Standards for Interoperable OSS Access Management

SAML and OIDC Proxy based FIM architectures and solutions based on Open Source Software

TIIME 2020

2020/02/18

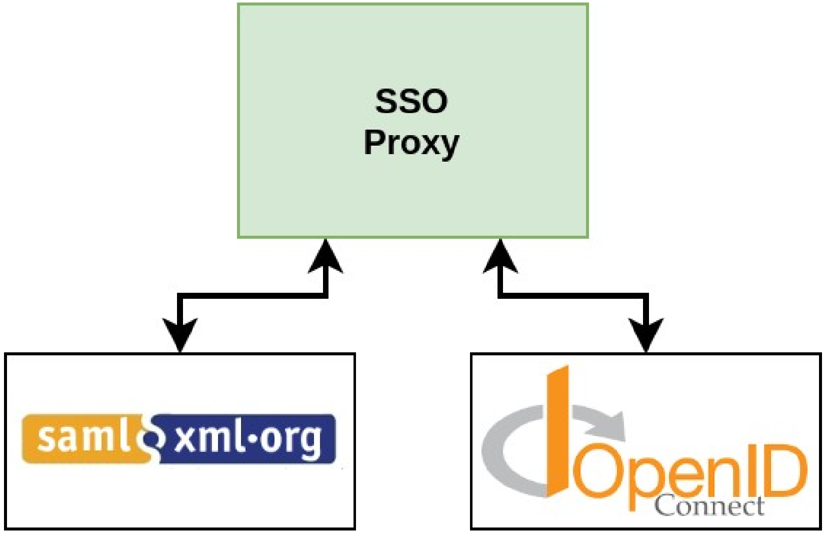
David Hübner
DAASI International GmbH

saml xml·org

OpenID
Connect

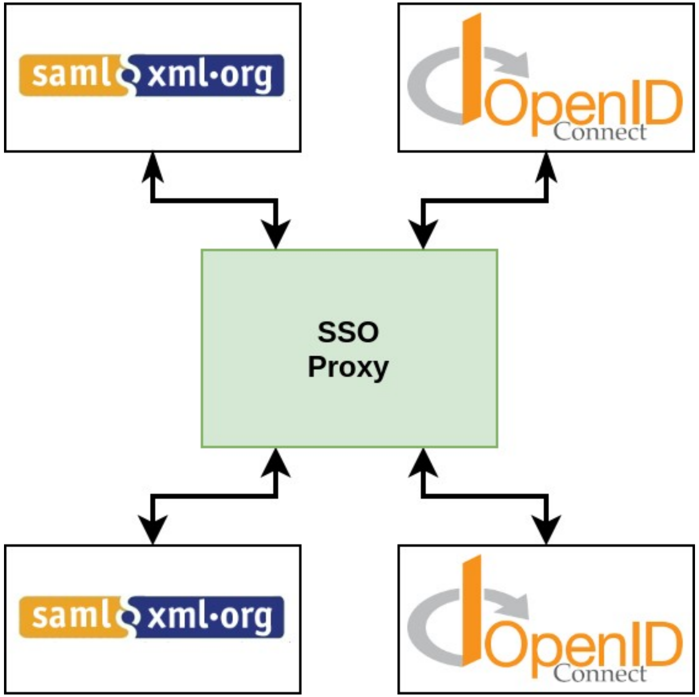
OAUTH
2
OAUTH

Multi-Protocol SSO

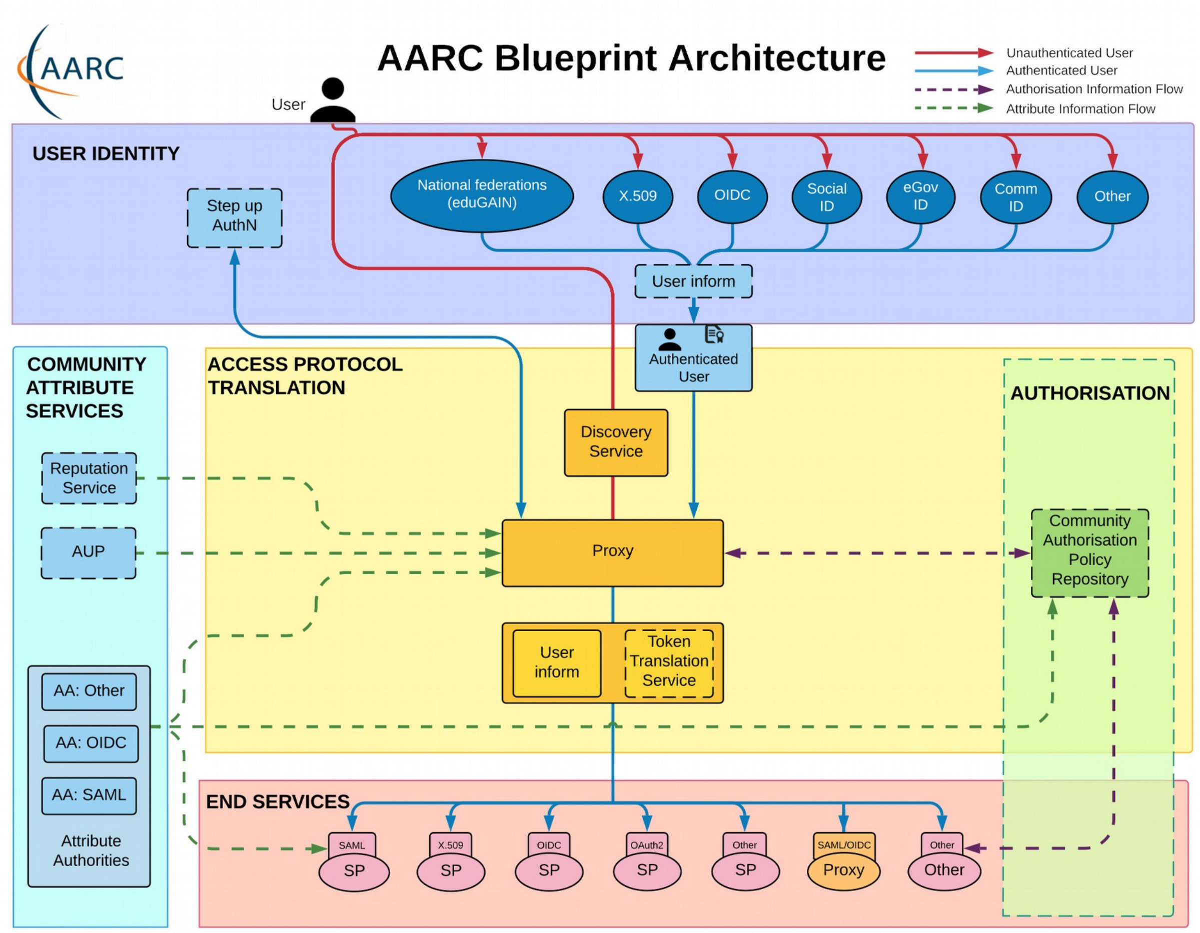


SSO
Proxy

Proxy-based Scenarios



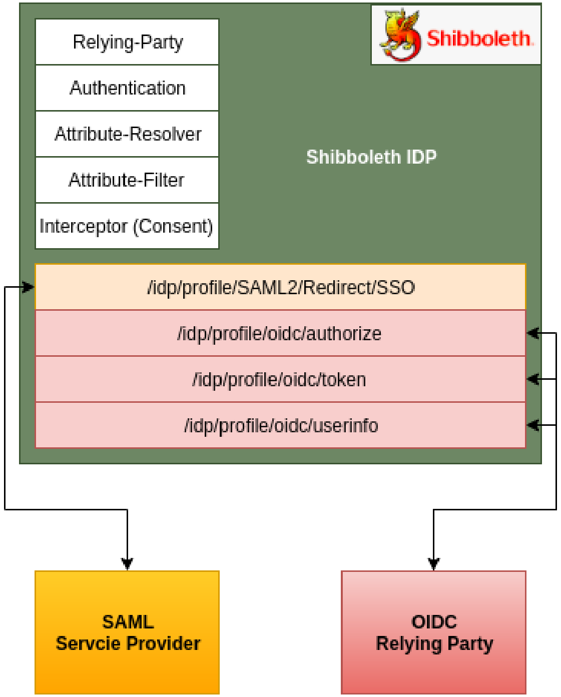
The AARC BPA


AARC
AARC Blueprint Architecture
Unauthenticated User
Authenticated User
Authorisation Information Flow
Attribute Information Flow
User
USER IDENTITY
Step up AuthN
National federations (eduGAIN)
X.509
OIDC
Social ID
eGov ID
Comm ID
Other
User inform
Authenticated User
COMMUNITY ATTRIBUTE SERVICES
Reputation Service
AUP
AA: Other
AA: OIDC
AA: SAML
Attribute Authorities
ACCESS PROTOCOL TRANSLATION
Discovery Service
Proxy
User inform
Token Translation Service
AUTHORISATION
Community Authorisation Policy Repository
END SERVICES
SAML
SP
X.509
SP
OIDC
SP
OAuth2
SP
Other
SP
SAML/OIDC
Proxy
Other
Other

Different Software Solutions

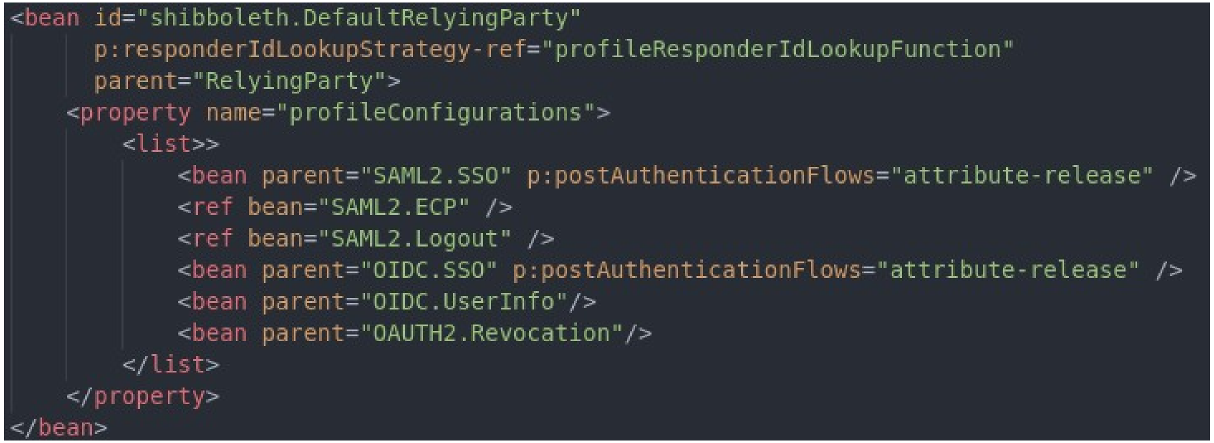
- Shibboleth IDP
- Gluu
- Satosa / didmos Authenticator

Shibboleth IDP & OIDC Extension

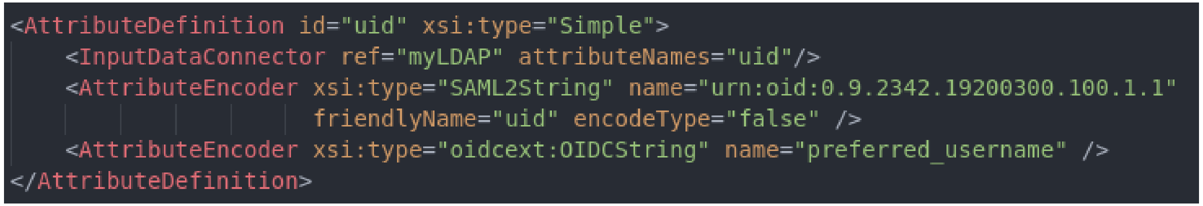


Relying-Party
Authentication
Attribute-Resolver
Attribute-Filter
Interceptor (Consent)
Shibboleth IDP
/idp/profile/SAML2/Redirect/SSO
/idp/profile/oidc/authorize
/idp/profile/oidc/token
/idp/profile/oidc/userinfo
SAML
Servcie Provider
OIDC
Relying Party

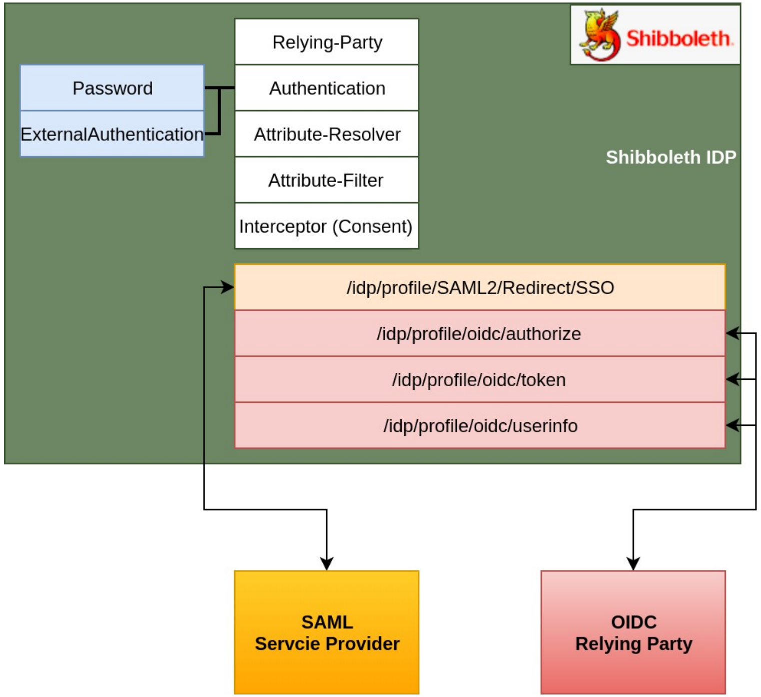
Configuration



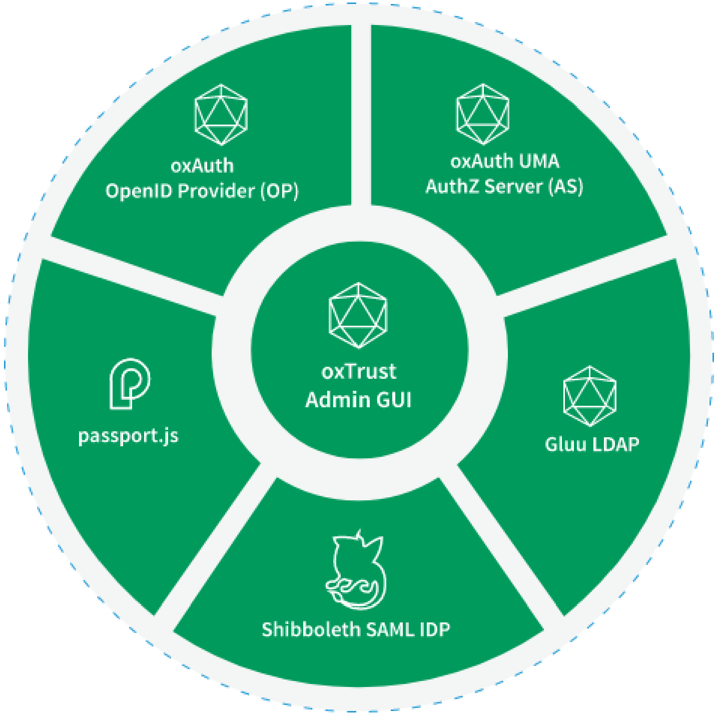
```
<bean id="shibboleth.DefaultRelyingParty"
      p:responderIdLookupStrategy-ref="profileResponderIdLookupFunction"
      parent="RelyingParty">
    <property name="profileConfigurations">
        <list>>
            <bean parent="SAML2.SSO" p:postAuthenticationFlows="attribute-release" />
            <ref bean="SAML2.ECP" />
            <ref bean="SAML2.Logout" />
            <bean parent="OIDC.SSO" p:postAuthenticationFlows="attribute-release" />
            <bean parent="OIDC.UserInfo"/>
            <bean parent="OAUTH2.Revocation"/>
        </list>
    </property>
</bean>
```



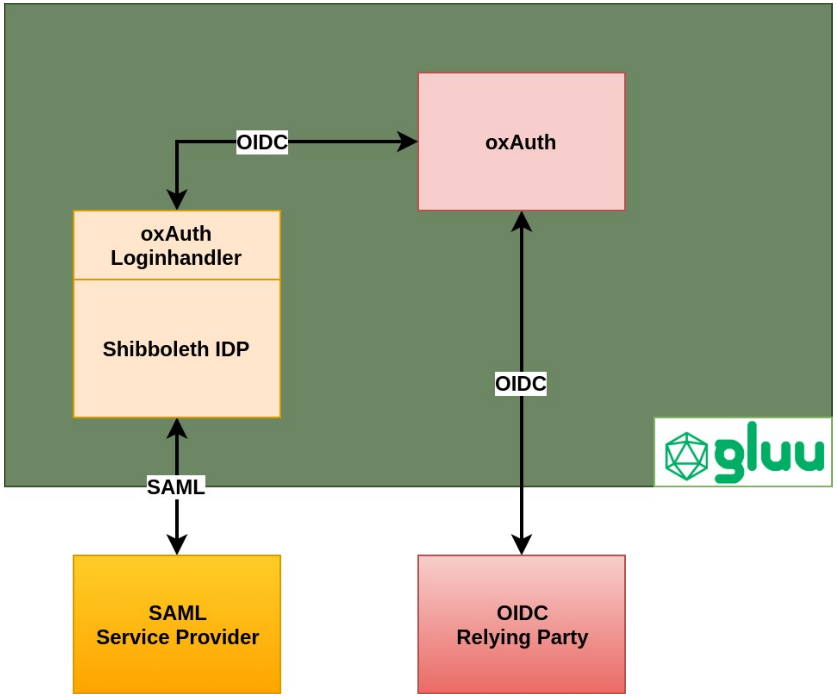
```
<AttributeDefinition id="uid" xsi:type="Simple">
    <InputDataConnector ref="myLDAP" attributeNames="uid"/>
    <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1"
                      friendlyName="uid" encodeType="false" />
    <AttributeEncoder xsi:type="oidcext:OIDCString" name="preferred_username" />
</AttributeDefinition>
```

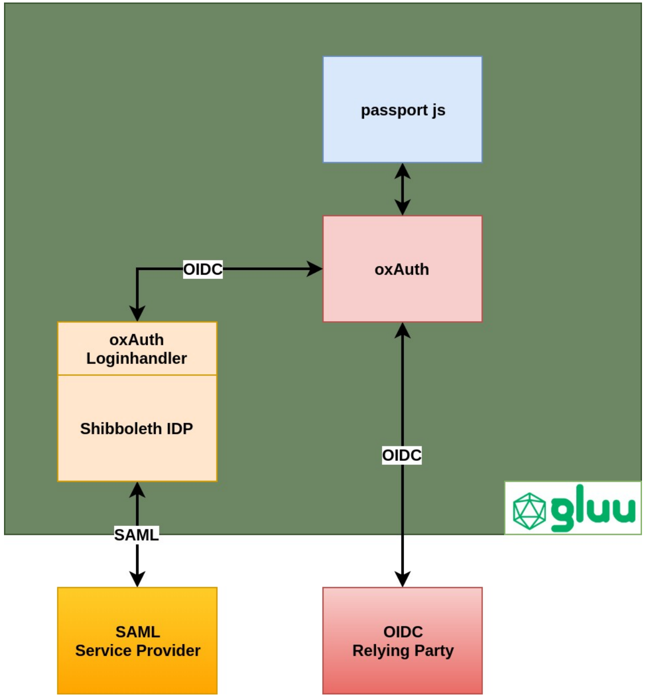

Relying-Party
Authentication
Attribute-Resolver
Attribute-Filter
Interceptor (Consent)
Password
ExternalAuthentication
Shibboleth
Shibboleth IDP
/idp/profile/SAML2/Redirect/SSO
/idp/profile/oidc/authorize
/idp/profile/oidc/token
/idp/profile/oidc/userinfo
SAML
Servcie Provider
OIDC
Relying Party

Components in Gluu

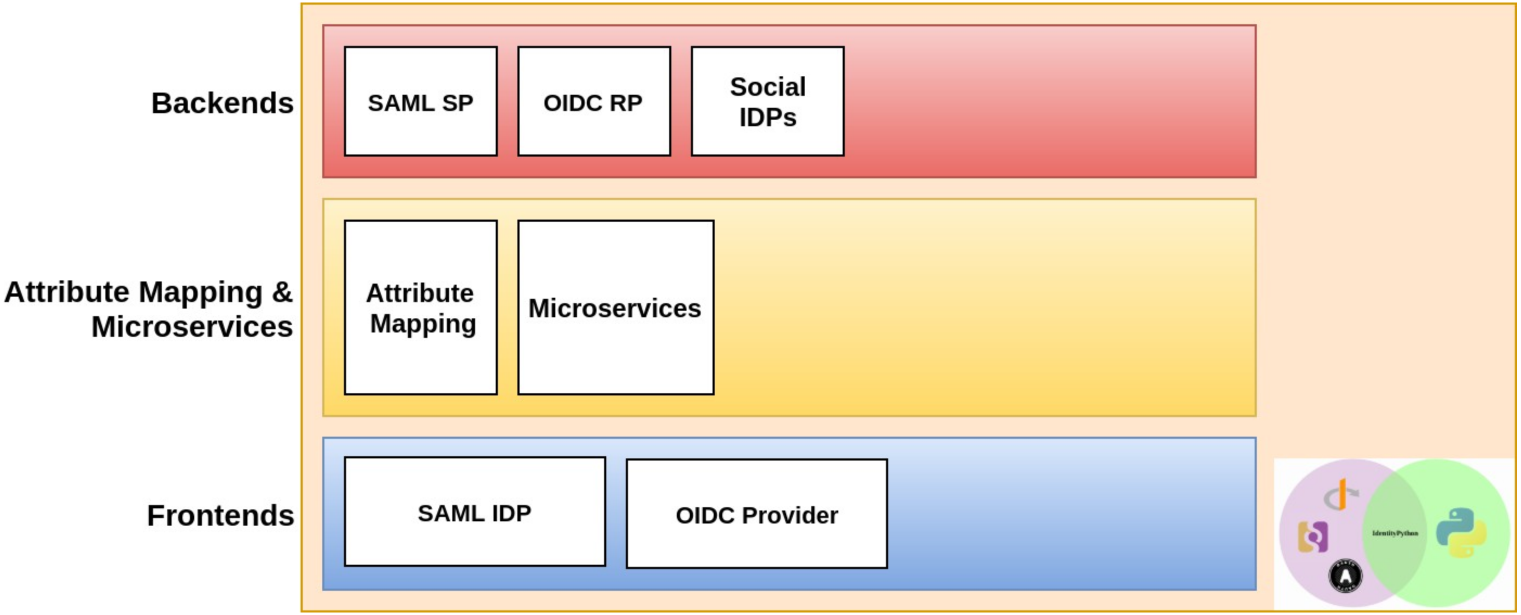


Gluu


oxAuth
OIDC
oxAuth Loginhandler
Shibboleth IDP
OIDC
gluu
SAML
SAML Service Provider
OIDC Relying Party


passport js
OIDC
oxAuth
oxAuth Loginhandler
Shibboleth IDP
OIDC
gluu
SAML
SAML Service Provider
OIDC Relying Party

Satosa



Backends

- SAML SP
- OIDC RP
- Social IDPs

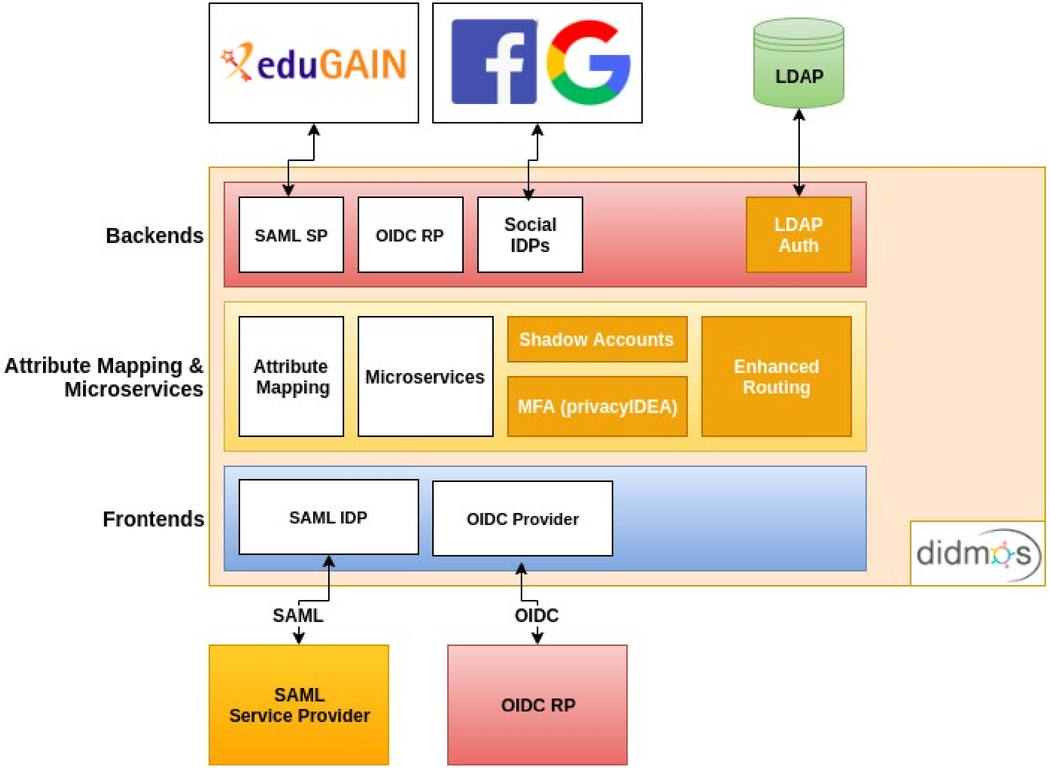
Attribute Mapping & Microservices

- Attribute Mapping
- Microservices

Frontends

- SAML IDP
- OIDC Provider

Example Use-Case: didmos Authenticator



Summary

Shibboleth	gluu	didmos IdentityPython
• Easy to extend existing Shibboleth IDP deployment with OpenID Provider capabilities • Widespread in R&E and beyond	• Extensive OAuth2 capabilities & configuration parameters • Scalability & HA scenarios	• Modular approach allows for easy extensions • Lightweight • Close to research in R&E

Thank you!

David Hübner

DAASI International

www.daasi.de

david.huebner@daasi.de