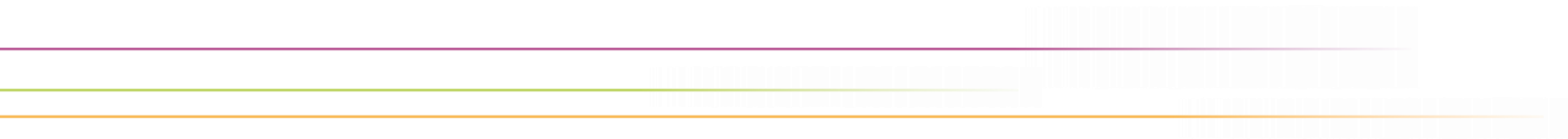


deutsches forschungsnetz



IAM Basics + Federating Services

NFDI AAI Workshop March 7th, 2023

Wolfgang Pempe (pempe@dfn.de)



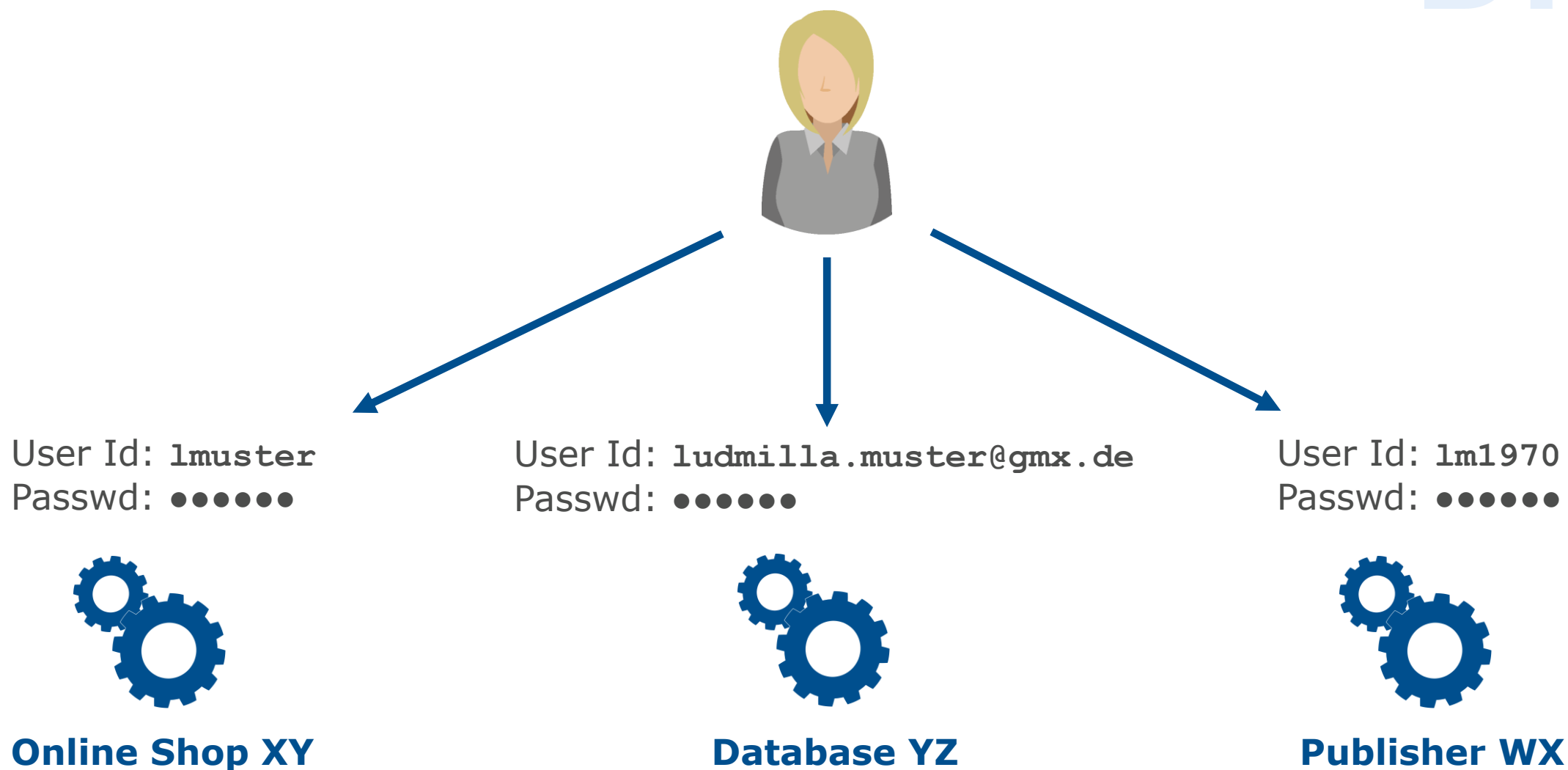
Agenda

- ▶ Introduction to Identity and Access Management
- ▶ Overview Federated Identity Management and Federations
- ▶ Standards: SAML and OpenID Connect
- ▶ Trust and Levels of Assurance
 - Break --
- ▶ RDMO Use Case
- ▶ AARC Blueprint Architecture and Community AAI
- ▶ NFDI Basic Service IAM and NFDI AAI
- ▶ Federating Services with Shibboleth SP

Federated Identity Management and Identity Federations

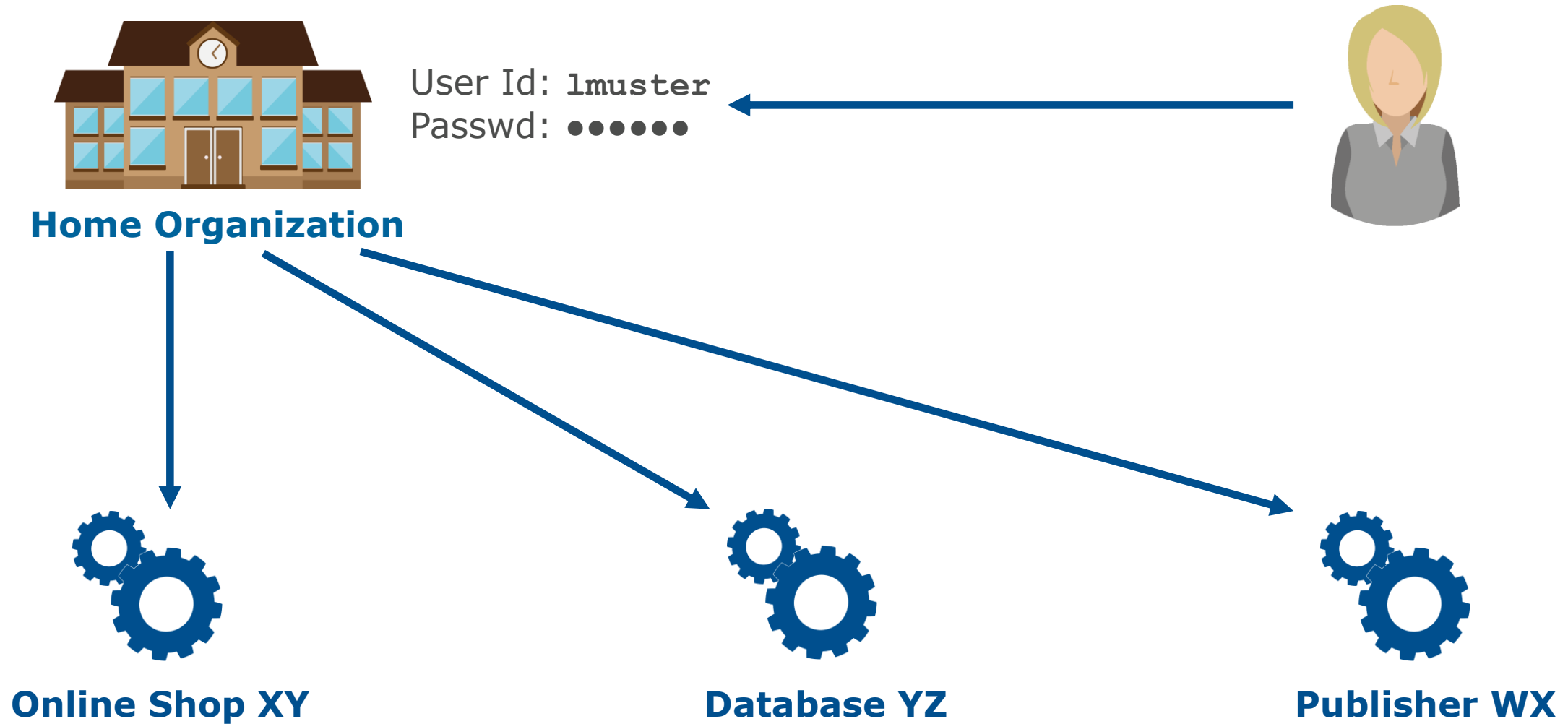


Service-specific Identities



Federated Identity

DFN

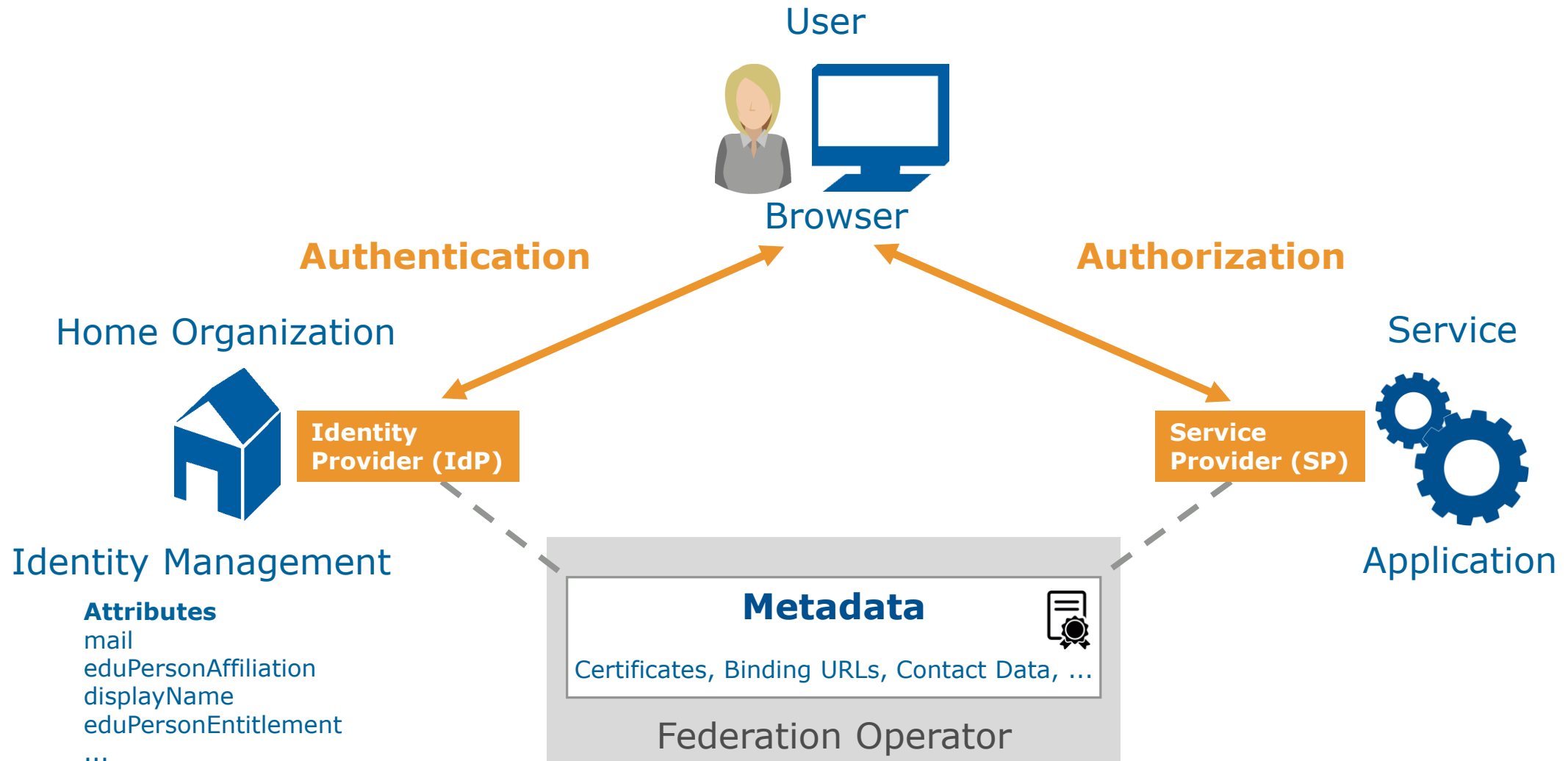


Definition of Terms

- ▶ Federated Identity Management
 - ▶ Exchange of identity data across service and organisational boundaries
 - ▶ Avoidance of service-specific identities/accounts and credentials
 - ▶ One identity source as leading system (usually the IdP of the Home Organization)
- ▶ AAI = **A**uthentication and **A**uthorization **I**nfrastructure
 - ▶ The technical and organizational framework for federated identity management
- ▶ AAI enables **S**ingle **S**ign-**O**n (SSO)
 - ▶ Log in once to access all services I'm entitled to use
 - ▶ Usually relevant for web-based applications, but there are also solutions for non-web szenarios

- ▶ Federated identity management requires a central instance (“trusted third party”):
Federation Operator
 - ▶ Defines the organizational, technical and legal framework conditions
 - ▶ ensures/enforces compliance with them
 - ▶ and establishes the relationship of trust within the federation
- ▶ DFN Association is operator of the cross-institutional federation DFN-AAI
 - ▶ Target group: Higher education and research institutions
 - ▶ DFN holds contracts with about 420 Research and Education Institutions
 - ▶ plus more than 200 contracts with external Service Providers (commercial and non-commercial)
- ▶ The concept of Federation allows for hierarchies:
inter-federation (eduGAIN), sub-federations (bwIDM, IDM.nrw, ...)

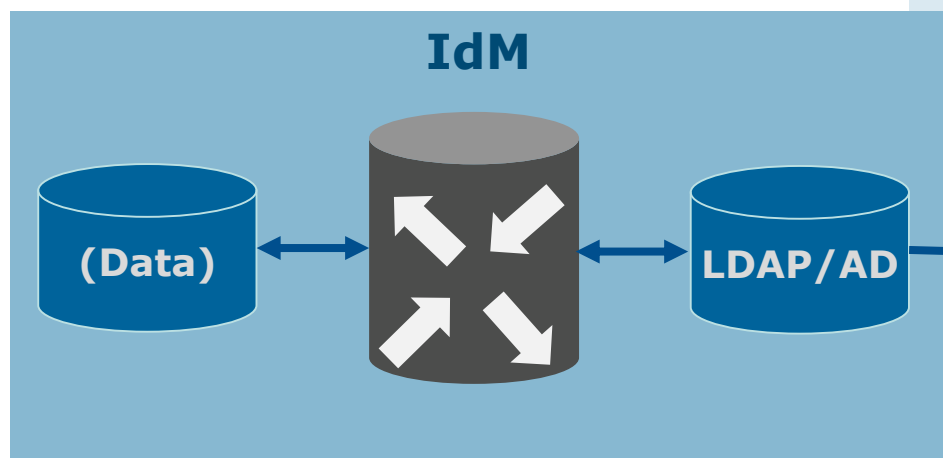
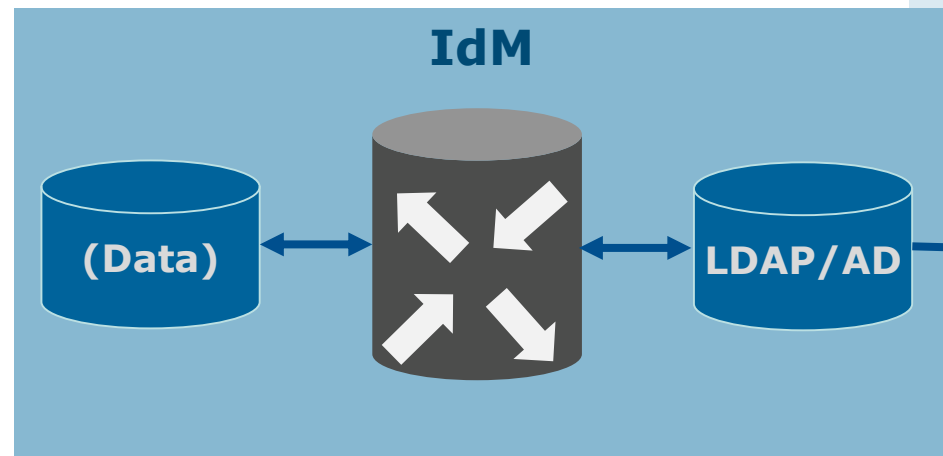
How does a federation work?



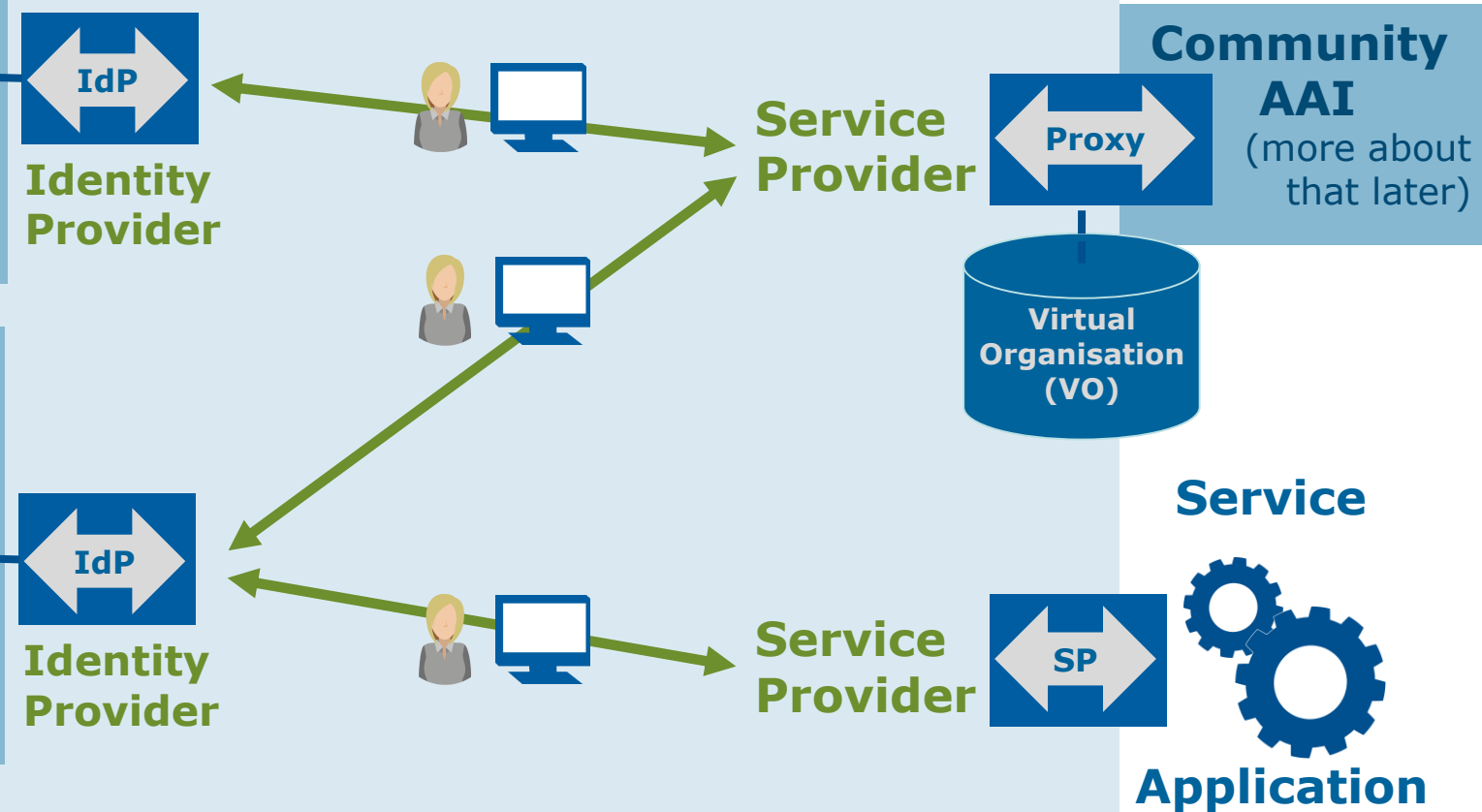
The Big Picture...

DFN

Home Organizations



Federated IdM



Example DFN-AAI

DFN

- **Federation Operator**

DFN-Verein

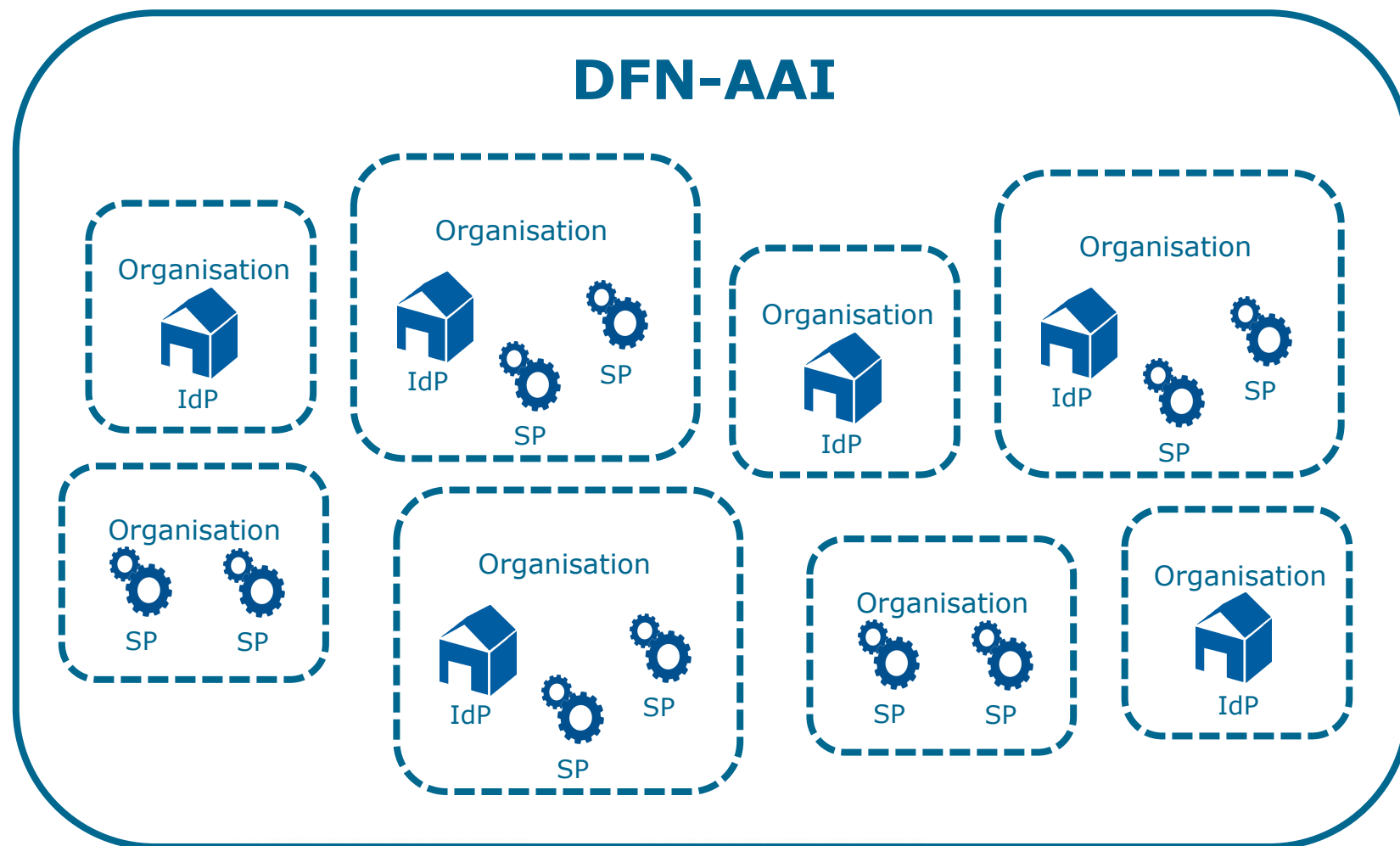
- **Trust**

Contracts with all
Participants, Policies,
Levels of Assurance

- **Technical**

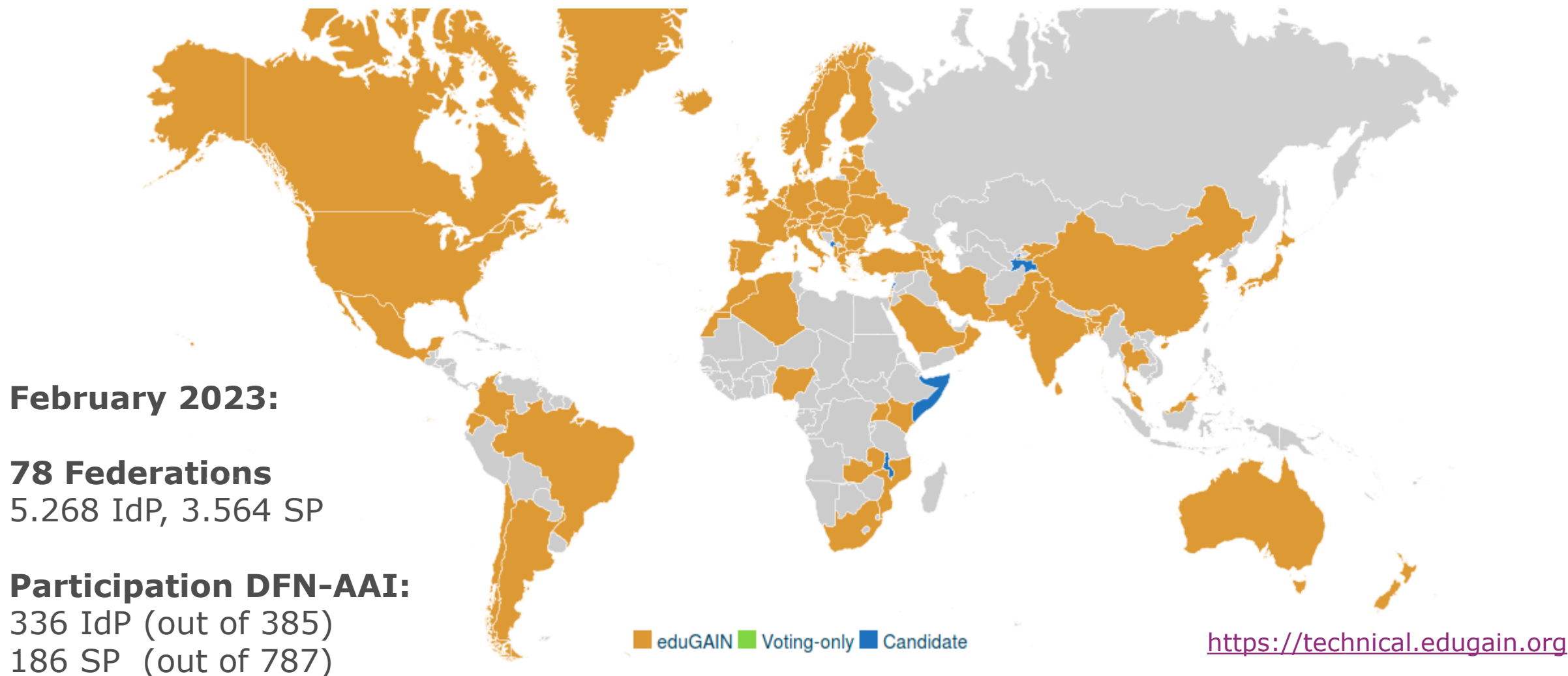
Metadata Management
and Distribution

Currently approx. 390 actively
participating Home Orgs and 790
Services (plus ~1420 local SPs)



- ▶ eduGAIN is a global Inter-Federation
 - ▶ Enables cross-federation AAI, i.e. collaboration between entities (IdP/SP) from other federations
- ▶ Operated by GÉANT, in production since end of 2011
 - ▶ DFN is one of the very first eduGAIN members
- ▶ Basically a metadata exchange service:
 - ▶ Aggregation of the metadata of the member federations
 - ▶ Member federations are responsible for distributing the metadata within their constituency
- ▶ No contracts between DFN and IdPs/SPs from other federations(!)
 - ▶ Establishing inter-federation trust is still an issue...

eduGAIN – Participating Federations



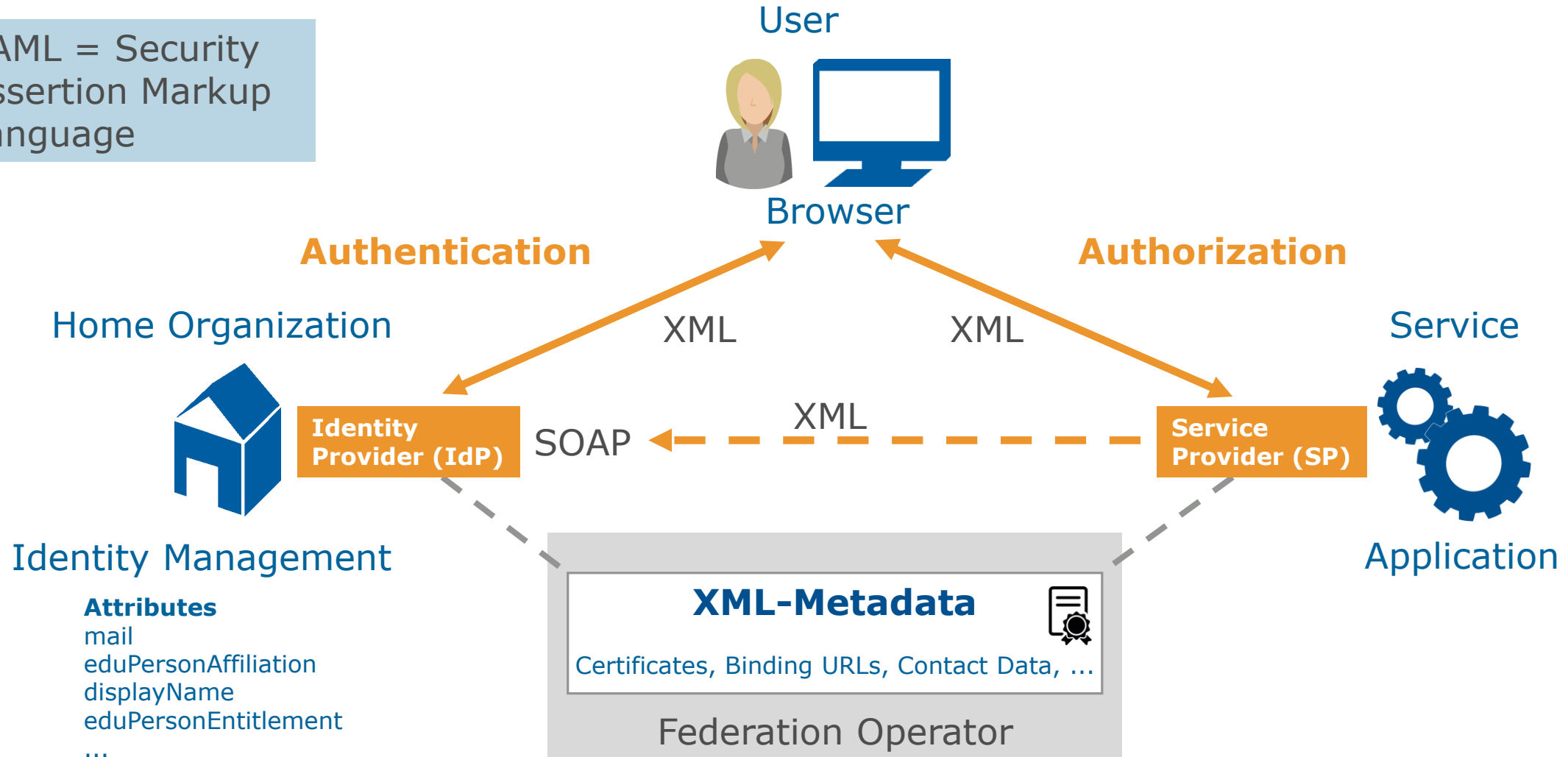
Participation in DFN-AAI (+ eduGAIN)

- ▶ Checklist: <https://doku.tid.dfn.de/en:join>
 - ▶ Requirements
 - ▶ Best Practices
 - ▶ etc.
- ▶ Documentation: <https://doku.tid.dfn.de/en:dfnaai:start>
- ▶ Contact: <https://doku.tid.dfn.de/en:aai:contact>
 - ▶ Support, Consulting, Incident Response etc.
- ▶ Mailing Lists: <https://doku.tid.dfn.de/en:aai:mailinglists>

Standards: SAML and OpenID Connect

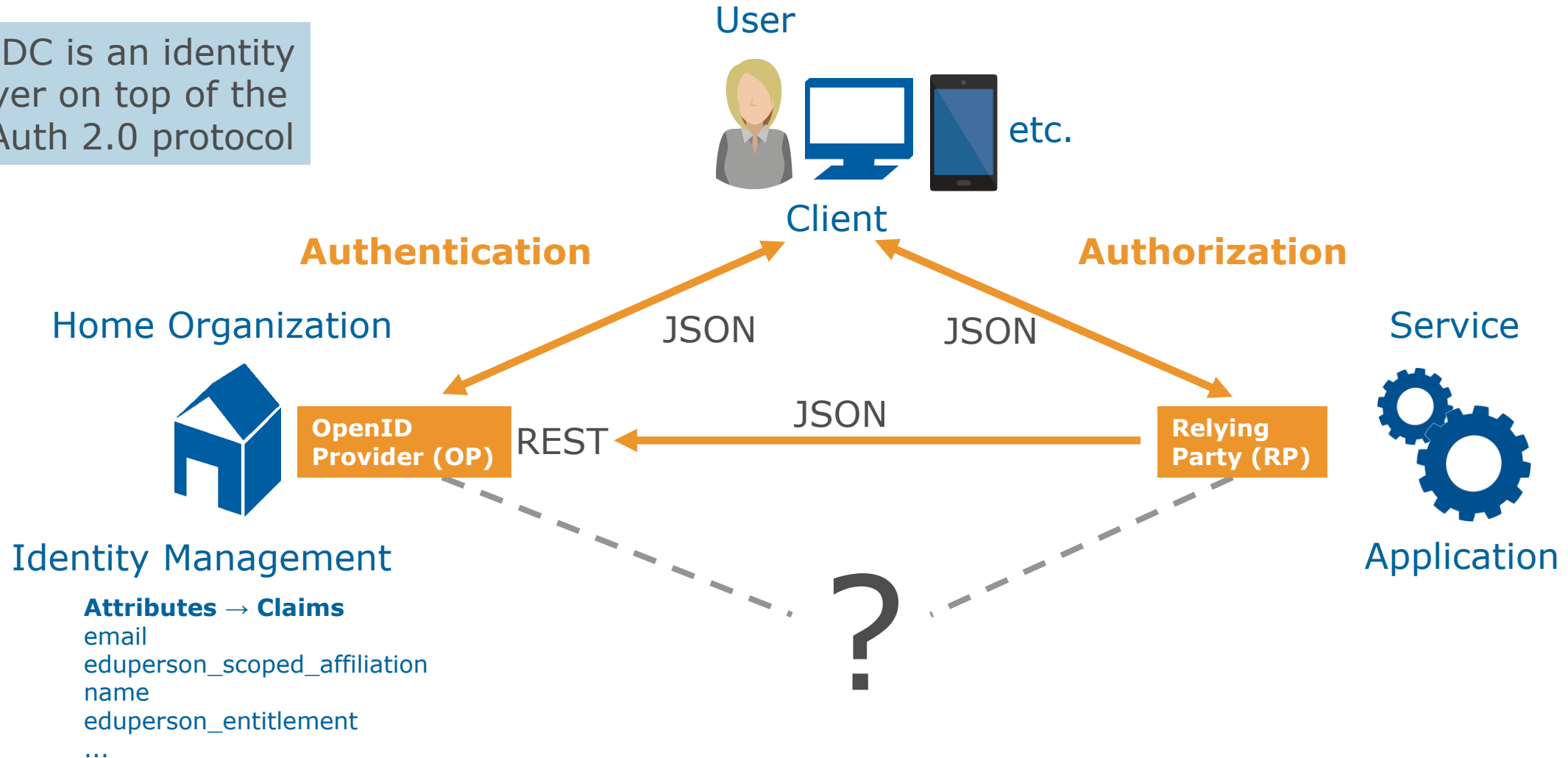
AAI based on SAML

SAML = Security
Assertion Markup
Language

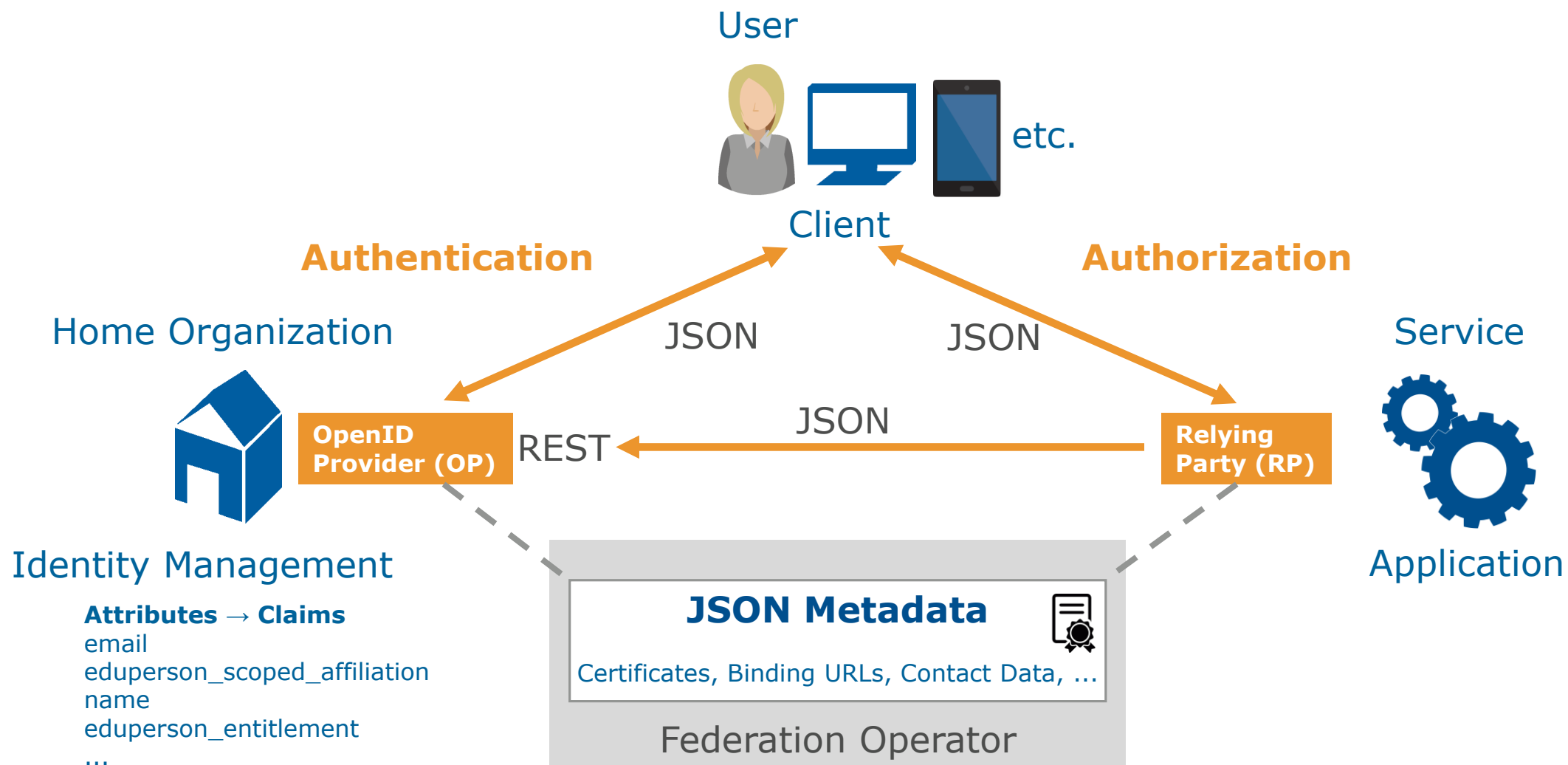


AAI based on OpenID Connect (OIDC)

OIDC is an identity layer on top of the OAuth 2.0 protocol



AAI based on OpenID Connect



OIDC: Current Status

- ▶ Specification OpenID Connect Federation still a draft #27(!)
- ▶ There is still a need for standardization in the Research & Education sector
 - ▶ Translation of SAML attributes e.g. from the eduPerson schema in corresponding OIDC claims and scopes and vice versa
- ▶ Best practice recommendations by the AARC Community are in progress
 - ▶ <https://aarc-community.org/guidelines/#upcoming> (AARC-G028)
 - ▶ [Research and Education Profile for OpenID Connect](#)
- ▶ Services (Relying Parties) are often operated behind proxies
- ▶ Heterogeneous picture, much is still in flux...

Trust and Levels of Assurance (LoA)



- ▶ Federation DFN-AAI
 - ▶ Contracts with all participating organizations
 - ▶ Obligation to comply with the federation policies and best practices
 - ▶ Implementation of and support for international standards
 - ▶ Identity Assurance: REFEDS Assurance Framework --> next slide
 - ▶ Incident Response: Sirtfi 1+2 (<https://refeds.org/sirtfi>)
 - ▶ Data Protection: CoCo 1+2 (<https://refeds.org/category/code-of-conduct>)
- ▶ Example Community AAI: Helmholtz AAI
 - ▶ <https://hifis.net/doc/helmholtz-aai/policies/>

- ▶ Different aspects of identity assurance are addressed independently of each other and can be expressed per identity (and not the whole IdM/IdP)
- ▶ Information is transmitted in the form of attribute/claim values (eduPersonAssurance / eduperson_assurance)
- ▶ Three categories (cf. <https://refeds.org/assurance>)
 - ▶ Assurance that an identifier represents a single natural person and the mapping of identifier to person remains the same over time (identifier uniqueness)
 - ▶ Identity proofing and credential issuance, renewal and replacement (identity assurance)
 - ▶ Quality and freshness of attributes (attribute assurance).

REFEDS Assurance Suite

DFN

REFEDS Assurance Framework (RAF)

Identifiers

ID is unique,
personal,
traceable,
never
re-assigned

ePPN
re-assigned?

ID proofing

low

medium

high

local-
enterprise

Attributes

affiliation
freshness
1 month

affiliation
freshness
1 day

AuthN Profiles

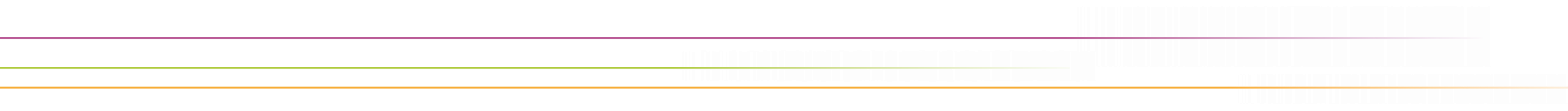
Authentication

single-factor
(SFA)

multi-factor
(MFA)

DFN

Break



RDMO Use Case

→ David Wallace, TUDa

AARC Blueprint Architecture (BPA) and Community AAIIs

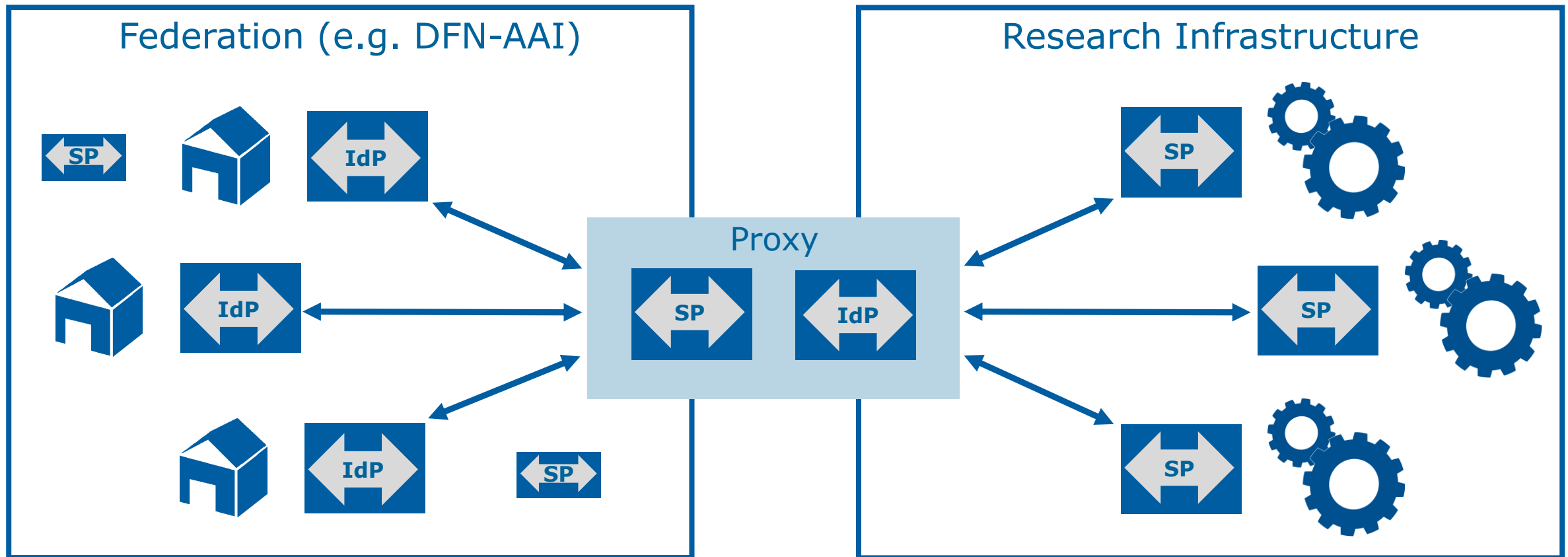


The Power of Proxies

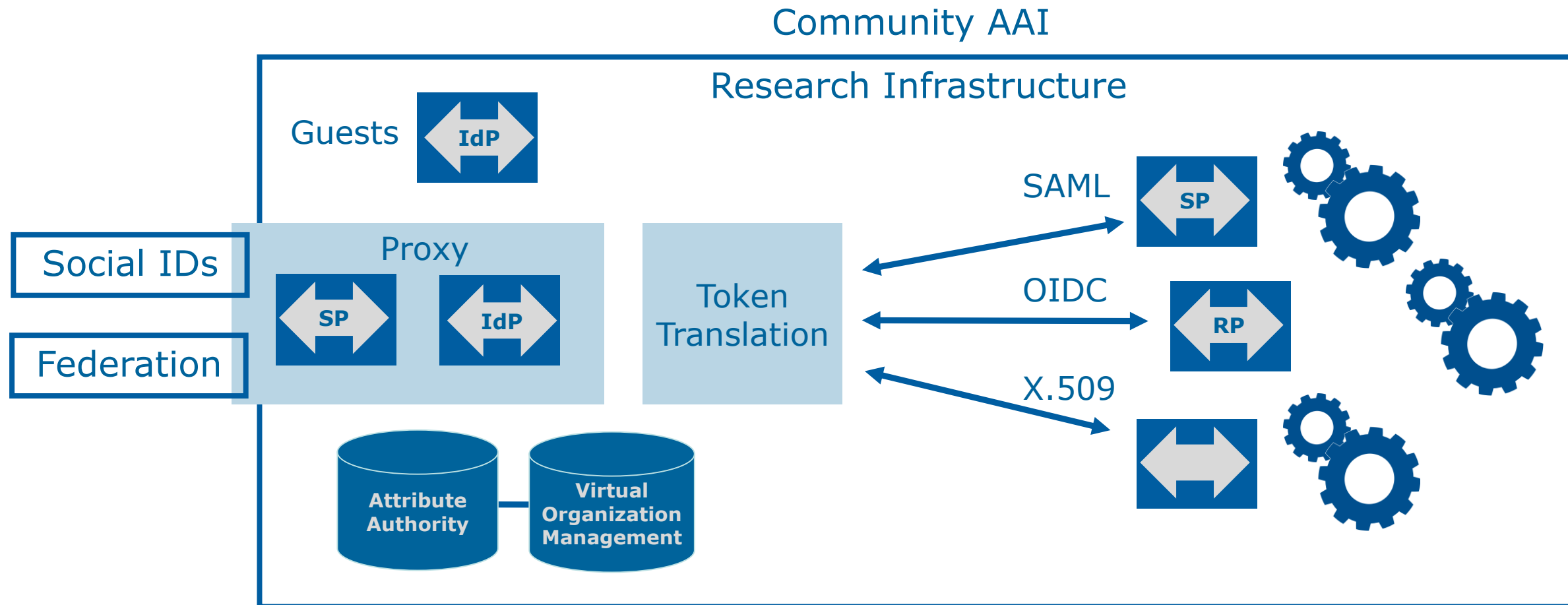
- ▶ Wikipedia (https://en.wikipedia.org/wiki/Proxy_server):
„[...] as a way to simplify and control [...] complexity. Proxies were invented to add structure and encapsulation to distributed systems.”
- ▶ Federated Identity Management
 - ▶ One well-defined interface of a Community AAI to an Identity Federation
--> services behind the proxy
 - ▶ Support for several protocols and standards
 - ▶ Community VO Management
 - ▶ Integration of further technical components

Proxy – a simple Model

The simplest variant consists only of an IdP and an SP component

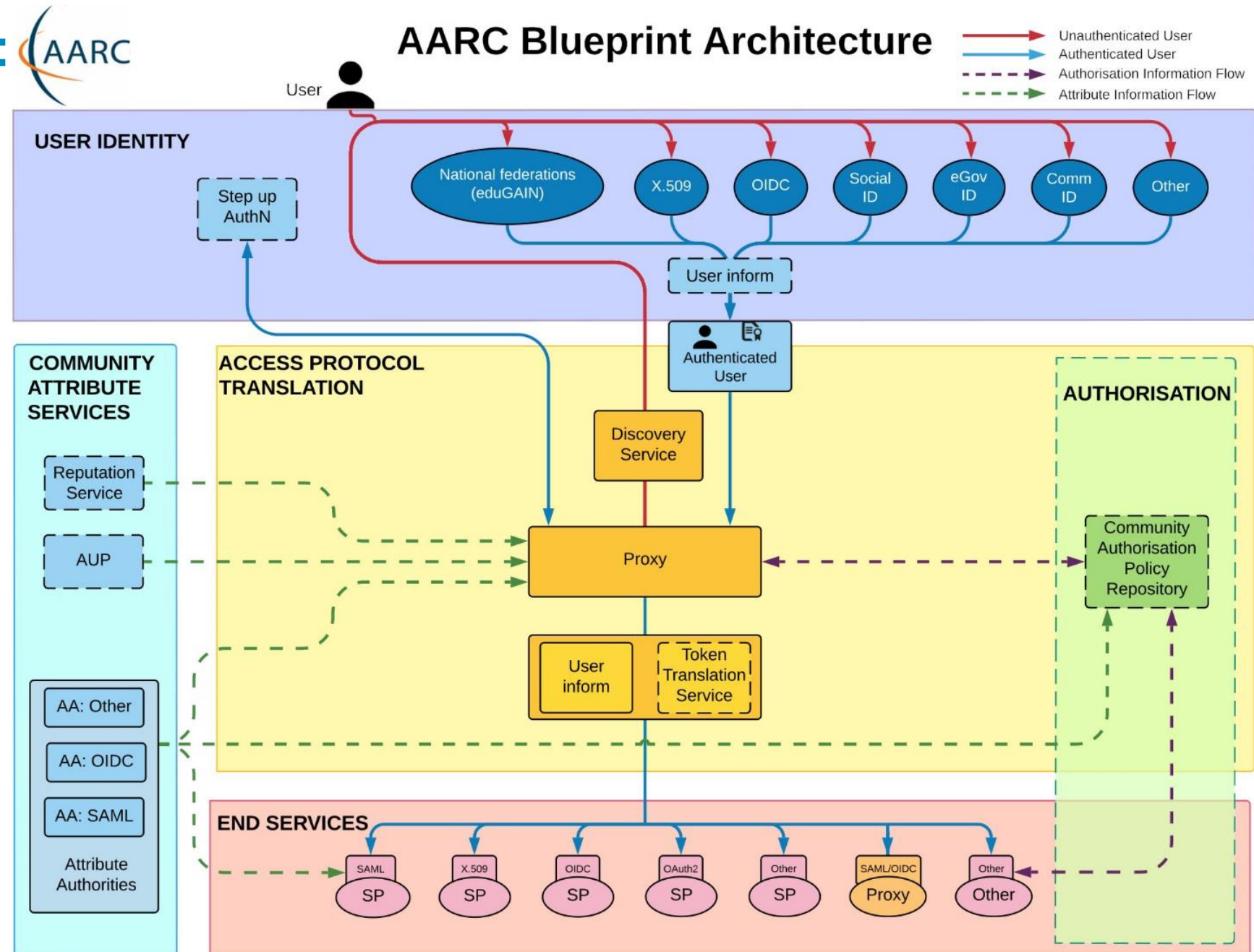


... that can be easily extended



And here we are: 

AARC = Authentication and Authorization for Research and Collaboration
<https://aarc-community.org/>

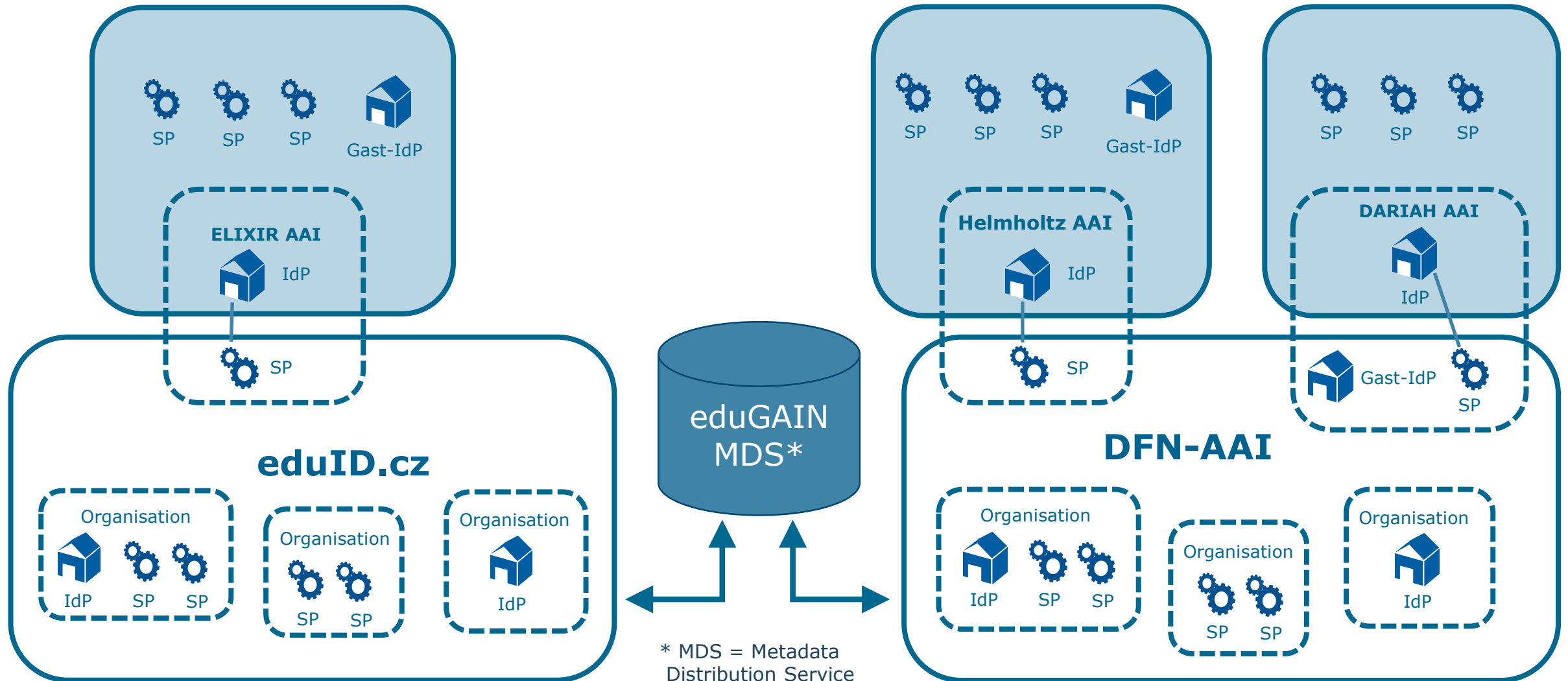


AARC Blueprint Architecture

- ▶ Five components that can be combined to implement federated IAM solutions for (international) research collaborations:
 - ▶ **User Identity:** Authentication via AAI, Social Media IDs, ORCID, etc.
 - ▶ **Community Attribute Services:** Rights, Roles, VO Management
 - ▶ **Access Protocol Translation:** IdP-/SP-Proxy, Token Translation, ...
 - ▶ **Authorisation:** Authorization, management of access to services/resources
 - ▶ **End-services:** the actual services and resources
- ▶ <https://aarc-community.org/architecture/>

Interoperability: Federations and Community AAIs

DFN



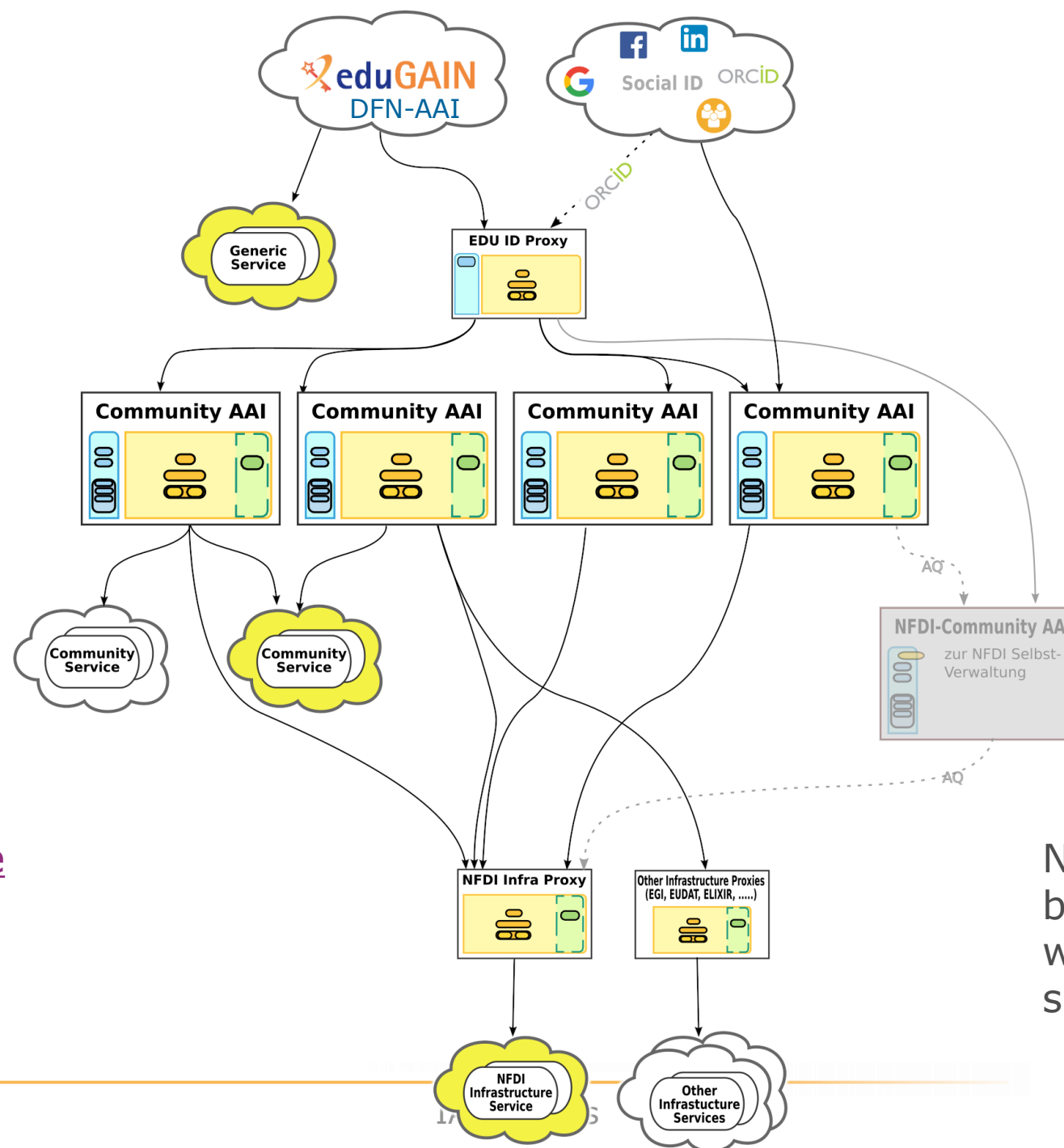
NFDI Basic Service IAM and NFDI AAI



- ▶ NFDI Consortia supposed to operate (or have operated) Community AAI
- ▶ NFDI AAI Architecture as connecting element --> interoperability
- ▶ Three-layered Service Model
 - ▶ Generic services --> Federation (DFN-AAI)
 - ▶ Community services --> Community AAI
 - ▶ Infrastructure services --> Infrastructure Proxy
- ▶ Additional components
 - ▶ NFDI Infrastructure Proxy (simplify connection to services, AuthZ, ID linking)
 - ▶ NFDI Attribute Authority (NFDI-internal rights management)
 - ▶ edu-ID Proxy – optional (lifelong self-managed ID, Guest IdP, Account Linking)

Architecture

DFN



<https://doc.nfdi-aai.de>

NFDI Architecture will be topic of a separate workshop in early summer 2023

Community AAI Implementations

- ▶ NFDI Basic Service IAM will provide support for 4 Community AAI implementations (<https://doc.nfdi-aai.de/community-aai-software/>)
 - ▶ AcademicID (GWDG)
 - ▶ didmos (DAASI)
 - ▶ RegApp (KIT)
 - ▶ Unity (FZ Jülich)
- ▶ Community-AAI-as-a-Service as part of the Service Portfolio (i.e. Hosting)
- ▶ Further information in the IAM Basic Service proposal:
https://doc.nfdi-aai.de/documents/iam4nfdi_initialization.pdf

Interoperability

- ▶ The most important goal of the NFDI AAI Architecture is to enable interoperability
 - ▶ Community AAI <--> Community AAI
 - ▶ Community AAI <--> NFDI AAI
 - ▶ Community AAI <--> EOSC AAI
 - ▶ NFDI AAI <--> EOSC AAI <--> EGI etc.
- ▶ Based on AARC Guidelines (BPA etc.) and the EOSC AAI Architecture
 - ▶ Mandatory attribute/claim profiles for NFDI AAI
 - ▶ Policy Framework
 - ▶ ...

Basic Service IAM: Work Packages

- ▶ WP1: Policy, Governance, and Legal Aspects
- ▶ WP2: AAI Architecture and Implementation
- ▶ WP3: Incubator
- ▶ WP4: Operations
- ▶ WP5: Dissemination, Training, and Community Engagement

Federating Services Introduction



Service Provider | Relying Party

- ▶ Protects resources --> authorization
- ▶ ‚lives‘ somewhere in between web server and resource
- ▶ Discovery: Enables users to select their Home Organizations and thus the relevant IdP/OP (only in federation scenarios)
- ▶ Sends an Authentication Request to the Home IdP/OP of the user
- ▶ Processes the response(s) of the IdP/OP
 - ▶ Authorization of user
 - ▶ passes on certain data (mostly attributes/claims) to the application behind it
- ▶ Logout: Logout Request to IdP/OP and termination of application session

Federating Services: Things to consider

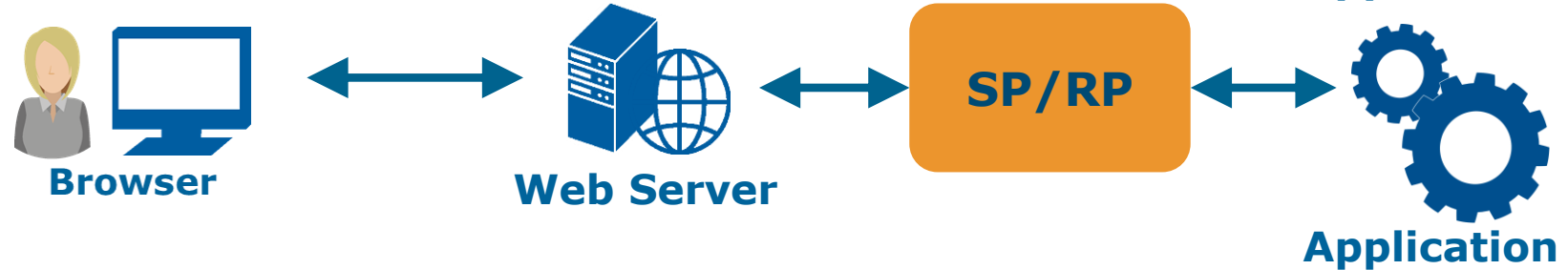
- ▶ Information needed to authorize a user
- ▶ If the protected resource is an application
 - ▶ Any plugins/extensions available that support SAML and/or OIDC?
 - ▶ Existing interfaces? Basic Auth?
 - ▶ How to pass user data to the application?
 - ▶ Mapping of attributes/claims to server variables
 - ▶ How to terminate the application session (if any) at logout?
- ▶ Otherwise you only have to protect the URL of the resource
 - ▶ Only the web server part of configuration relevant
 - ▶ No need to pass any information

Implementation: Different Approaches

1. Library



2. Standalone



3. Integration in Web Server



4. „Platform“



Examples – Open Source Implementations

- ▶ Library
 - ▶ [OpenSAML](#)
- ▶ Standalone
 - ▶ [SimpleSAMLphp](#)
- ▶ Integration Web Server
 - ▶ [mod_auth_openidc](#)
 - ▶ [PySAML2](#) (+ mod_wsgi)
 - ▶ [Shibboleth Service Provider](#)
- ▶ Platform
 - ▶ [Keycloak](#)

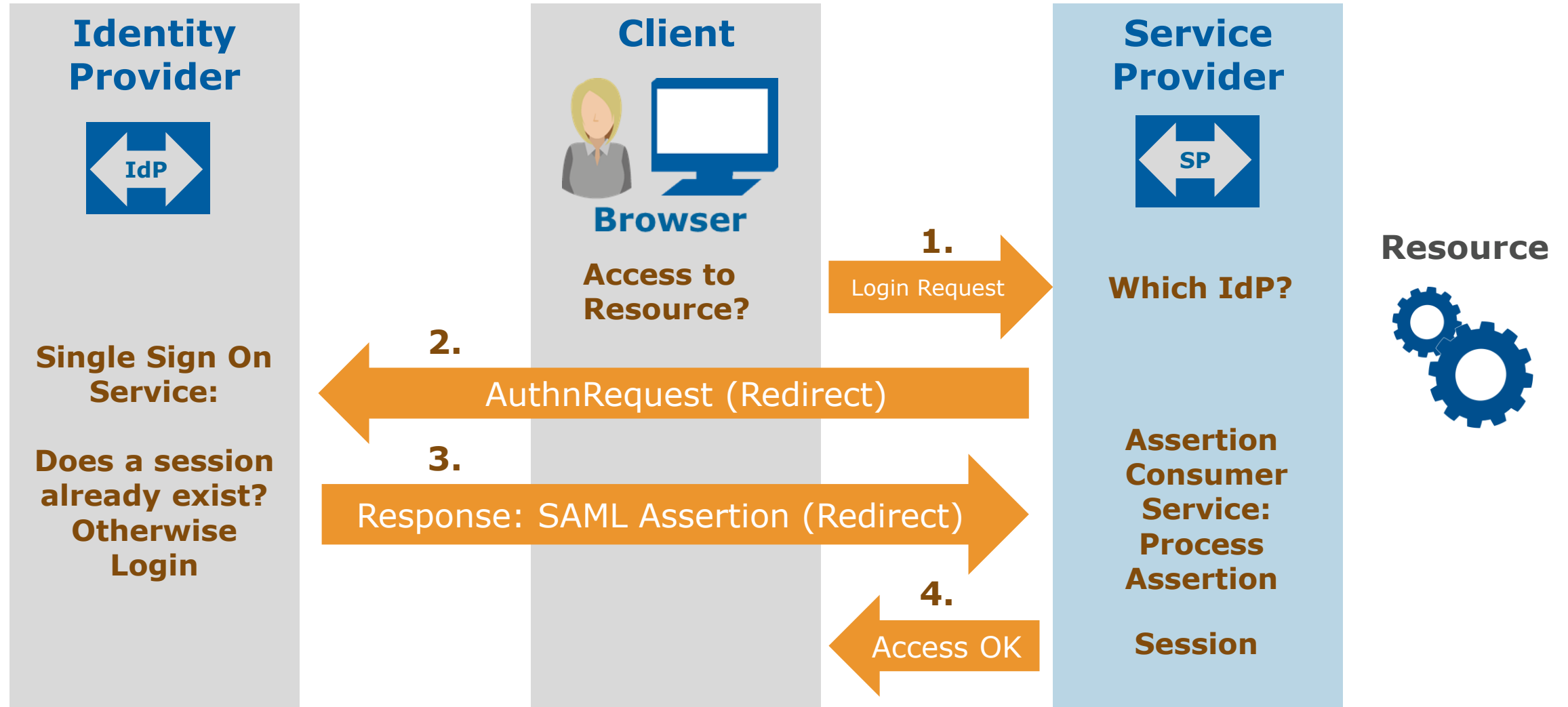
Federation: Technical Requirements

- ▶ Technical Implementation must be able to consume and process federation metadata → Key Rollover at IdPs
- ▶ Seamless Key Rollover:
Simultaneous support of two private key - certificate pairs
- ▶ Implementation must be able to handle encrypted assertions
- ▶ Support for current security standards!
- ▶ Security updates must be made available as soon as possible

Federating Services

Example Shibboleth Service Provider

Web Browser SSO with SAML



SP → IdP: AuthnRequest

- ▶ Service provider finds out the Entity ID of the relevant IdP
- ▶ The Entity ID is used to search the (federation) metadata for a `<SingleSignOnService>` URL to which the AuthnRequest is sent, usually via HTTP-Redirect

`Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"`

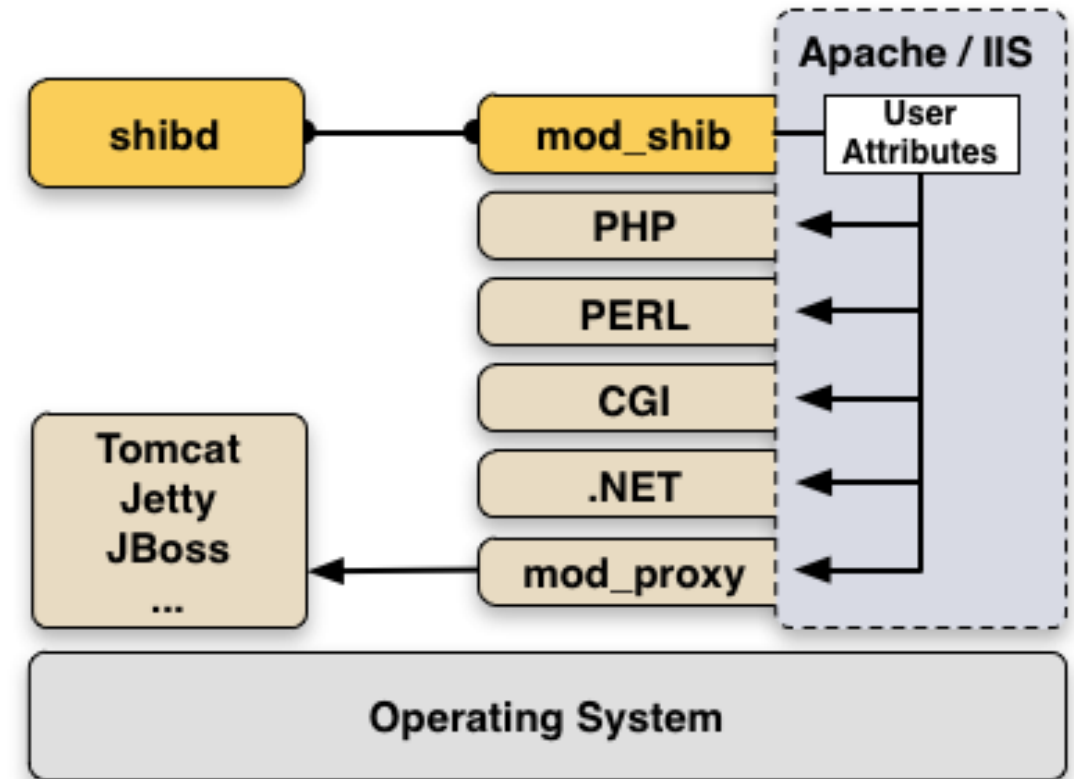
- ▶ AuthnRequest is not encrypted and usually not signed

IdP → SP: SAML Assertion

- ▶ Assertion Consumer Service
- ▶ Processes assertions (encrypted+signed), especially
 - ▶ Name IDs
 - ▶ Authentication Context
 - ▶ Attributes
- ▶ Based on this information,
 - ▶ the service provider makes an authorisation decision
 - ▶ if necessary, it consults further attribute sources, e.g. Attribute Query against the group/VO management of a Research Infrastructure
 - ▶ passes information to the protected application

Overview Shibboleth SP

- ▶ Two Components:
 - ▶ Web Server-Modul for Apache (mod_shib) and IIS Web Server (iis7_shib.dll): Protects files, directories, locations and enforces AAI-based Authorization
 - ▶ shibd Daemon: State management, XML processing, security, „logic“
- ▶ Communication with Application:
 - ▶ Attributes are stored on environment variables that can be accessed by all applications running in the web server, z.B. PHP: \$_SERVER['mail']
 - ▶ Handler (see following slides)



Quelle: <https://www.switch.ch/aai/guides/sp/>

Directories under Debian (Selection)

- ▶ `/etc/shibboleth/`
 - ▶ Central configuration in `shibboleth2.xml`
 - ▶ Attributes: `attribute-map.xml`, `attribute-policy.xml`
 - ▶ Logging: `native.logger (mod_shib)`, `shibd.logger (shibd)`
 - ▶ HTML Templates (`*.html`)
 - ▶ Locally generated certificates + keys
- ▶ `/var/cache/shibboleth/`
 - ▶ Backup Remote Metadata
- ▶ `/var/log/shibboleth/`
 - ▶ Among others: `shibd.log` **and** `transaction.log` (`native.logger` → **syslog**)

Editing the Configuration (1)

Usually, only a few adjustments in `shibboleth2.xml` are required:

- ▶ Entity ID of the SP and (if applicable) the `REMOTE_USER` variable

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"  
REMOTE_USER="pairwise-id persistent-id subject-id">
```

- ▶ Security Settings for SP-Sessions (Cookies, https, Timeout, etc.)

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"  
    checkAddress="false" consistentAddress="true"  
    handlerSSL="true" cookieProps="https"  
    redirectLimit="host">
```

Editing the Configuration (2)

- ▶ Session Initiator: defines, among other things, how users are forwarded to the IdP (hard-wired or Discovery Service)

```
<SSO discoveryProtocol="SAMLDS"  
  discoveryURL="https://wayf.aai.dfn.de/DFN-AAI/wayf">  
  SAML2
```

`</SSO>` (element `<SSO>` is simplified version of `<SessionInitiator>`)

- ▶ Contact information to be displayed on error pages

```
<Errors supportContact="helpdesk@example.org"  
  helpLocation="/about.html"  
  styleSheet="/shibboleth-sp/main.css"/>
```

Editing the Configuration (3)

► (Federation) Metadata

```
<MetadataProvider type="XML"
  url="http://www.aai.dfn.de/metadata/dfn-aai-idp-metadata.xml"
  validate="true" backingFilePath="dfn-aai-idp-metadata.xml" reloadInterval="3600">
  <MetadataFilter type="Signature" certificate="/etc/ssl/aai/dfn-aai.pem"/>
</MetadataProvider>
```

► Certificate(s) and Private Key(s) for Signing and en/decryption of the SAML-based communication (Shib SP is able to handle two cert/key pairs)

```
<CredentialResolver type="File"
  key="/etc/ssl/private/myvhost.mydomain.de.key.pem"
  certificate="/etc/ssl/localcerts/myvhost.mydomain.de.crt.pem"/>
```

- ▶ Kind of an API that provides several functions via URLs:

`https://sp.uni-musterstadt.de/Shibboleth.sso/...`

- ▶ Discovery Feed – generated in JSON format from the consumed (and filtered) metadata, used as input for an Embedded Discovery Service (EDS):

`.../Shibboleth.sso/DiscoFeed`

- ▶ Login/Session Initiator, e.g. to initiate a Shib Session by the application:

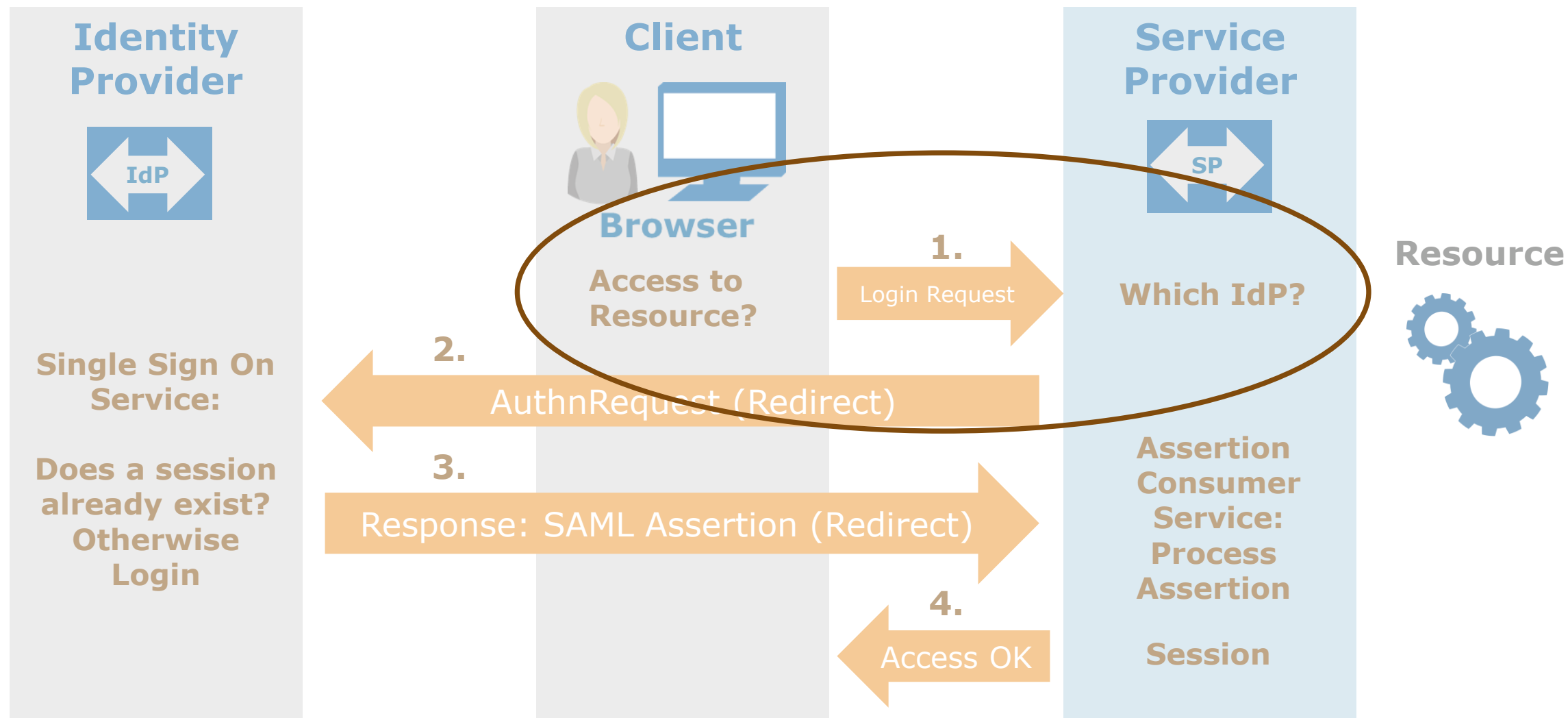
`.../Shibboleth.sso/Login`

- ▶ Logout Initiator, e.g. to terminate a Shib Session by the application:

`.../Shibboleth.sso/Logout`

Web Browser SSO Process

DFN



Protecting Applications

- ▶ Rules for Access Control can be implemented in different ways:
 - ▶ Web Server / Apache Configuration: Apache Access Rules
 - ▶ SP Configuration: XML Access Control
 - ▶ SP Handler: Attribute Checker (later in the flow, after attribute processing)
- ▶ Apache Access Rules allow for simple AND/OR connectives of conditions
- ▶ XML Access Control allows for more complex conditions

Apache Access Rules

Protect Files, Directories, Locations and (if applicable) trigger Session Initiator

```
<Location /protected>  
    AuthType shibboleth  
    ShibRequestSetting requireSession true  
    <RequireAll>  
        Require shib-attr affiliation staff@uni-xyz.de  
        Require shib-attr mail .*  
    </RequireAll>  
</Location>
```

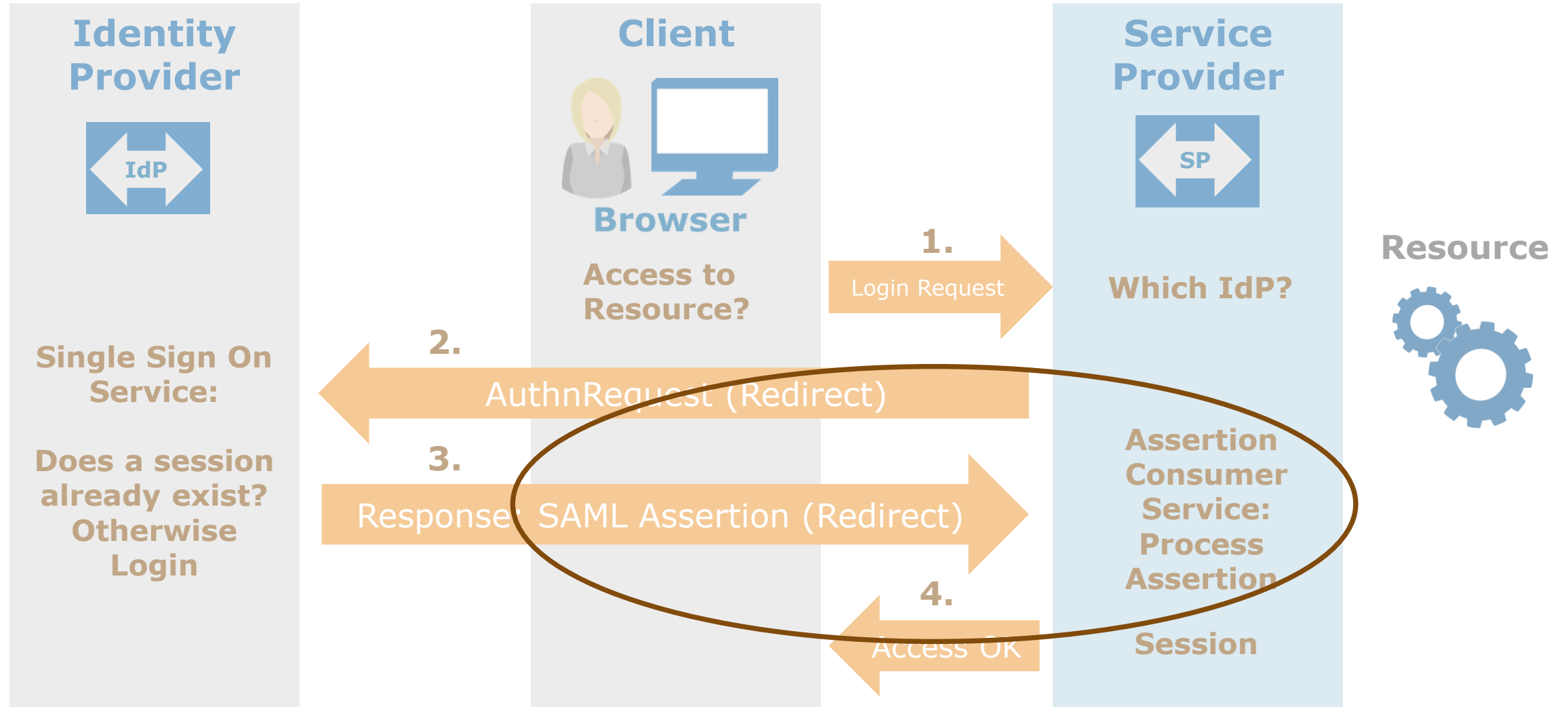
The names of attributes resp. variables are defined in
/etc/shibboleth/attribute-map.xml (see following slides)

Access rules in XML-Syntax outside the Apache configuration (important: in Apache UseCanonicalName On must be set!). Usually in etc/shibboleth/shibboleth2.xml:

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="sp.uni-musterstadt.de">
      <Path name="protected" authType="shibboleth" requireSession="true">
        <AccessControl>
          <AND>
            <Rule require="unscoped-affiliation">staff</Rule>
            <RuleRegex require="mail">.*</RuleRegex>
          </AND>
        </AccessControl>
      </Path>
    </Host>
  </RequestMap>
</RequestMapper>
```

Web Browser SSO Process

DFN



Processing of Attributes (1)

- ▶ Per default the Shib SP extracts attributes from SAML Assertions, i.e. from `<saml2:AttributeStatement>` and `<saml2:Subject>` (transient-id, persistent-id)

```
<AttributeExtractor type="XML" validate="true" reloadChanges="false"
path="attribute-map.xml"/>
```

- ▶ Further possibilities (see [Shib Wiki](#)):

```
<AttributeExtractor type="Metadata"> (e.g. contact data)
```

```
<AttributeExtractor type="Assertion"> (other elements)
```

... and/or via Attribute Query from an Attribute Authority (→ separate slide)

Processing of Attributes (2)

In `/etc/shibboleth/attribute-map.xml` attributes from assertions are mapped to web server variables (other Attribute Extractors do this directly), the name of the variable is defined via „id“, for instance:

```
<!-- Input: eduPersonScopedAffiliation -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" id="affiliation">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>
<!-- Input: eduPersonAffiliation -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" id="unscoped-affiliation">
  <AttributeDecoder xsi:type="StringAttributeDecoder" caseSensitive="false"/>
</Attribute>
<!-- Input: samlSubjectID -->
<Attribute name="urn:oasis:names:tc:SAML:attribute:subject-id" id="subject-id">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder" />
</Attribute>
```

Processing of Attributes (3)

In an additional step, further attributes can be aggregated from additional attribute sources, so-called Attribute Authorities

cf. https://doku.tid.dfn.de/de:aai:attribute_authority

shibboleth2.xml:

```
<AttributeResolver type="SimpleAggregation" attributeId="subject-id"
format="urn:oasis:names:tc:SAML:attribute:subject-id">

  <Entity>https://trusted-attribute-authority.example.org/idp/shibboleth</Entity>

  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="eduPersonEntitlement" />

</AttributeResolver>
```

Processing of Attributes (4)

- ▶ Next Step: Which attributes/variables and values are processed further and passed to the application?
- ▶ Filtering options via `/etc/shibboleth/attribute-policy.xml`, usually the defaults are sufficient
- ▶ Examples
 - ▶ Syntax check: do scoped attributes actually contain a scope? (`@uni-xyz.de`)
 - ▶ Controlled vocabulary: permissible values for (unscoped-)affiliation
 - ▶ Accept specific attributes, e.g. entitlements only from selected IdPs or Attribute Authorities

Attribute Checker Handler

- ▶ This handler becomes active before a forwarding to the protected resource takes place, Session Hook mechanism:

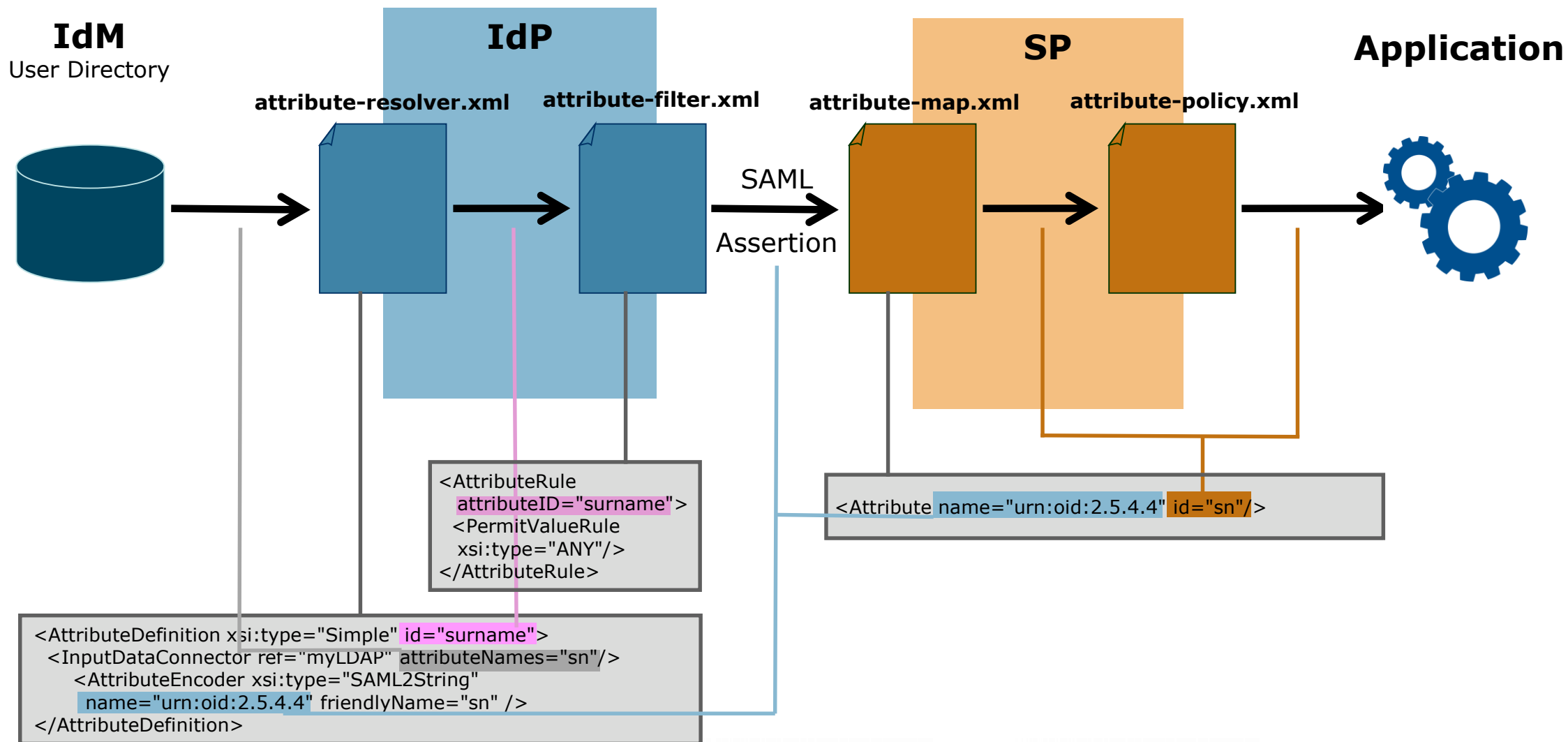
```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"  
... sessionHook="/Shibboleth.sso/AttrChecker">
```

and

```
<Handler type="AttributeChecker" Location="/AttrChecker"  
template="attrChecker.html" attributes="mail displayName"  
flushSession="true"/>
```

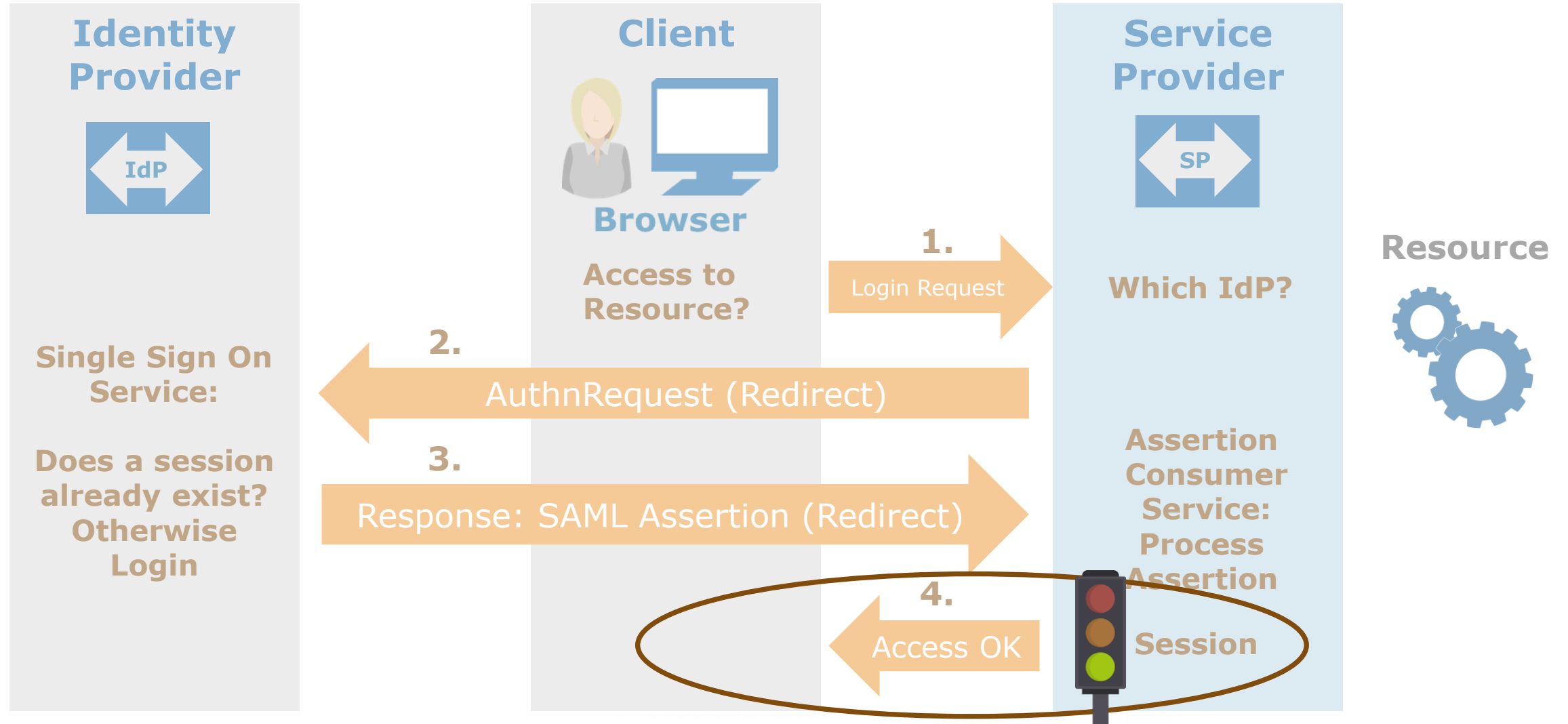
- ▶ Comprehensive example in GÉANT wiki:
<https://wiki.geant.org/display/eduGAIN/How+to+configure+Shibboleth+SP+attribute+checker>

The Way of the Attributes



Web Browser SSO Process

DFN



Thanks! Questions? Comments?

DFN

- ▶ Contact

- ▶ Wolfgang Pempe

- Team Leader DFN-AAI

- E-Mail: pempe@dfn.de

- Tel.: +49-30-884299-308

- Fax: +49-30-884299-370



References

- ▶ Shibboleth Wiki:
<https://wiki.shibboleth.net/confluence/display/SP3/Home>
- ▶ Comprehensive documentation on installation and configuration provided by SWITCH: <https://www.switch.ch/aai/guides/sp/>
- ▶ DFN-AAI Wiki: Basic configuration and Embedded Discovery Service:
<https://doku.tid.dfn.de/de:shibsp>
- ▶ Training material: <https://doku.tid.dfn.de/de:aai:training:shibsp>