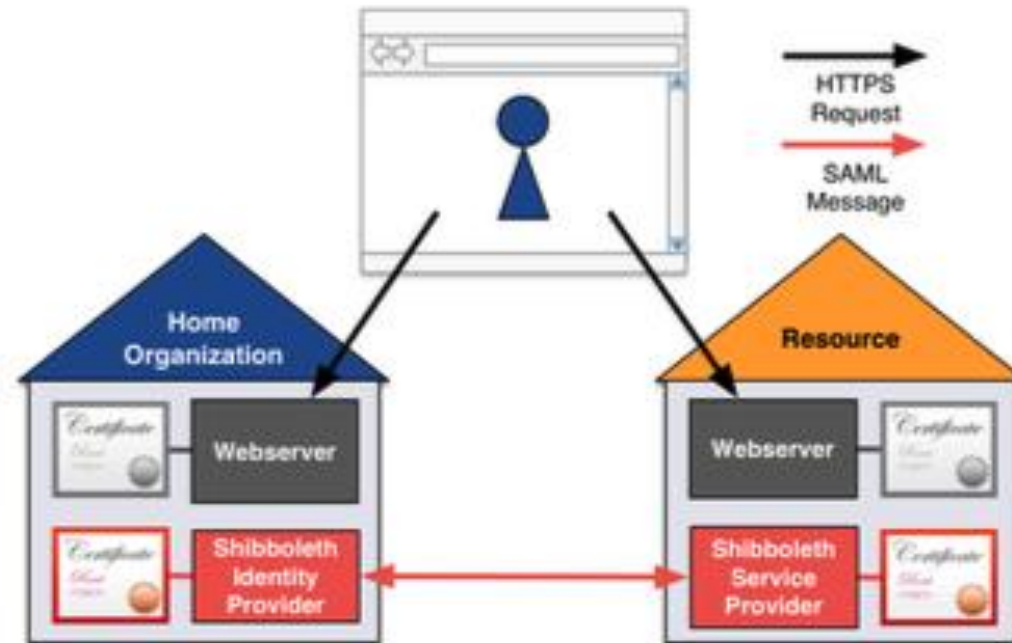
- To trust the metadata, it should be **protected** properly.
- No defined order of IdPs and SPs.
- Other entities could be described too. But mostly IdPs and SPs.



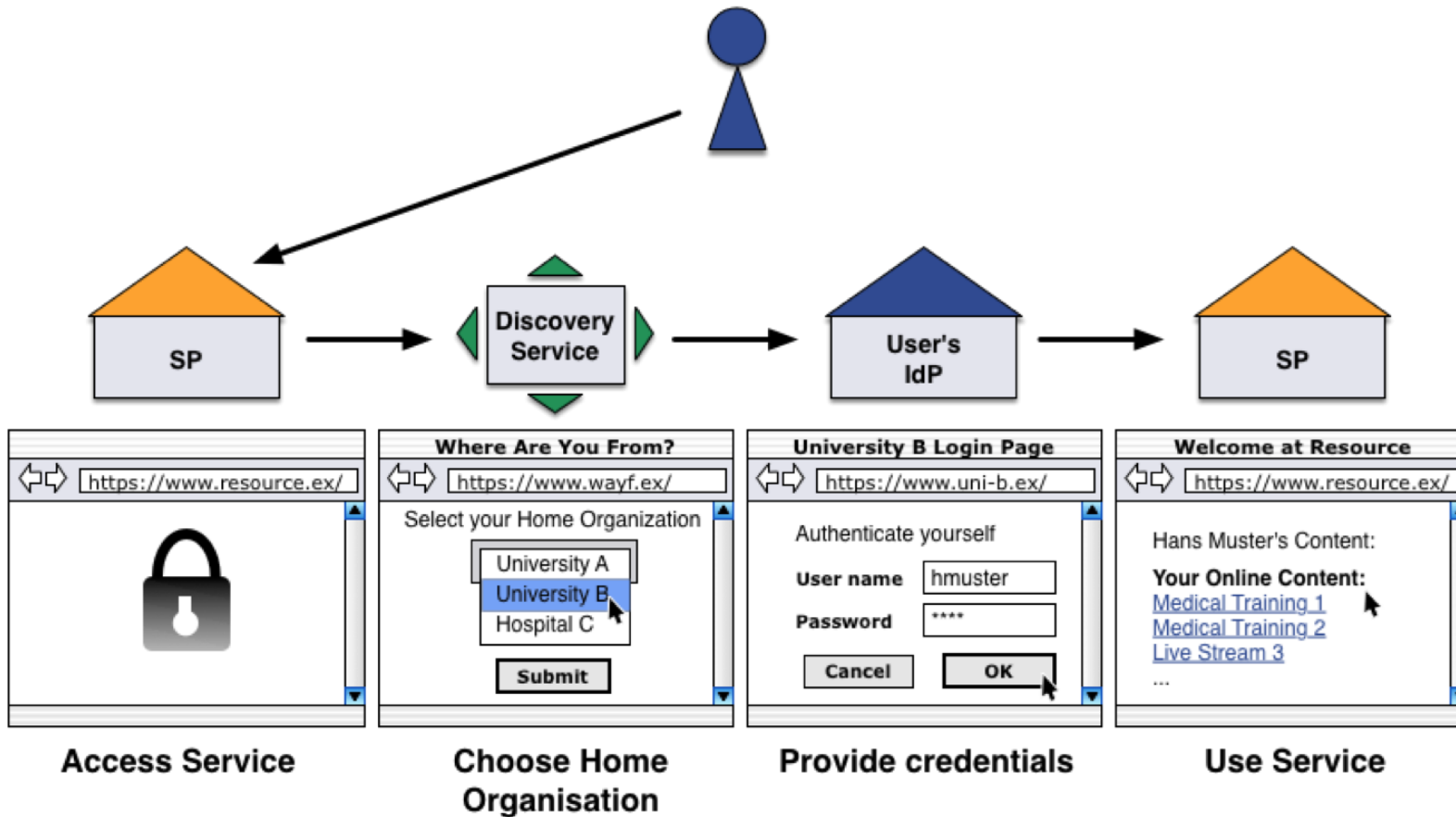
Certificates usage between IdPs and SPs

- **SSL/TLS** between the user's browser and the Web server:
 - indicates that the Web Service protects user data and ensures that the user is connected to an authentic site.
- **Self-signed certificate** (and private key) for signing/encrypting, with long lifetime (> 10y)
 - The signing of SAML assertions
 - Encryption of SAML assertions

Certificates usage between IdPs and SPs



Example of Authentication flow



SAML Authentication Flow

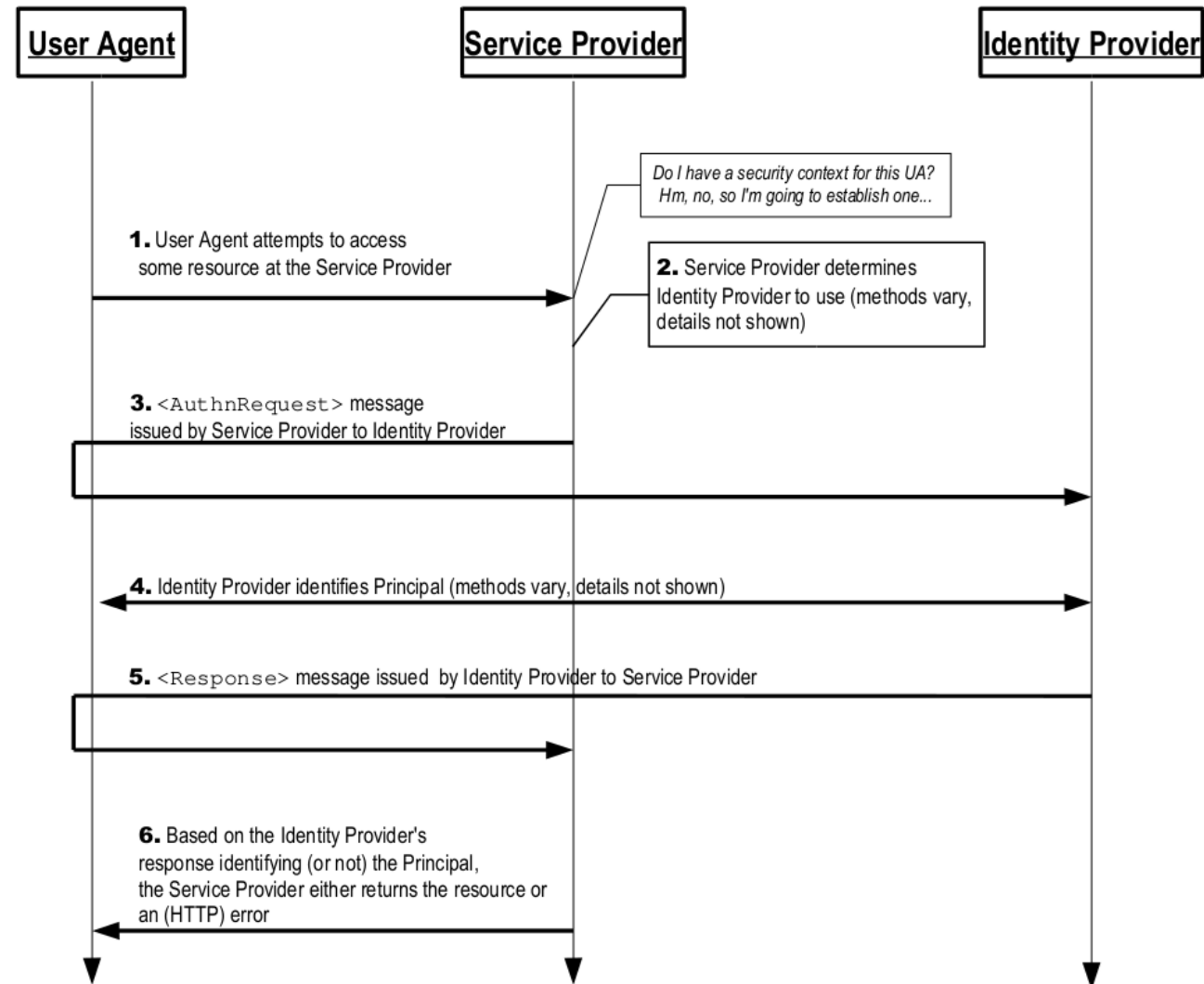


Figure 1

SAML Authentication Flow

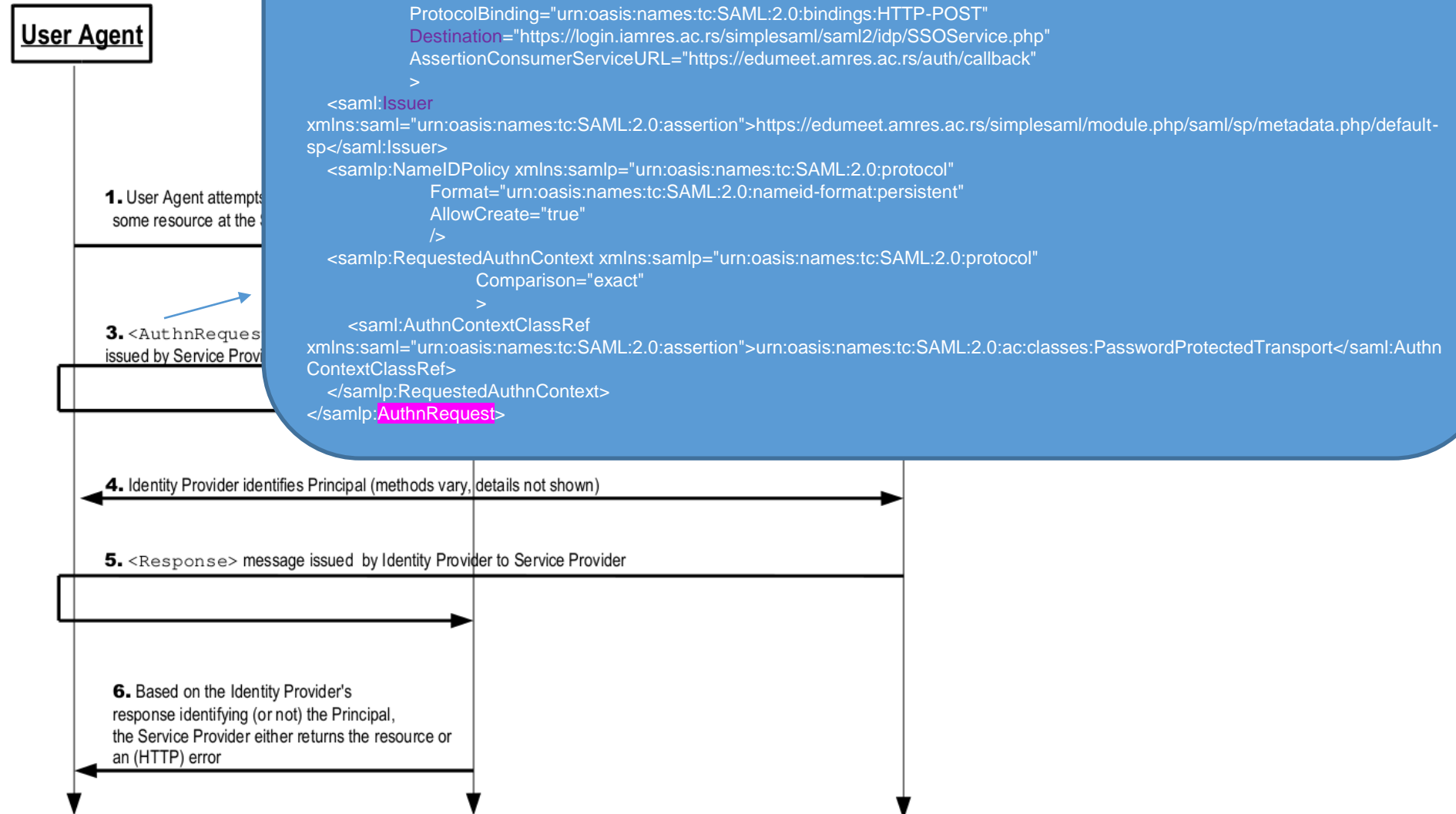
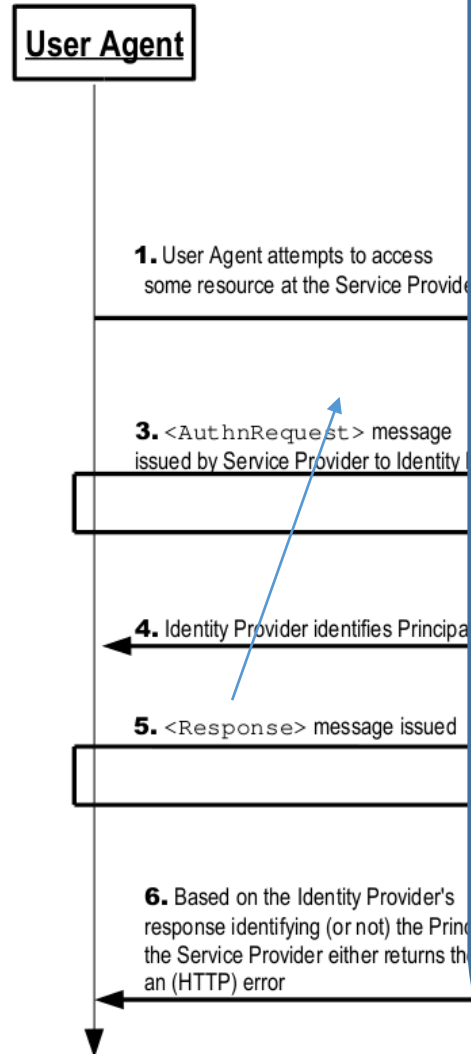


Figure 1

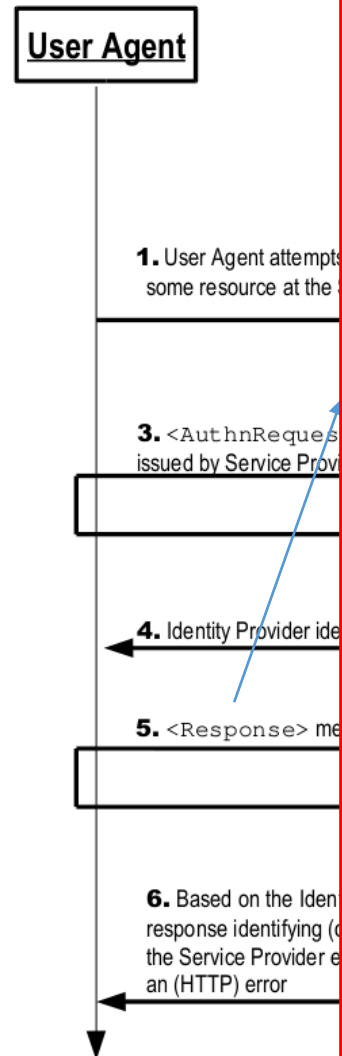
SAML Authentication Flow



```

<saml:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_9e642bc6de3c0e3884e56f6da46adbc4cbc1b1402f"
  Version="2.0"
  IssueInstant="20xx-02-24T17:03:59Z"
  Destination="https://edumet.ac.rs/auth/callback"
  InResponseTo="_77e997b22177e5e024d9"
>
<saml:Issuer>https://login.iamres.ac.rs</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="#_9e642bc6de3c0e3884e56f6da46adbc4cbc1b1402f">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
      <ds:DigestValue>QFOoZiWLYv32KPsSZv2s5OLR9orn+lbQ5QPIdy5TxfM=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue> XXX </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate> XXX </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  ID="_331d27fc03f54d27735ca401636b8fc10477d5d001"
  Version="2.0"
  IssueInstant="20xx-02-24T17:03:59Z"
>
  ...
</saml:Assertion>
</saml:Response>
  
```

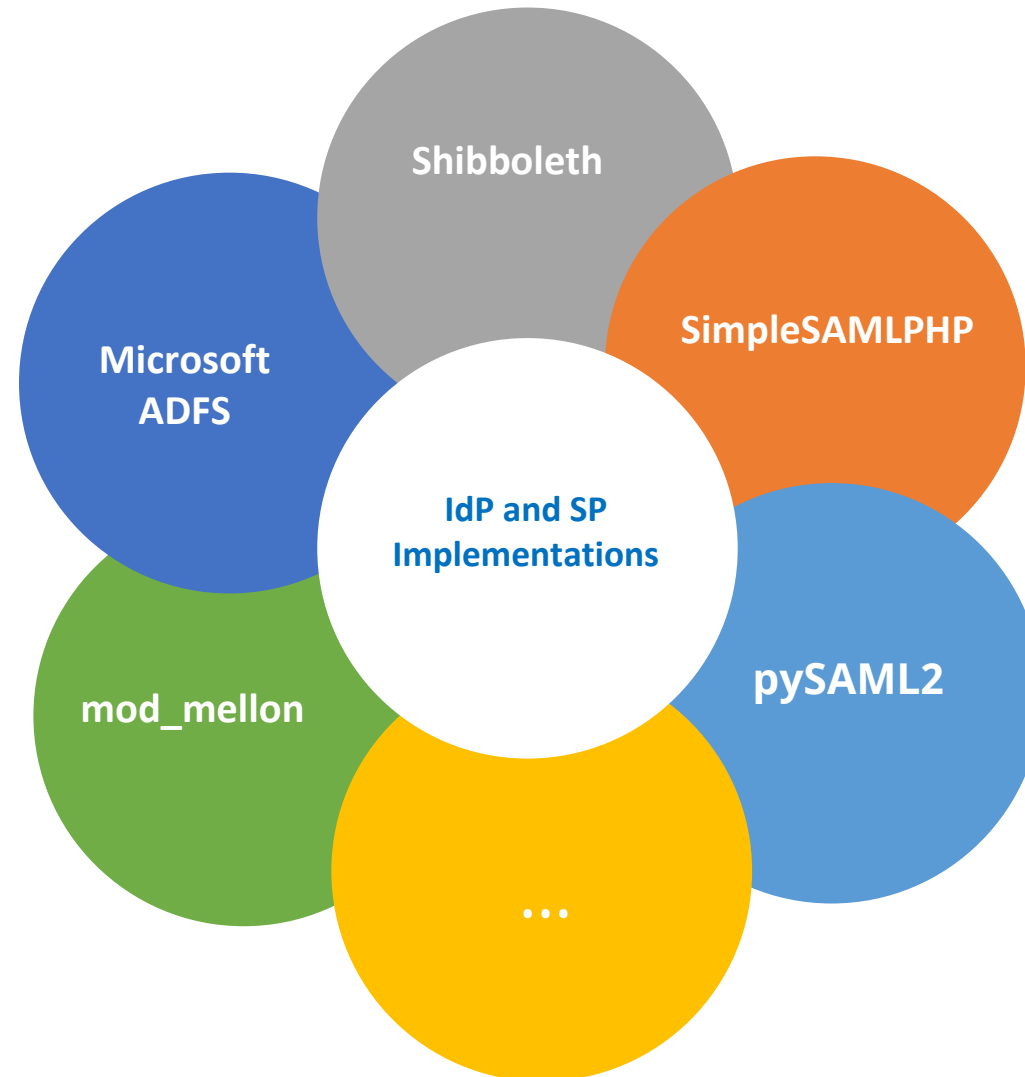
SAML Authentication Flow



```

<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  ID="_331d27fc03f54d27735ca401636b8fc10477d5d001"
  Version="2.0"
  IssueInstant="20xx-02-24T17:03:59Z"
  >
  <saml:Issuer>https://login.iamres.ac.rs</saml:Issuer>
  <ds:Signature ...
  </ds:Signature>
  <saml:Subject>
    <saml:NameID SPNameQualifier="https://edumet.amres.ac.rs/simplesaml/module.php/saml/sp/metadata.php/default-sp"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
      > xxx
    </saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData NotOnOrAfter="20xx-02-24T17:08:59Z"
        Recipient="https://edumet.amres.ac.rs/auth/callback"
        InResponseTo="_77e997b22177e5e024d9"
        />
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions ...
  </saml:Conditions>
  <saml:AuthnStatement ...
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      >
      <saml:AttributeValue xsi:type="xs:string">andrijana-test@amres.ac.rs</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      >
      <saml:AttributeValue xsi:type="xs:string">zaposleni</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
  
```

SAML2 IdP and SP Implementations



Introduction to Shibboleth



01

Origin

Internet2 in the US launched the open source project in 2000

02

Name

Word Shibboleth was used to identify members of a group

03

Standard

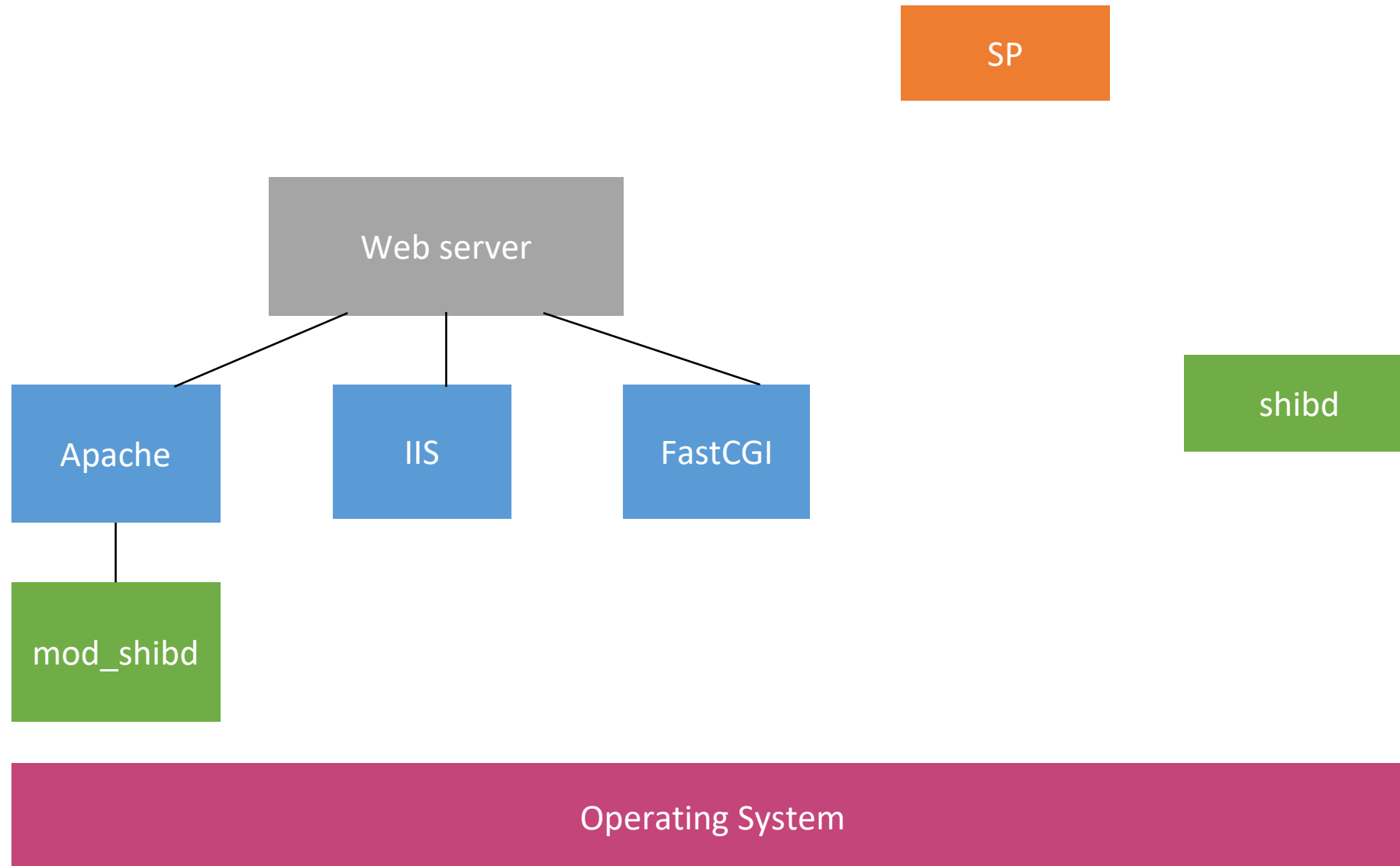
Based on Security Assertion Markup Language (SAML)

04

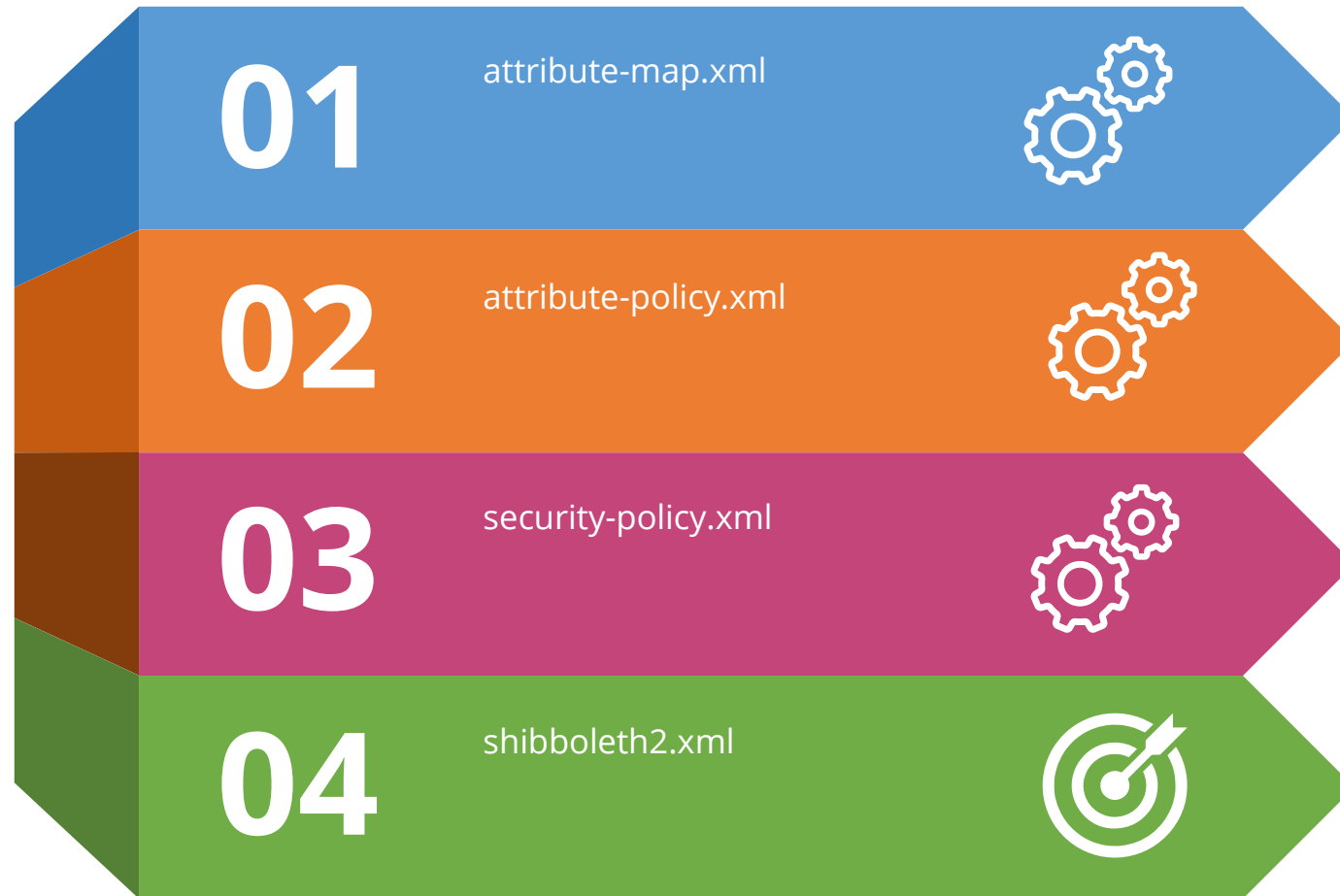
Consortium

The new home for Shibboleth development
Collect financial contributions from deployers worldwide

Shibboleth Service Provider



Shibboleth Service Provider



Shibboleth Identity Provider

- Authentication Engine
- Attribute Resolver
 - Attribute Registry
- Attribute Filter
- Metadata



Authentication

- Based on Spring Web Flow

- Login flows

- **Password**
- RemoteUser
- RemoteUserInternal
- X509
- X509Internal
- SPNEGO / Kerberos
- IPAddress
- External
- Function
- SAML (i.e. Proxying to other SAML IdP(s))
- Multi-Factor

Most popular

Where to specify which authentication flow to use ?

`/opt/shibboleth-idp/conf/authn/*`

`/opt/shibboleth-idp/conf/c14n/*`

Where can I find available flows ?

`/opt/shibboleth-idp/auth/...`

Attribute Resolver

- Sample files provided by default
 - `/opt/shibboleth-idp/conf/attribute-resolver.xml`
- It contains :
 - **DataConnectors**
 - **Attribute definitions**
- Attribute Resolver relies on Attribute Registry (attributes schemas and custom attr mappings)

DataConnectors

DataConnector Plugin Types

- Static
- ScriptedDataConnector
- ComputedId
- StoredId
- PairwiseId
- RelationalDatabase
- LDAPDirectory
- HTTP
- Subject
- StorageService
- EntityAttributes

```

<!-- ===== -->
<!--      Data Connectors      -->
<!-- ===== -->

<!--
Example LDAP Connector

The connectivity details can be specified in ldap.properties to
share them with your authentication settings if desired.
-->
<DataConnector id="myLDAP" xsi:type="LDAPDirectory"
  ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
  baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
  principal="%{idp.attribute.resolver.LDAP.bindDN}"
  principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
  useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}"
  connectTimeout="%{idp.attribute.resolver.LDAP.connectTimeout}"
  trustFile="%{idp.attribute.resolver.LDAP.trustCertificates}"
  responseTimeout="%{idp.attribute.resolver.LDAP.responseTimeout}">
  <FilterTemplate>
    <![CDATA[
      %{idp.attribute.resolver.LDAP.searchFilter}
    ]]>
  </FilterTemplate>
  <ConnectionPool>
    minPoolSize="%{idp.pool.LDAP.minSize:3}"
    maxPoolSize="%{idp.pool.LDAP.maxSize:10}"
    blockWaitTime="%{idp.pool.LDAP.blockWaitTime:PT3S}"
    validatePeriodically="%{idp.pool.LDAP.validatePeriodically:true}"
    validateTimerPeriod="%{idp.pool.LDAP.validatePeriod:PT5M}"
    expirationTime="%{idp.pool.LDAP.idleTime:PT10M}"
    failFastInitialize="%{idp.pool.LDAP.failFastInitialize:false}" />
</DataConnector>

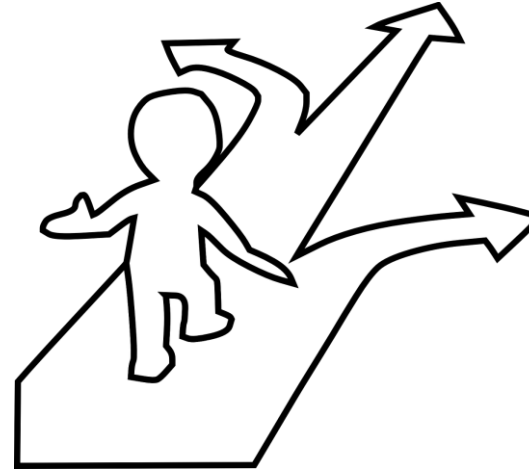
```

Attribute Definitions

Attribute Definition

- Simple
- PrincipalName
- Scoped
- Prescoped
- RegexSplit
- ScriptedAttribute
- Mapped
- Template
- SubjectDerived
- ContextDerived
- Decrypted

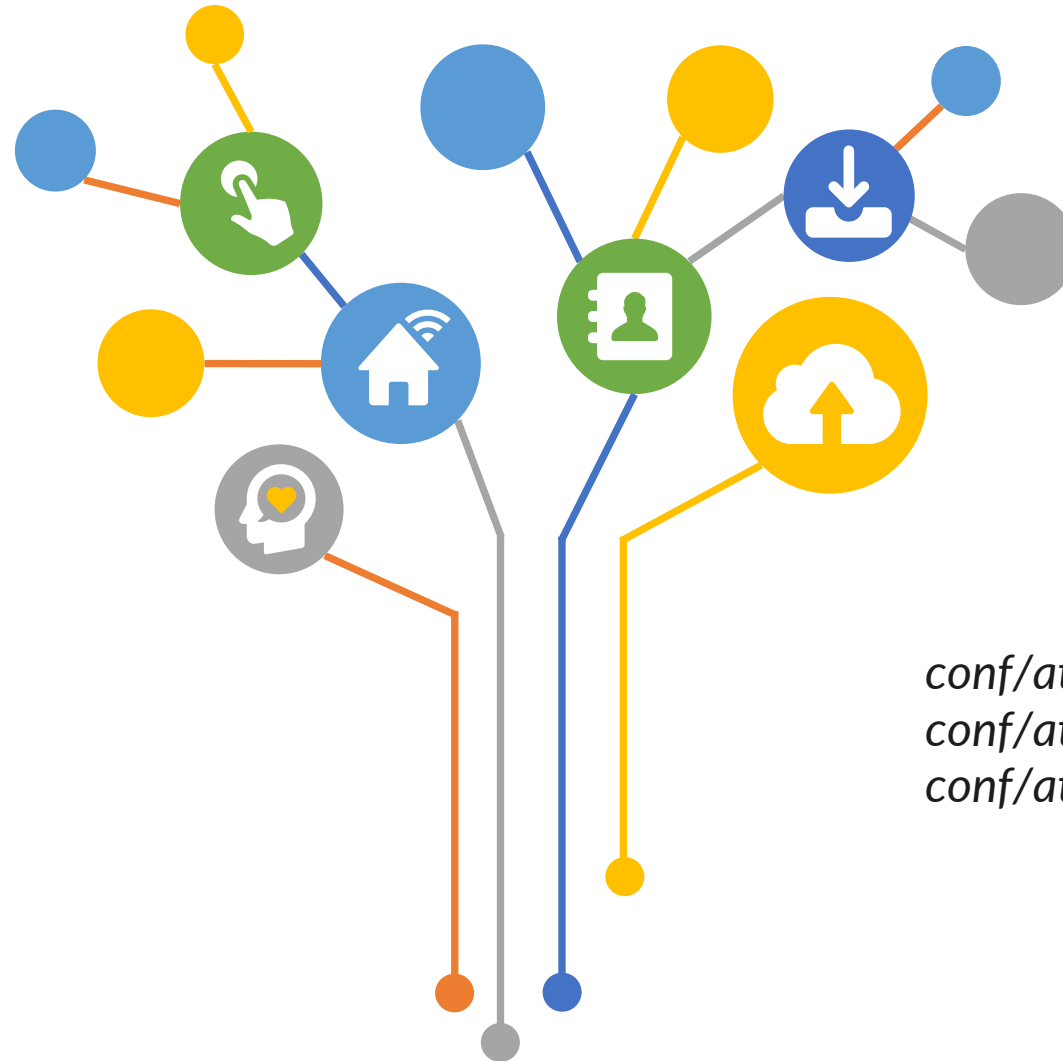
Which Attribute Definition to choose?



Attribute Registry

Attribute Schemas

- samlSubject.xml
- eduCourse.xml
- inetOrgPerson.xml
- eduPerson.xml
- schac.xml
- Custom schemas



*conf/attribute-registry.xml,
conf/attributes/default-rules.xml,
conf/attributes/custom/*

Attribute Filter

- Sample files provided by default
 - `/opt/shibboleth-idp/conf/attribute-filter.xml`
 - Defines rules for each SP
 - Defines rules for each attribute
- Use of Dynamic Filter configuration:
 - Requested attributes could be shared in the metadata (SP or federation metadata)
 - IdPs can be configured to release automatically these attributes if available in metadata

Identifiers Attributes

- Properties of identifiers:
 - Uniqueness
 - Reassignability
 - Opacity
 - Persistency
 - Targetedness
 - Transientness
- Types of identifiers:
 - **Persistent NameID**
 - **eduPersonPrincipalName**
 - **eduPersonTargetedID**
 - **eduPersonUniqueid**
 - **eduPersonOrcid**
 - **subject-id**
 - **pairwise-id**



Thank You

www.geant.org



Co-funded by
the European Union