# cessda saw

Research and Innovation Action

# CESSDA Strengthening and Widening

Project Number: 674939          Start Date of Project: 01/08/2015          Duration: 27 months

# Deliverable 4.2

# Stakeholder Workshop Report – AAI workshop

| Dissemination Level | PU |
|---|---|
| Due Date of Deliverable | 30/04/17 |
| Actual Submission Date | 16/06/17 |
| Work Package | WP4 |
| Task | 4.1 |
| Type | Report |
| EC Approval Status | 16 November 2017 |
| Version | V1.6 |
| Number of Pages | p.1 – p.14 (+ Annex) |

**Abstract:** Report on the "Integration Workshop on Strategies for Authentication and Authorization Infrastructures (AAI)" held in Zagreb, Croatia on March 1st and 2nd, 2017. This workshop was part of the "Second Training workshop on Trust and Technical Aspects within the CESSDA infrastructure" that was originally scheduled in October 2016. This report contains the preparations and setup of the AAI workshop as well as the outcomes of the sessions.

## History

| Version | Date | Reason | Revised by |
|---------|------|--------|------------|
| 1.0 | 20/03/2017 | 1st draft | Anna K. Schwickerath (GESIS), Sebastian Netscher (GESIS), Ellen Leenarts (DANS) |
| 1.1 | 21/04/2017 | Contributions received from Peter Gietz (DAASI GmbH) & Hossein Abroshan (CESSDA - MO) | Anna K. Schwickerath (GESIS) |
| 1.2 | 24/04/2017 | Review of version 1.1 | Sebastian Netscher (GESIS), task-leader |
| 1.2 | 26/04/2017 | Review of version 1.1 | WP Leader, Marion Wittenberg (DANS) - WP4 |
| 1.3 | 27/04/2017 | 2nd draft | Anna K. Schwickerath (GESIS) |
| 1.4 | 22/05/2017 | Review of version 1.3 | Ivana Versic (CESSDA AS) |
| 1.5 | 29/05/2017 | Request for changes by Ivana Versic | Ellen Leenarts (DANS) |
| 1.6 | | Final draft version | Anna K. Schwickerath (GESIS) |

## Author List

| Organisation | Name | Contact Information |
|--------------|------|---------------------|
| GESIS | Sebastian Netscher | sebastian.netscher@gesis.org |
| GESIS | Anna K. Schwickerath | anna.schwickerath@gesis.org |
| DANS | Ellen Leenarts | ellen.leenarts@dans.knaw.nl |
| DAASI International | Peter Gietz | peter.gietz@daasi.de |
| CESSDA Main Office | Hossein Abroshan | hossein.abroshan@cessda.net |

## Time Schedule before Delivery

| Next Action | Deadline | Care of |
|---|---|---|
| 1st draft | 20/03/2017 | GESIS, DANS |
| Review by Task leader | 22/04/2017 | GESIS |
| Review by WP leader | 26/04/2017 | DANS |
| Final draft | 30/05/2017 | GESIS |
| Review by the Delivery Committee Chair | 15/06/2017 | CSDA |
| Review by Project Coordinator | 12/06/2017 | CESSDA AS |
| Submission of final version | 16/06/2017 | CESSDA AS |

## Abbreviations and Acronyms

| | |
|---|---|
| **AAI** | Authentication and Authorization Infrastructures |
| **AARC** | Authentication and Authorisation for Research and Collaboration |
| **CESSDA** | Consortium of European Social Science Data Archives |
| **CESSDA SaW** | CESSDA Strengthening and Widening |
| **FIM4D** | Federated Identity Management for DARIAH (working group) |
| **CC-BY** | Creative Commons By Attribution license |
| **IdP** | Identity Provider (AAI) |
| **SP** | Service Provider (AAI) |
| **SRCE** | University of Zagreb, Computing Centre |
| **VRE** | Virtual Research Environment |

## Executive Summary

The CESSDA-SaW H2020 project aims at achieving full European coverage. Global best practice is to be built into the infrastructure of European social science and research. Therefore, a series of workshops and a final dissemination event are being organised throughout the two-year project.

This report is on the "Integration Workshop on Strategies for Authentication and Authorization Infrastructures (AAI)" that took place in Zagreb on March 1st and 2nd 2017 as part of the "Second Training workshop on Trust and Technical Aspects within the CESSDA infrastructure". The integration workshop aimed mainly as a kick-off meeting for the discussion on implementation strategies for Authentication and Authorization Infrastructures (AAI) for technical and non-technical staff of Service Providers (SP). The deliverable includes a description of the preparation, the content and the results of the workshop.

## Inhalt

# 1   INTRODUCTION

## 1.1   GOAL OF TASK 4.1 & DELIVERABLE 4.2

Promoting knowledge exchange between current and future members with the aim of strengthening CESSDA is one central component of Work Package 4. A bottom-up approach is central to this WP. The establishment of new data archives and strengthening of existing ones is promoted by WP4 through the necessary administrative, technical, and methodological support from countries with a more developed data archiving infrastructure. The key objective of WP4 consists of five development support tasks, each focusing on an aspect of the required knowledge exchange. Task 4.1 focuses in particular on the development of a rolling programme of hands-on training for data archive practitioners on ingest and dissemination practices.

Part of the task 4.1 programme was the workshop on "Strategies for Authentication and Authorization Infrastructures (AAI)". This workshop served as a kick-off meeting for the introduction as well as the starting point of discussion on implementation strategies for AAI. Deliverable 4.2 (Workshop 2 report) aimed at the documentation of its development, organisational structure, and the topics discussed during the event. The Annex therefore includes a list of institutions who participated in the event as well as the presentations held during the workshop, enabling CESSDA (aspiring) members to recapitulate the event and to discuss its results internally and between organisations.

## 1.2   PREPARATION OF THE WORKSHOP

The Integration Workshop on Strategies for AAI was organised by GESIS and DANS, in collaboration with CESSDA Main Office. The idea behind this collaboration was to bring together people with a technical background as well as those experienced in developing trainings in order to achieve the best possible outcome.

In preparation of the workshop, Hossein Abroshan, CESSDA Chief Technical Officer, compiled information on the topic. His report „CESSDA AAI - Challenges, Best Practices, Solutions (v1)" was used as guidance to develop a preliminary workshop program, consisting of four sessions, as described in greater detail in chapter 2 of this report. Additionally, it was decided to engage the participants in group work with the aim of encouraging knowledge exchange. Regarding the participants' background knowledge on AAI, the organisers assumed their level of expertise to vary greatly. As the workshop was considered to serve as a kick-off meeting for the discussion on implementing AAI strategies between (aspiring) CESSDA members, the organisers put emphasise on enabling the participants to outline the approaches and positions of their home organisations. Therefore, all participants were contacted two weeks before the event. As preparation for the workshop, they were asked to bring their questions and related issues on AAI to the workshop, and to discuss the following questions with colleagues in their institutions:

1. *Which Authentication and Authorisation techniques and systems is your institution currently using?*

2. *Who are your AAI users (e.g. employees, researchers, etc.)?*

3. *Are there any resources in your organisation that are only available for authenticated users? If yes, which ones? And how are these protected?*

4. *How can a federated AAI help CESSDA Service Providers and their users? What features and/or functionalities are needed for that?*

5. *Do you have any AAI or IT Security expert in your organisation?*

Many participants elaborated these questions with colleagues in their organisations and were aware of the AAI approach at their institute, which proved to be helpful for discussions during the workshop.

Furthermore, it was decided to engage an external trainer experienced in AAI solutions. Therefore, the partners gathered information on qualified trainers among CESSDA SaW colleagues. The decision was made to engage Peter Gietz, who was highly recommended by a number of CESSDA members. Peter Gietz is partner and executive director at DAASI International GmbH and specialises in overlaps between information technology and the humanities. As a member of several project related working groups, e.g. 'Federated Identity management for DARIAH (FIM4D)' and the Authentication and Authorisation for Research and Collaboration (AARC) project, and therefore particularly experienced in collaborative settings, Peter Gietz was an ideal candidate for the AAI workshop. He was included in the process of developing a program and advised task 4.1 members in content issues. Furthermore, the organisers benefited from his extended network; Peter Gietz recommended Miroslav Milinovic to give a presentation during the workshop. Mr. Milinovic from the Computing Centre of Zagreb University (Croatian Research and Education Identity Federation) joined the workshop to introduce eduGAIN, a GÉANT project with the aim of enabling research and education organisations to exchange information securely. Mr. Gietz and Mr. Milinovic complemented each other to the great benefit of the workshop, since the former represented a research infrastructure (DARIAH-DE) and the latter represented an operator of a national federation (i.e. the Croatian) and thereby the inter-federation eduGAIN.

# 2 WORKSHOP AAI - GENERAL DESCRIPTION

## 2.1 AIM OF THE WORKSHOP

Following the key objective of WP4, the workshop aimed fostering knowledge exchange between current CESSDA members and potential or aspiring members. The idea was to introduce different AAI solutions and discuss their technical and policy implications. In addition, the participants had the opportunity to describe current AAI solutions of their organisations. Furthermore, and with a special emphasis on learning

about the needs of aspiring or small members, challenges of the implementation process were discussed. The integration workshop aimed mainly as a kick-off meeting for the discussion on implementation strategies for AAI within CESSDA.

The desired outcome of the workshop was for participants to gain knowledge about different AAI solutions and discuss these in their home organisations as the foundation for encouraging all CESSDA (aspiring) members to engage in a lively (joint) discussion on the topic in the future.

## 2.2   TARGET AUDIENCE

The integration workshop was part of the "Second Training workshop on Trust and Technical Aspects within the CESSDA infrastructure". Having both technical and policy oriented sessions, the organisations were asked to send technical and non-technical staff members to join. In the end, only a small number of the 21 CESSDA service providers' employees attending the integration workshop on AAI had a technical background. However, the program was adjusted accordingly, focusing on best-practice examples and an extended discussion on the implementation of AAI solutions with a special emphasis on the question in which way CESSDA will be able to support (aspiring) member organisations in this matter.

## 2.3   WORKSHOP APPROACH

The workshop was held by an external and very knowledgeable speaker. Mr Gietz presented theory on AAI enriched with several use cases in a traditional teaching setting. The last session was planned as a more hands-on session. During one of the preparation calls the organisers discussed ways to ensure giving participants the opportunity to discuss their questions. Furthermore, a so-called 'wall of wonder' -inspired intermezzo was included wherein the participants could share their views on how a 'perfect AAI'-solution would look like, and discussed what would be needed to achieve this in their organisation. The second speaker, Miroslav Milinovic, provided valuable input on the Croatian experiences which resulted in a very lively and interactive Q&A with the participants.

## 2.4   PROGRAMME

The Workshop on AAI contained four sessions: an introductory plenary 45-minute session, two 90-minute sessions on technologies and solutions, and a hands-on session about the implementation and development of AAI solutions. The last session was spent mostly on a discussion of questions and remarks from the participants. During the hands-on technical session guidance based on the sheets that also contained implementation examples specifically for developers was provided. The following chapter includes short descriptions of the topics and questions discussed during the sessions.

## 2.5   WORKSHOP AAI – SESSIONS

As described in the programme the workshop contained four sessions which are described in more detail below. The slides presented by Peter Gietz and Miroslav Milinović may be found in the ANNEX of this report.

### 2.5.1   PLENARY SESSION: INTRODUCTION TO AAI

The integration workshop sessions on AAI started with a plenary session moderated by Peter Gietz, which aimed to reach a broad audience by introducing the topic to interested service provider employees. AAI terminology was introduced, including terms such as 'Identity Provider', 'Service Provider' (clearly differentiated from the CESSDA Service Provider term), 'Federation' and 'Federated Identity Management'.
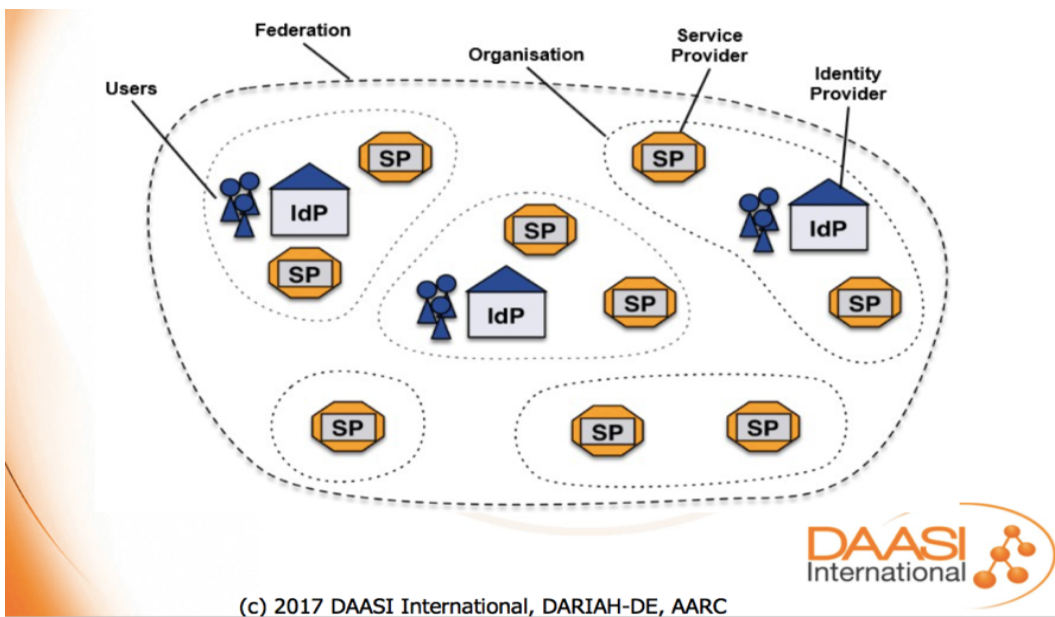


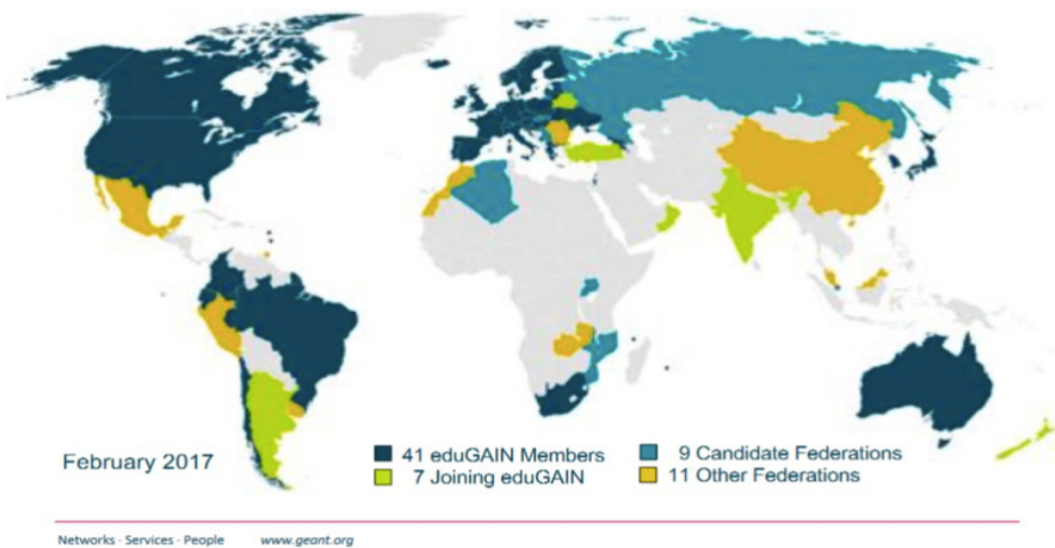Figure 1: Introduction of AAI terminology



Figure 2: EduGAIN members across the world (February 2017)

Furthermore, Peter Gietz introduced already existing AAI projects including best practice examples, such as eduGAIN. Becoming a member of the world-wide interfederation eduGAIN, interconnecting identity federations, is seen as an important step in the process of implementing AAI. eduGAIN was established in 2011 and acts as a policy framework as well as a metadata distribution service. For CESSDA a Europewide AAI can be achieved with eduGAIN.

As research e-infrastructures have similar AAI requirements, Peter Gietz reported on the workshops held for a federation for eHumanities and eSocial Sciences (DARIAH/DASISH workshop: http://dariah-aai.daasi.de/, 10 'Federated Identity Management for Research'-workshops (FIM4R), the common vision for Federated Identity Management (https://cdsweb.cern.ch/record/1442597).
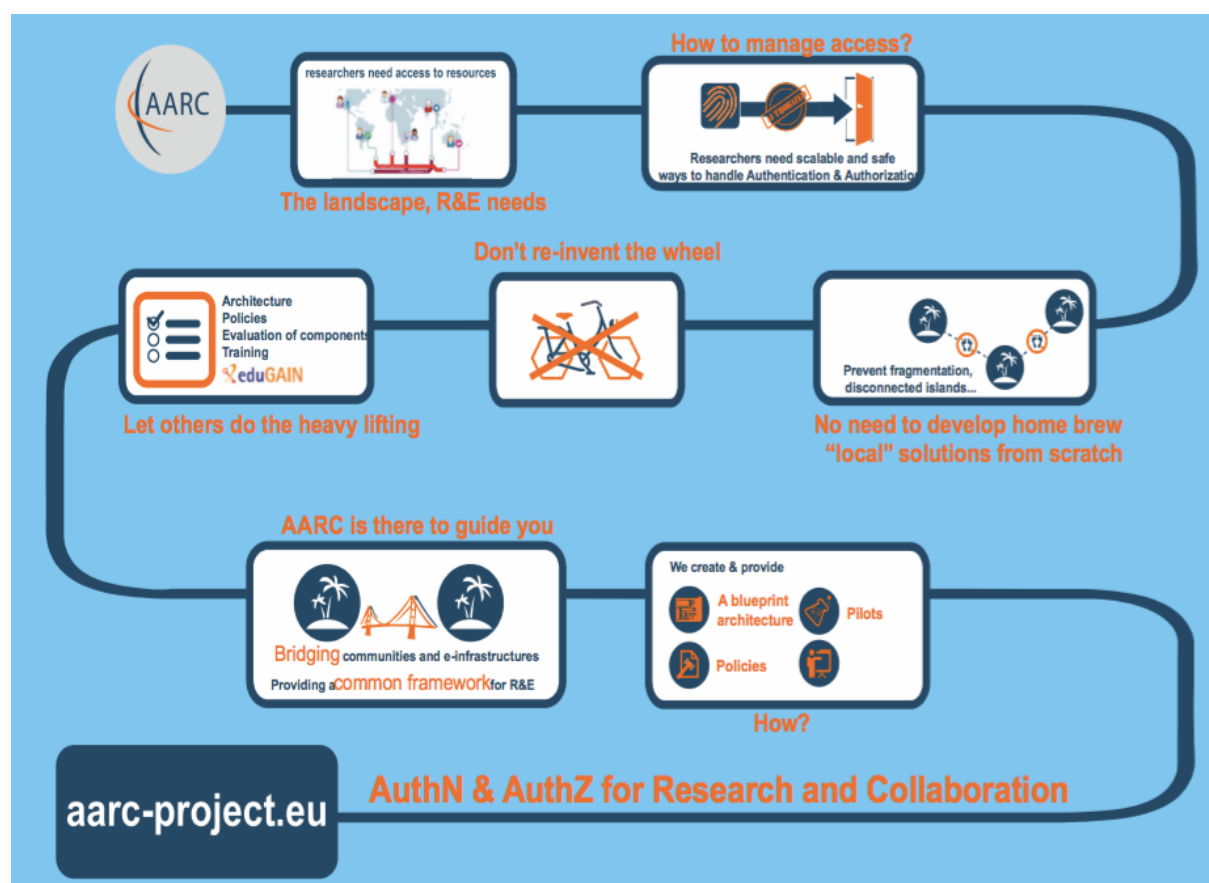


Figure 3:  AARC Project

Project AARC can be seen as an outcome of FIM4R and eduGAIN and infrastructure projects EUDAT (eudat.eu) and EGI (egi.eu). Within AARC2 there will be AARC pilots and demonstrators again that might be interesting for CESSDA.

### 2.5.2    SESSIONS I & II: TECHNOLOGIES & SOLUTIONS

The following two sessions were designed to bring together technical staff of CESSDA service providers. AAI infrastructures and preparations towards its implementation into the participants' home organisations were discussed, as well as an overall strategy to implement AAI in the CESSDA community.

The first of these two sessions started with an introduction round: The participants gave a short overview on the CESSDA Service Provider's current AAI status and their expectations from the future implementation of AAI. This was followed by a description of AAI techniques, case studies, and best practices by Peter Gietz. Thereafter Miroslav Milinovic gave an introduction into the current status and best practices of the Croatian Hub&Spoke Federation. The AAI@EduHR was established in 2006 and is a hub-and-spoke architecture, connected to eduroam and eduGAIN in cooperation to the national service NIAS. This solution might serve as a best practice example for the implementation of AAI strategies.  SRCE also provides workshops for this purpose.

During the final part of this session, Peter Gietz continued with a more detailed description of AAI standards, components, and protocols. Participants had the opportunity to ask questions and Peter Gietz shared more technical examples on authentication for non-academic users, particularly on how to enable access confidential data.

### 2.5.3    SESSION III: IMPLEMENTATION & DEVELOPMENT

This session was originally planned to be a hands-on technical session focusing on design, development, and implementation of AAI solutions. The program was adapted to reach the background knowledge of most participants, not focussing too much on technical aspects but more on exchanging ideas on the implementation of AAI.

During the interactive beginning of the session, participants were asked to share their ideas on a 'perfect AAI'. Furthermore, they were asked to make suggestions on how CESSDA could support the service providers in achieving this 'perfect AAI'. There was consent among participants on the following aspects being relevant for the implementation of a 'perfect AAI': technical support by CESSDA, a good tool (keeping in mind that Nesstar does not support AAI), and the harmonisation of attribute definitions about users (e.g. EduPerson Attributes, and memberOf). Furthermore, Virtual Research Environments (VRE) were considered very important.

According to the participants, CESSDA could support the road to a 'perfect AAI' by making the use of both national AAIs and a CESSDA AAI possible. Peter Gietz suggested doing so by either inter-federating, an own separate federation, or by connecting single service providers and identity providers with the various national federations. It should be stressed here, that centralised technical support (by CESSDA MO or an archive with AAI in place) was seen as an important aspect of a 'perfect AAI' solution. With regard to a platform independent solution, some participants favoured support by the UKDA. All participants agreed that a 'perfect AAI' solution cannot mean imple-

menting the same AAI tool for all, although this would enable finding the metadata and accessing data. Due to national regulations, in practice the implementation would consist of interoperable AAIs. The service providers should agree on a uniform method to handle personal data, for example by protection of sensitive data via anonymisation as well as regulating access using privileged roles or groups and higher levels of authentication; these methods require additional resources to maintain the system. Also, some participants suggested providing guidance on the integration with existing authentication systems or produce migration guides.

Specifically addressing the group of technical staff, the last part of the workshop was dedicated to the question of integrating an application with a Shibboleth SP, during which different strategies were introduced.

## 3   WORKSHOP AAI - RESULTS & FUTURE IMPLICATIONS

The workshop sessions on AAI were characterized by an excellent working atmosphere. In conclusion, they resulted in the following achievements:
1.   Introduction into AAI solutions and already existing projects
2.   Identification and discussion of the Service Provider's main requirements and concerns
3.   Identification of the most suitable AAI solutions for CESSDA

The following questions, requirements, and ideas will be further discussed as the foundation of a joint implementation of AAI solutions within CESSDA:

- How can national/individual AAI solutions be connected to the CESSDA community? CESSDA should support strategies, enabling CESSDA Service Providers to use both their national as well as CESSDA AAI solution, either as inter-federate or as separate federations. Also, there is the possibility to include single SP and IdP into the various national federations.
- A common AAI solution for CESSDA requires excellent technical support, either provided by CESSDA or by one of the experienced CESSDA Service Providers who has in-house experts and experiences on the topic.
- A common AAI strategy for all CESSDA members would facilitate access to data and metadata. However, disseminating personal data online comes with serious security challenges. Therefore, the CESSDA Service Providers must agree on a common approach to handle these data in line with current national and European data protection regulations (e.g. limiting distribution to anonymised data sets).
- Questions to consider, when implementing AAI in CESSDA:
    - Can AAI solutions be used to allow access to confidential data?
    - Can a common CESSDA AAI provide solutions to data-access for non-academic users, or for Virtual Research Environments?
    - Deciding on an appropriate AAI solution/tool is a significant challenge for CESSDA Service Providers, especially for those who are obligated to use a particular system due to national provisions.

# 4 Annex

- LIST OF ATTENDANCE/ORGANISATIONS
- LIST OF FIGURES
- PRESENTATION: PETER GIETZ
- PRESENTATION: MIROSLAV MILINOVIĆ

## LIST OF ATTENDANCE/ORGANISATIONS

| List of attendance/organisations | |
|---|---|
| CESSDA AS | CESSDA Main Office |
| CESSDA – TWG | CESSDA TECHNICAL WORKING GROUP |
| ADP | Slovenian Social Science Data Archives |
| AUSSDA | Austrian Social Science Data Archive |
| CSDA | Czech Social Science Data Archive |
| DAASI* | DAASI International GmbH |
| DANS** | DANS / Koninklijke Nederlandse Akademie van Wetenschappen |
| EKKE | Ethniko Kentro Koinonikon Erevnon |
| FORS | Swiss Foundation for Research in the Social Sciences |
| FSD | Finnish Social Science Data Archive |
| GESIS** | GESIS - Leibniz Institute for the Social Sciences |
| IES | Institute of economic sciences Serbia |
| ISPJR | Institute for sociological, political and juridical research Macedonia |
| ISSDA | Irish Social Science Data Archive, University College Dublin |
| NSD | Norsk samfunnsvitenskapelig datatjeneste AS |
| Polish SDA | Polish Social Data Archive (ADS) |
| SND | University of Gothenburg - Swedish National Data Service |
| SRCE* | University of Zagreb - Computing Centre |

* Trainer/speaker
** Organisers

# List of figures

# CESSDA
# AAI Workshop

Second Training workshop on Trust and Technical Aspects within the CESSDA infrastructure

Peter.Gietz, DAASI International

`Peter.gietz@DAASI.de`

# Agenda 1/2

- Plenary Part 2
  - Very short introduction to AAI by Peter Gietz
  - research e-Infrastructure AAI benefits, objectives, etc. for researchers and service providers by Peter Gietz
  - CESSDA's AAI situation and plan (AS-IS and TO-BE situations) by Hossein Abroshan
- AAI Session 1 [11:00-12:30]
  - AAI techniques in a nutshell by Peter Gietz
  - CESSDA Service Provider's current AAI status, and their expectations from AAI by all participants
  - case studies and best practices in the frame of the DARIAH-AAI by Peter Gietz
  - current status & experiences from the Croation Hub&Spoke Federation by Miroslav Milinovic

# Agenda 2/2

- ➢ AAI Session 2 [14:00-15:30]
  - ▪ standards and technologies
  - ▪ AAI components, dataflow, protocols, ...
  - ▪ Authentication and Authorization technologies/comparison
  - ▪ federation and inter-federation
  - ▪ How to implement AAI
- ➢ AAI Session 3 [Day 2 09:00-10:30]
  - ▪ technical solutions to include services into existing AAI infrastructures based on Shibboleth Service Provider
  - ▪ example codes, PHP, Perl and Java

DAASI International

# Very short introduction to AAI
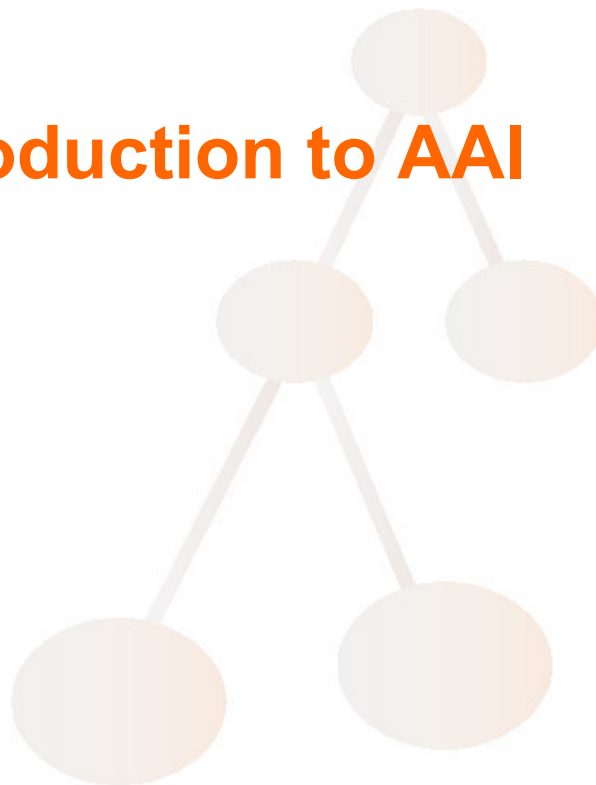
# What is AAI?

- ➢ **AAI stands for Authentication and Authorization Infrastructure**
- ➢ **It is mostly used in the sense of an infrastructure that allows for Federated Identity Management (FIdM)**
  - ▪ **IdM: Systems for the management of computer records that map identities of persons. Such records contain unique names (e.g. login name), Credentials (e.g. password) and any needed information about the person, such as name, email, group memberships, etc. IdM takes place within an organisation**
  - ▪ **FidM: Systems that allow for using identities beyond cross organizational borders**
- ➢ **Such infrastructures allow the user to authenticate (proove her identity to a technical system) and services to decide about access based on authorization information**
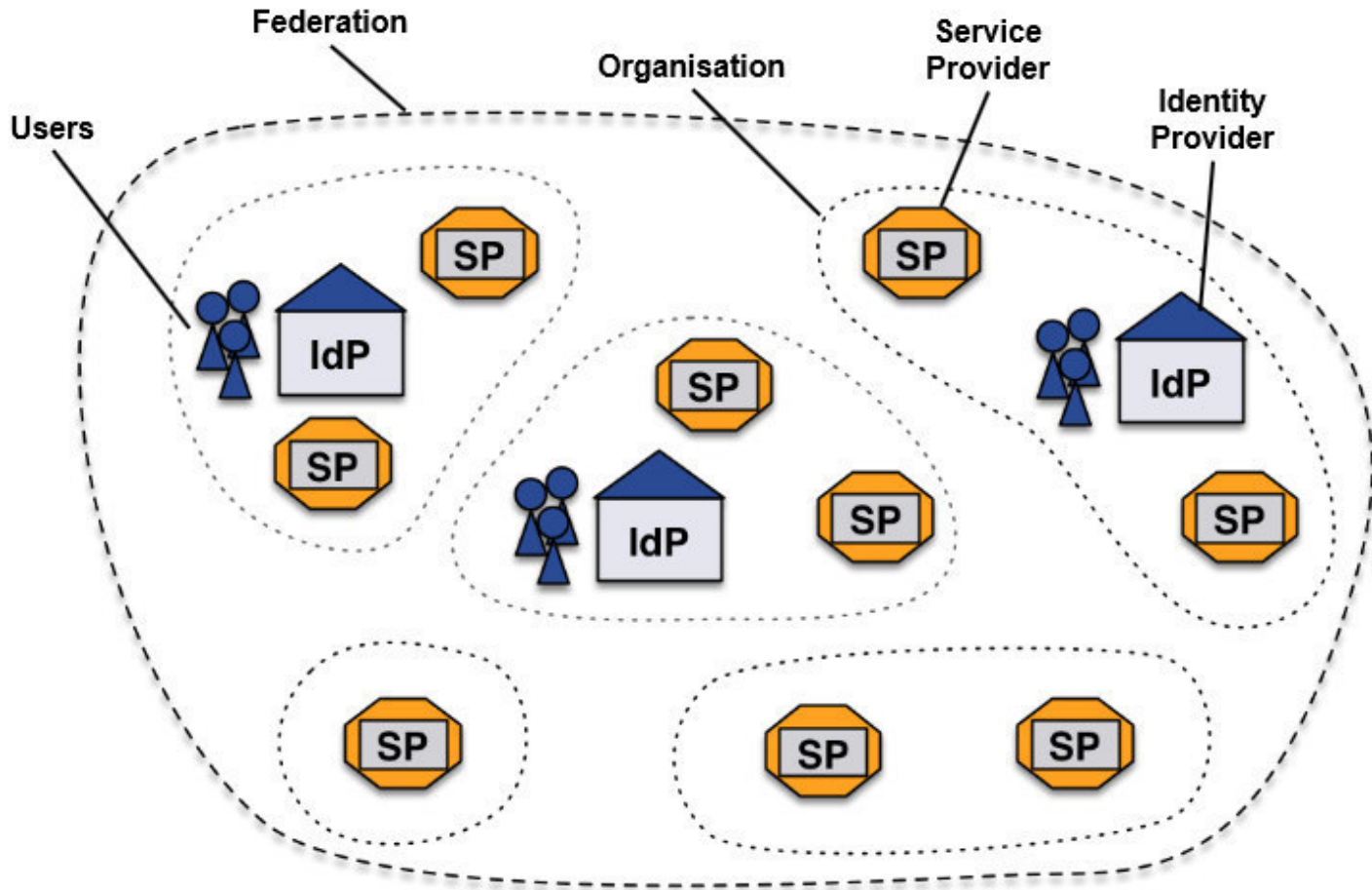
# Identity Management
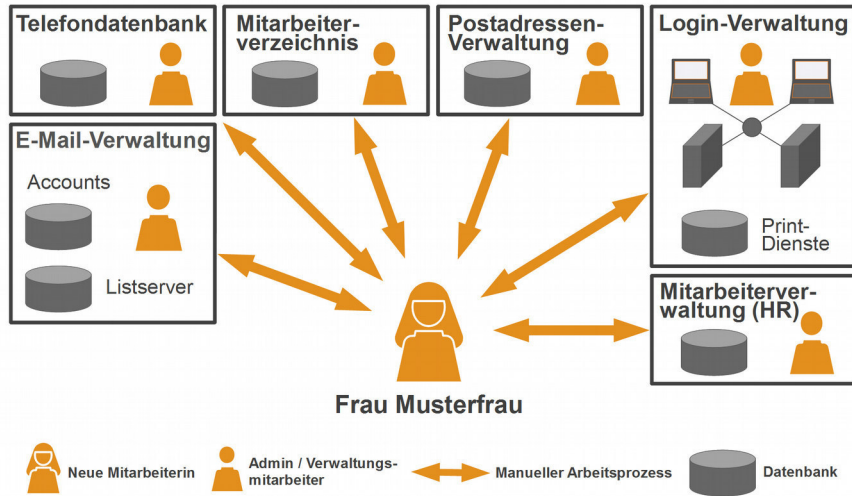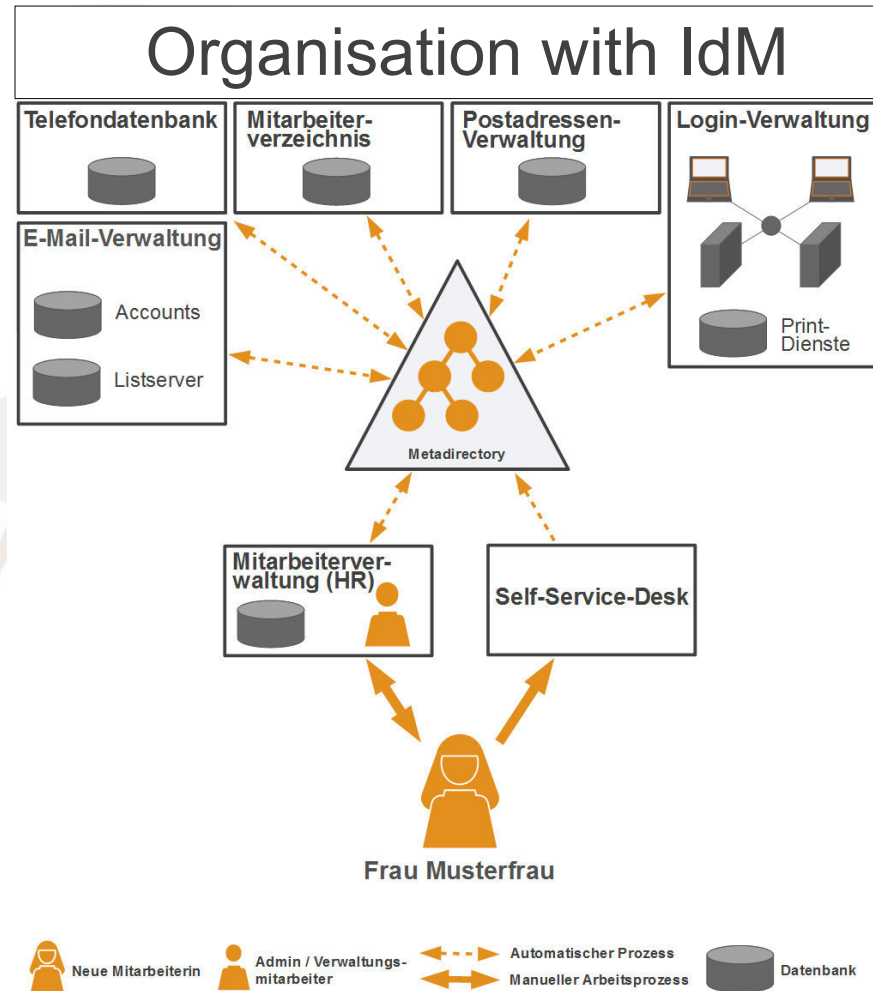
# What is a federation?

- ➢ **Two or more organizations can form a federation to share resources**
  - ▪ **Trust within the federation is established by contracts**
- ➢ **The organization can have one or two roles:**
  - ▪ **Identity Provider (IdP)**
    - • **having an Identity Management, so that their users can authenticate**
    - • **state in contract that the information about the identities is correct**
  - ▪ **Service Provider (SP)**
    - • **providing any kind of resource to authorized users within the federation**
    - • **State in contract that they will use the data given by the IdP only for the agreed upon use case**

**DAASI** International

# What is a federation?

- ➢ **A Federation also needs a central management**
  - ▪ **Taking care of the contracts (1 to n instead of n to n)**
  - ▪ **Managing the membership list**
  - ▪ **Managing technical data about the computer systems involved (URLs, server certificates)**
  - ▪ **Managing a central discovery service (DS)**
- ➢ **Summary: A federation is a group of organizations running IdPs and SPs that agree on a common set of rules and standards**
  - ▪ **It's a label - to talk about such a collection of organizations**
  - ▪ **An organization may belong to more than one federation at a time**

# The whole picture

# Benefits of Federated Identity Management

- ➢ **Reduces work**
  - ▪ **You do not need a separate user account at every Service**
  - ▪ **Less management, less passwords forgotten, etc.**
- ➢ **Provides current data**
  - ▪ **Data are only managed at the "home organization" of the user, which knows best, e.g. if a student still belongs to the university.**
  - ▪ **By having Identity Management data are held current automatically**
- ➢ **Insulation from service compromises**
  - ▪ **Data gets pushed to services as needed**
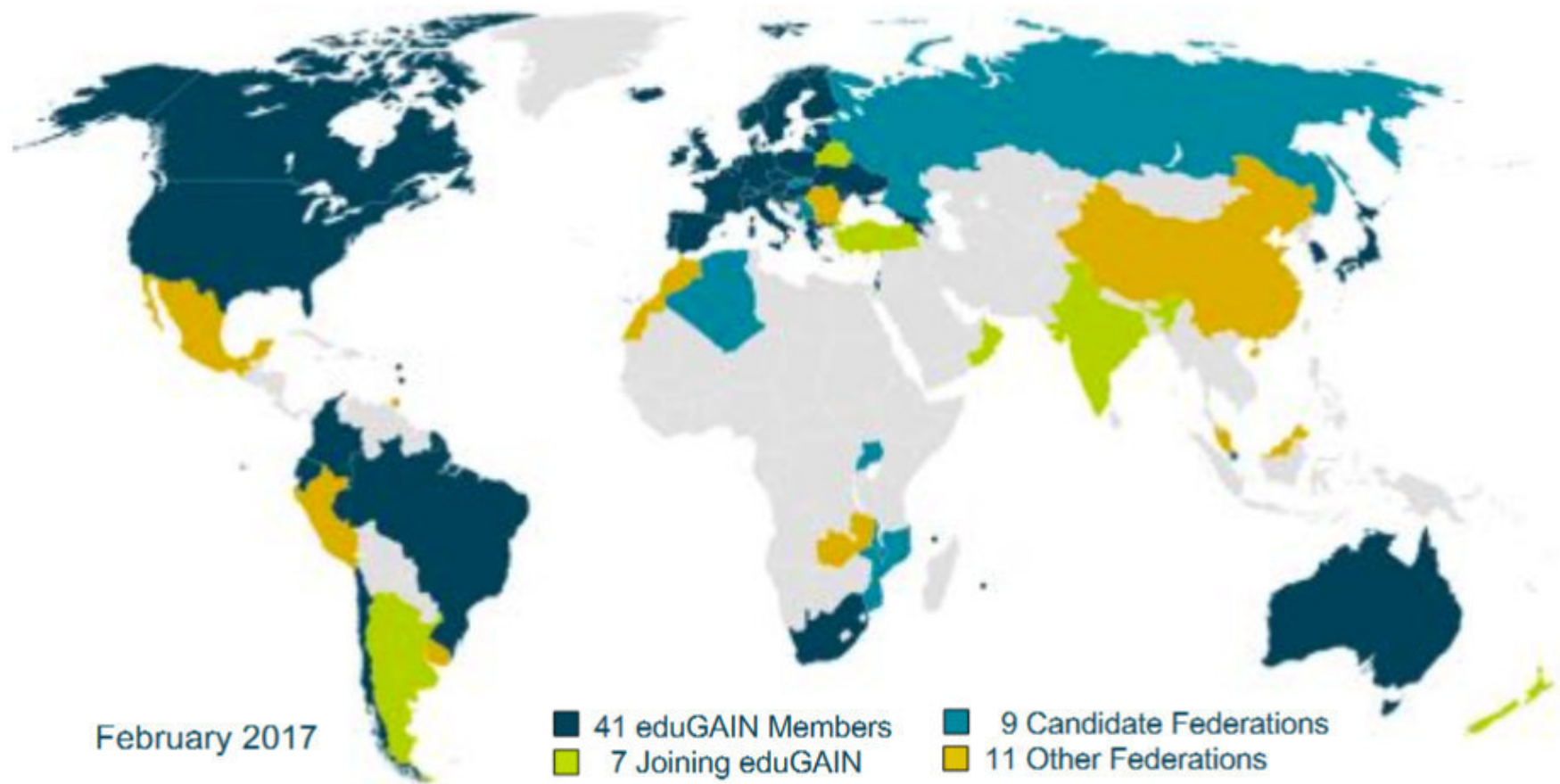  - ▪ **An attacker can't get everyone's data on a compromised server**

# Benefits of Federated Identity Management

➢ **Insulation from service compromises**
- ▪ **Data gets pushed to services as needed**
- ▪ **An attacker can't get everyone's data on a compromised server**

➢ **Minimize attack surface area**
- ▪ **Only the IdP needs to be able to contact user data stores**
- ▪ **All effort can be focused on securing this single connection instead of one (or more) connection per**

**DAASI International**

# Benefits of Federated Identity Management

➢ **Users generally find the resulting single sign-on experience to be nicer than logging in numerous times.**

➢ **Usability-focused individuals like that the authentication process is consistent regardless of the service accessed (with exception of IdP Discovery).**

➢ **A properly maintained federation drastically simplifies the process of integrating new services.**

➢ **There are a lot of higher-ed national federations operated by the NRNs**

➢ **There is a world-wide interfederation called eduGAIN**

# eduGAIN & Federation Status

**GÉANT**



February 2017

- ■ 41 eduGAIN Members
- ■ 7 Joining eduGAIN
- ■ 9 Candidate Federations
- ■ 11 Other Federations

# research e-Infrastructure
## AAI benefits, objectives, etc.
### for researchers and service providers

# Research e-Infrastructures

➢ **Research becomes more and more digital**

➢ **Virtual Research Environments help researchers in the whole research lifecycle**

➢ **Research infrastructures provide**

▪ **generic services, such as Computing facilities, Storage, generic search systems, repositories, etc, etc.**

▪ **And an infrastructure that makes sure that only those can access services and data, that are authorized.**

➢ **AAI technologies are thus vital for research infrastructures**

➢ **Research Infrastructures have similar AAI requirements, thus it makes sense that they communicate**

**DAASI**
International

# DARIAH-DASISH workshop

- ➤ **DARIAH/DASISH Workshop on a Federation for eHumanities and eSocial Science**
  - ▪ **Cologne October 17-18, 2013**
  - ▪ **Took place at GESIS with participants from CESSDA community**
- ➤ **Results can be seen at**
  - ▪ **http://dariah-aai.daasi.de/**

DASISH

DARIAH-DE

DAASI International

# FIM4R

- ➢ **A lot of research communities have set up research infrastructures**
- ➢ **These are often interoparable with AAI**
- ➢ **They are operated and used transnational**
- ➢ **Some of these research infrastructures have met**
  - ▪ **To formulate their requirements to the NRNs / to eduGAIN**
  - ▪ **To learn from each others experiences and technologies used**
- ➢ **These meeting were named FIM4R workshops (Federated Identity Management for Research)**

# FIM4R

- ➢ **10 Workshops:**
  - ▪ **The first workshop was held at CERN in June 2011**
  - ▪ **the second at RAL in November 2011**
  - ▪ **the third at ISGC in February 2012**
  - ▪ **the fourth at MPI Psycholinguistics Nijmegen in June 2012**
  - ▪ **the fifth at PSI Villigen in March 2013**
  - ▪ **the sixth at CSC in Helsinki in October 2013**
  - ▪ **the seventh at ESRIN in Franscati in April 2014**
  - ▪ **the eighth at CERN on 3-4th February 2015**
  - ▪ **the 9th FIM4R in Vienna on 30th November 2015**

# FIM4R

➢ **Through these workshops, the research communities have converged on a common vision for FIM, enumerated a set of requirements and proposed a number of recommendations for ensuring a roadmap for the uptake of FIM is achieved.**

➢ **These points have been documented in a paper**

▪ **https://cdsweb.cern.ch/record/1442597**

# FIM4R

➢ **The requirements paper was read by the NRNs/eduGAIN community**

➢ **Basically one outcome of the fruitful discussion between FIM4R and eduGAIN was the Horizon 2020 Project AARC**

- ▪ **Authentication and Authorization for Research Colaborations**
- ▪ **AARC 2 is currently starting**

➢ **The 10th FIM4R workshop**

- ▪ **took place last week in Vienna**
- ▪ **Assessed the progress of the Ris**
- ▪ **Integrated the two**
- ▪ **Brought back the results of AARC 1 to FIM4R**
- ▪ **layed the ground work for a version 2 of the FIM4R paper.**

**Boosting AAI for research and collaboration**

**David Groep**

*NA3 – Policy Harmonisation and Best Practice coordinator*

Nikhef



10th FIM4R Meeting

Vienna, 20-21 February 2017

**AARC**

researchers need access to resources

**The landscape, R&E needs**

**How to manage access?**

Researchers need scalable and safe
ways to handle Authentication & Authorization

**Don't re-invent the wheel**

Architecture
Policies
Evaluation of components
Training
**eduGAIN**

**Let others do the heavy lifting**

Prevent fragmentation,
disconnected islands...

**No need to develop home brew
"local" solutions from scratch**

**AARC is there to guide you**

Bridging communities and e-infrastructures
Providing a common framework for R&E

We create & provide

A blueprint
architecture

Pilots

Policies

**How?**

aarc-project.eu

**AuthN & AuthZ for Research and Collaboration**

# Starting Point: Identified Requirements

Attribute Release

User Managed Information Assurance

Community based AuthZ

Attribute Aggregation Persistent Unique Id

Guest users

Best Practices

User Friendliness Translation

Step-up AuthN

Social & e-Gov IDs

SP Friendliness Credential Delegation Web-browser

Incident Response

**Addressing e-Research Requirements**

Date: 6 March 2012

Sergio Florio (TERENA), Nicole Harris (JISC Advance), Christoph Witzig (SWITCH), Ajay Daryanani (RedIRIS), Ann Harding (SWITCH),

**Advancing Technologies and Federating Communities**

A Study on Authentication and Authorisation Platforms For Scientific Resources in Europe

# Common Scenario

- The scenario:

  - There is a **technical architect of a research community**

  - Her community is **distributed internationally**

  - **Increasing number of services** need authentication and authorization

  - She wants to **focus on research** and not reinvent the wheel

  - She starts googling and asking around

- So, there are some solutions available, but…

# Think Global: the AARC project

Bring federated access to eResearch

Avoid a future in which new research collaborations develop independent AAIs

Build on existing tools and framework

# What AARC does want to change and how

- Improve usage of FIM – Promote usage of FIM and organise training to leverage identity providers outside the academic boundaries

- Address Research requirements – Design a technical Blueprint Architecture that builds on top of eduGAIN to add components required

- Offer support for global policies – Sponsor the development of key policy frameworks that aim to add additional 'flavours' to eduGAIN.

- Sustainability – Ensure that operations of components of the blueprint architecture and deployment of assurance, security and policy frameworks rest with r/e-infrastructures

# Pilots and demonstr...



- AttributeManagementPilot
- AuthX509toSAMLDemo
- BBMRIAAIPilot
- CILogon-like pilot
- COmanageORCIDPilot
- COmanageSSHPilot
- LibrariesCockpitPanelConsortiumProxy
- LibrariesCockpitPanelEZproxy
- LibrariesCockpitPanelWalkInUsersPortal
- ORCIDpilotCockpitPanel
- PerunVOMSCILogonPilot
- SocialIDCockpitPanel

https://wiki.geant.org/display/AARC/Pilot+results+and+demo

# Solving the Policy Puzzle

**Pushing forward best practices and like policies across many participants**

- "Levels of Assurance" – baseline and differentiated profiles, capabilities and grouping
- "Incident Response" – beyond Sirtfi: a common understanding on operational se  r
- "Sustainability, Guest IdPs, use models" – how can a service be offered in the   run?
- "Scalable policy negotiation" – helping SPs move beyond bilateral discussion
- "Protection of (accounting) data privacy" – necessary aggregation without bre    the law too much
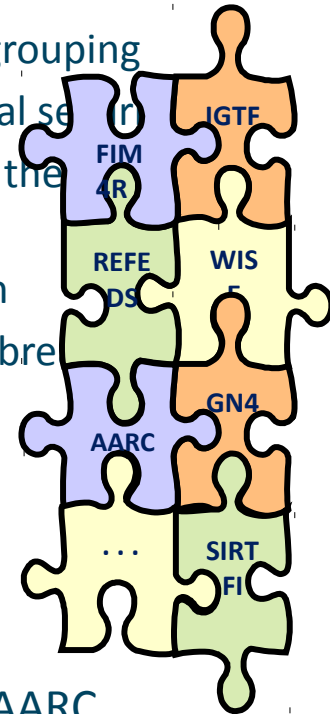
## Strategy

to support and extend established and emergent groups

leverage their support base - and 'multiply' the effect of policy work from AARC

# AARC2  In three bullets

## Support Use-driven approach

Enable federated access for a number of selected use-cases that meet data intensive and cross e-Infrastructures requirements

## Deploy AARC/AARC2 Results

Support e-Infrastructures to deploy AARC/AARC2 results to enable service delivery across all of them

## Continue the Training

Offer different level of training to enable communities do use the underlying AAIs when building new services

# Two new engagement mechanisms
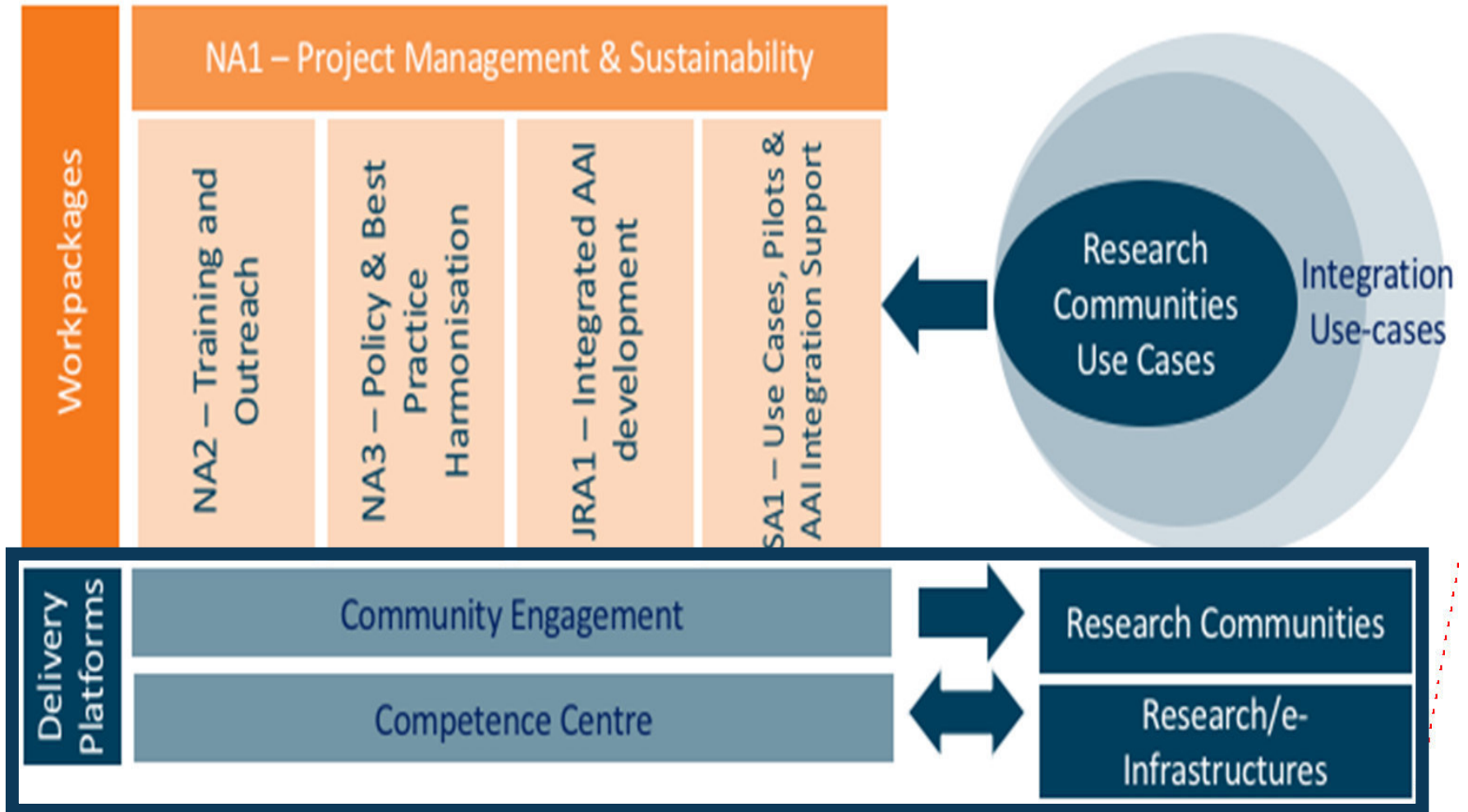
# Questions from Participants
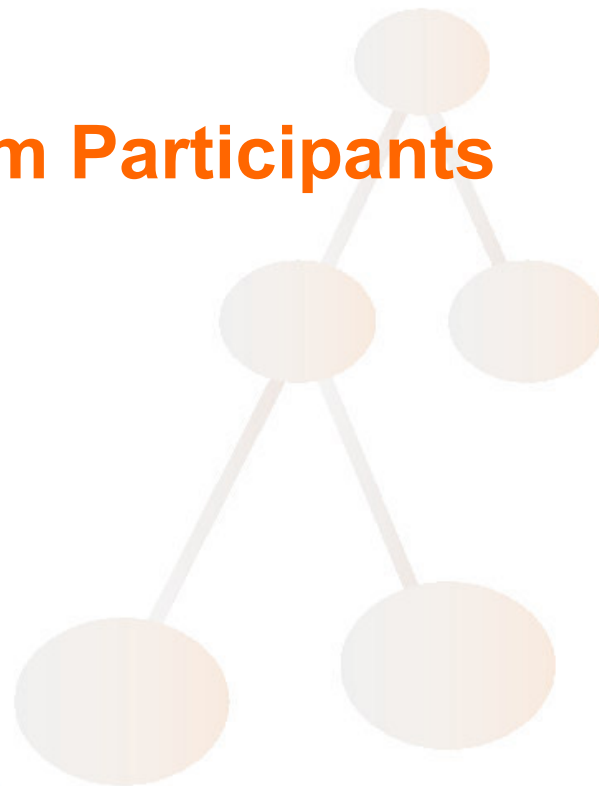
# Questions from you

➢ WAYF less URLs implementation for Central Discovery Service in our proxy IDP - possible examples

➢ Authentification for non-academic users, examples?

➢ Can AAI be used to allow access to confidential data? Can we extend the credentials to facilitate accreditation and/or ensure LOGIN is from a secure location?

➢ How would the national AAI infrastructures be connected to the CESSDA system?

# Postits from you

➢ "Perfect AAI"
- CESSDA  Technical support (UKDA)
  - Hossein: Yes there will be such
- Tools that would support dissemination of data files and AAI?
  - e.g. Nesstar does not support AAI
    - This is a politcal issue
- Harmonize Attribute definitions about users
  - EduPerson Attributes, such as ePAffiliation, ePEntitlement, but also attributes like memberOf (a priviledge group)

# Postits from you

➢ "Perfect AAI"
  ▪ AAI for Virtual Research Environments
    • VREs will happen more and mote and CESSDA should play a role here
    • Depends on the role of the archives in the different countries
    • Again a very political issue

# Postits from you

➢ Road to "Perfect AAI"

- CESSDA has to make it possible to use both national AAIs and a CESSDA AAI
  - Either interfederate an own separate federation
  - Or put the single Sps and IdP into the various national federations
- Platform independant (UKDA)
  - Support of MS IIS
    - Using IS-API?
- Technical support
  - Either from CESSDA Main Office
  - Or SP that already have something

# Postits from you

➢ Road to "Perfect AAI"

▪ If all the archives used the same AAI this would help the service providers with finding the metadata and accessing data etc.
However, it is a serious security problem to distribute personal data on the internet. Thus the service providers must agree on a <u>uniform method</u> to handle these data (e.g. only distribute anonymized data sets).
The features are out there, e.g. ADDS. However, the organizations need to agree on using the same system which is a politically hard decision to make; it requires extra resources to maintain the system when required

• Also an non-AAI question

• Protection of sensitive data via anonymization and via regulating access via priviledge roles or groups and higher levels of authentication

# Postits from you

➢ Road to "Perfect AAI" last long statement:
  - Not same AAI but interoperable AAIs
  - Also an non-AAI question
  - Protection of sensitive data via anonymization and via regulating access via priviledge roles or groups and higher levels of authentication
  - EduGAIN is only about visibility, the SP in any case decides who is able to use its service (authorization)

➢ Integration with existing authentication systems or produce migration guides

# Postits from you

➢ Road to "Perfect AAI"
  ▪ Shibbolized Nesstar for all!
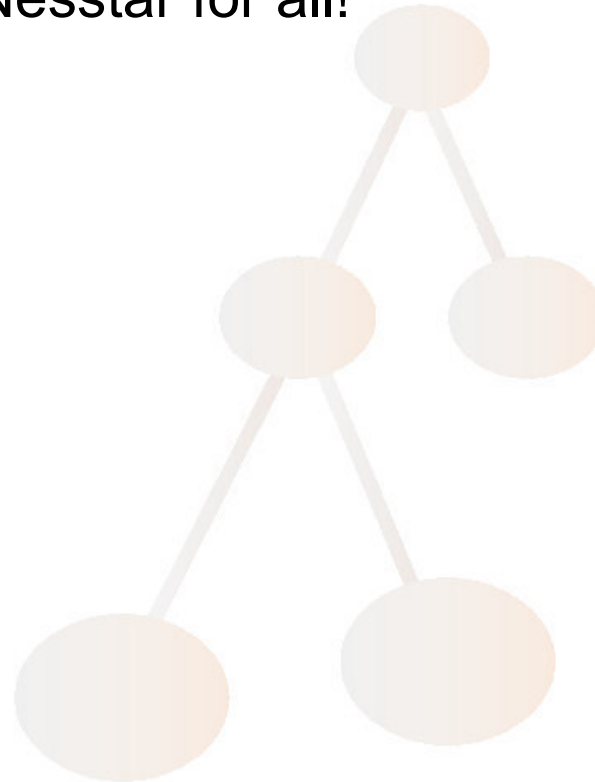
# Introduction to SAML

# SAML Basics

➢ **OASIS Standard, current version 2.0, March 2005**
➢ **Security Assertion Markup Language (SAML) specifies**
  ▪ **Profiles (e.g. Web Browser SSO, Single Logout, Assertion Query, Attribute Usage)**
  ▪ **Data exchange formats (esp. Assertions)**
  ▪ **Protocols and Bindings**
  ▪ **Metadata**
➢ **Components:**
  ▪ **Identity Provider (IdP), lets users log in using the home organization's user directory**
  ▪ **Service Provider (SP), protects Web resources and provides for information about the user sent by the IdP**
  ▪ **IdP Discovery Service (DS, old term: Where-Are-You-From, WAYF)**

**DAASI International**

# SAML Profile: Web Browser SSO (with IdP Discovery)

**(c) SWITCHaai**
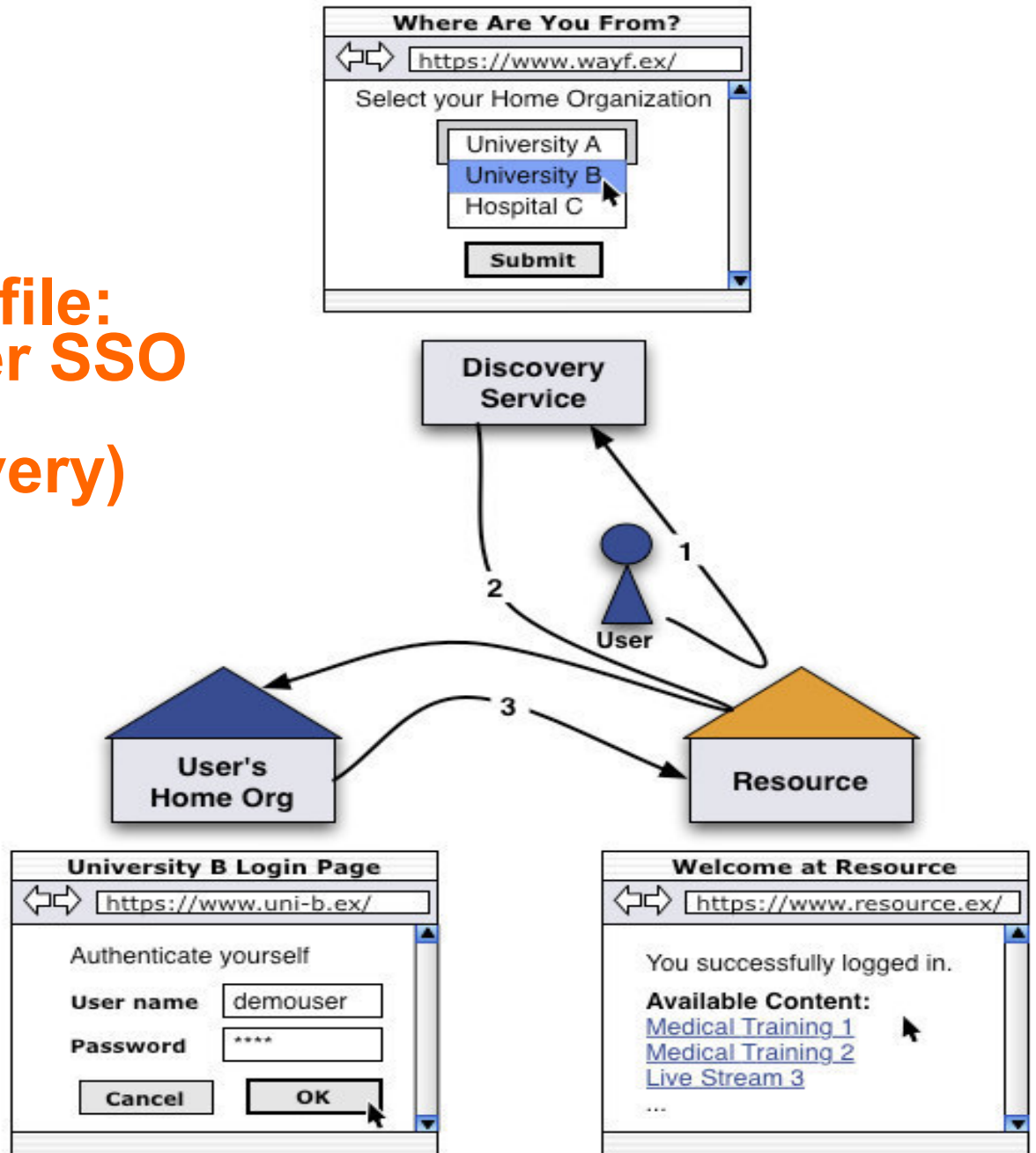
# SAML Vocabulary

➢ **Authentication, authN: proof a user's identity**

➢ **Authorization, authZ: grant the user access to a resource**

➢ **Single Sign-On, SSO: any mechanism enabling login without user interaction**

➢ **Authentication Request, issued by an SP for an IdP**

➢ **SAML Assertion, issued by an IdP for an SP**

➢ **EntityID: ID of an SP or IDP (an URL or URN)**

➢ **AA: Attribute Authority, Endpoint at IdP**

➢ **ACS: Assertion Consumer Service, Endpoint at the SP**

➢ **Session: Security context and cached data for a logged-in user (exists at both the IdP and the SP)**

➢ **SessionInitiator: Part of SP that generates SSO requests**

➢ **Artifact: A reference to an Assertion**

**DAASI International**

# SAML Assertion

- ➤ „SAML Ticket" issued to one single SP
- ➤ Usually signed and encrypted
- ➤ Can contain max. 3 statements:
  - 1 Authentication Statement: AuthN instant + method
  - 1 Attribute Statement: 1..n Attributes, each 1..n values
  - 1 Authorization Decision Statement
- ➤ Contains besides the three statements:
  - Issue Instant and Issuer EntityID
  - Signature by the IdP
  - Information about the authenticated Subject: Name Identifier (Format + Value), EntityID of IdP and SP
  - Conditions (optional), e.g. AudienceRestriction for the SP

# SAML Profiles

➢ **Web Browser SSO using various bindings (HTTP Redirect, HTTP POST, Artifact, SOAP)**

➢ **Enhanced Client or Proxy (ECP) for Browser-like Web Service Clients**

➢ **IdP Discovery**

➢ **Single Logout via Front- or Back-Channel**

➢ **Artifact Resolution**

➢ **Assertion Query / Request**

➢ **Various other:**

  ▪ **Name Identitfier Management**

  ▪ **Name Identifier Mapping**

  ▪ **Attribute Naming Formats**

# SAML further Core Concepts

- **Protocols**
  - **Abstract form: Request / Response**
  - **Usually one for each of the mentioned profiles**
- **XML Signature**
- **XML Encryption**
- **Bindings: method how a message is transported**
  - **HTTP Redirect**
  - **HTTP POST (and HTTP-POST-SimpleSign)**
  - **SOAP and reverse SOAP (PAOS)**
  - **„HTTP Artifact" (plus SOAP)**

# Base for SP ↔ IdP interaction

- ➢ **Metadata**
  - ▪ **SPs find information about IdPs, e.g. various endpoint locations for each binding, e.g. the SSO Service**
  - ▪ **IdPs find informationen about SPs, e.g. the ACS**
  - ▪ **embedded public X.509 keys for signature and encryption**
  - ▪ **various extensions (logo urls, contact info, Attr needs)**
  - ▪ **Metadata are public and usually signed**
- ➢ **Common Attribute encoding format, e.g.**
  - ▪ **urn:oid:2.5.4.42 for givenName**
  - ▪ **urn:oid:1.3.6.1.4.1.10126.1.35.3.15 for „TGacceptedTermsOfUse" (used in TextGrid)**
- ➢ **Synchronized clocks, HTTPS, etc...**

# Federation

- Federation concept: a trust infrastructure of IdPs and SPs („circle of trust")
- Minimal tasks:
  - Metadata maintenance (registration, access, signature)
  - Discovery Service operation
  - Legal issues...
- IdPs and SPs can be members of multiple federations (Federation ↔ Metadata)
- An IdP and an SP can trust each other also without a federation: just exchange metadata bilaterally
- Some SP / IdP implementations even cannot handle SAML metadata: just exchange some information that is contained in metadata

# WebSSO vs. ECP

- ➢ **Different SAML SSO Profiles:**
  - ▪ **WebSSO for Web Browser and usual Web Applications**
  - ▪ **ECP (Enhanced Client or Proxy) for other clients not capable of displaying a login page → can be used for RESTlike Web Services**
- ➢ **ECP needs Clients with special, Browser-like features**
  - ▪ **Issue HTTP GET, POST requests and follow HTTP Redirects**
  - ▪ **Process HTTP Headers**
  - ▪ **Handle Cookies**
  - ▪ **Process XML (SOAP + SAML messages themselves)**
  - ▪ **Handle HTTPS**
- ➢ **Supported by Shibboleth IdP (only Basic Auth) and SP**

# WebSSO vs. ECP



Web Browser

Rest API Client (ECP Client)

3 IdP Discovery

5 Basic AuthN

4 AuthN Red

6 SAML Resp

ECP Identity Provider 2

ECP Identity Provider 1

6 HTTP Response

1 HTTP Request

2 IdP Discovery

3,5 HTTP Redirect

4 Form AuthN

8 HTTP Response

1 HTTP Request

2 AuthN Request

7 SAML Response

ECP Service Provider

Access Layer

Basic Storage Layer

DAASI International

(c) 2017 DAASI International, DARIAH-DE, AARC

# WS-Security and SAML

➢ **Using SAML Assertions as WSS-Tokens for SOAP Web Services**

➢ **The Assertion is embedded in the SOAP Header just like another Authentication Token**

➢ **WSS SAML Token Profile defines this model**

➢ **IdP = Security Token Service (STS)**

➢ **SP issues a RequestSecurityToken (RST) message via the Client for the STS (RST is defined in WS-Trust)**

➢ **STS reply: RequestSecurityTokenResponse (RSTR)**

➢ **NOT supported by Shibboleth**

# WS-Security and SAML
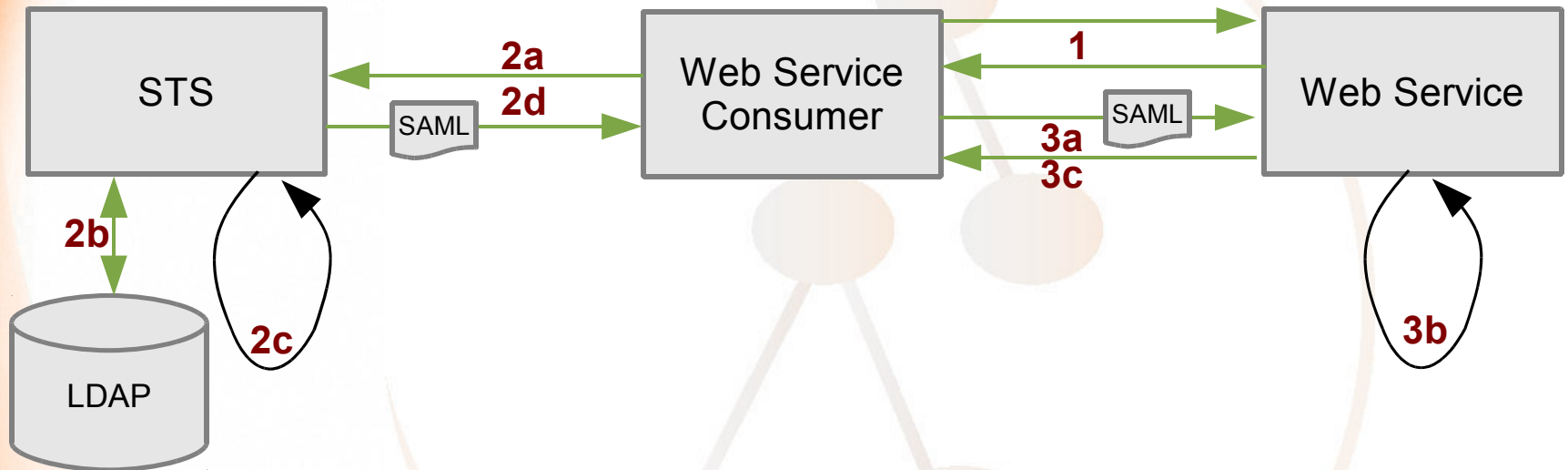
# Web Services Delegation

➢ **Delegation**
  - ▪ **1-Tier: IdP issues „token" for User U to Service A and A requests resources from Service B on behalf of U**
  - ▪ **N-Tier: Service A → Service B → Service C→ ...**

➢ **Delegation with SAML/Shibboleth alone is complex ( https://spaces.internet2.edu/display/ShibuPortal/Home )**

➢ **OAuth2.0 allows and is designed for 1-Tier delegation**

➢ **Combination of SAML infrastructure and OAuth2.0 is possible**

➢ **Most common use case: some SAML-protected Web portal application wants to access some RESTlike service in the user's name**

# Web Services Delegation



(c) 2017 DAASI International, DARIAH-DE, AARC
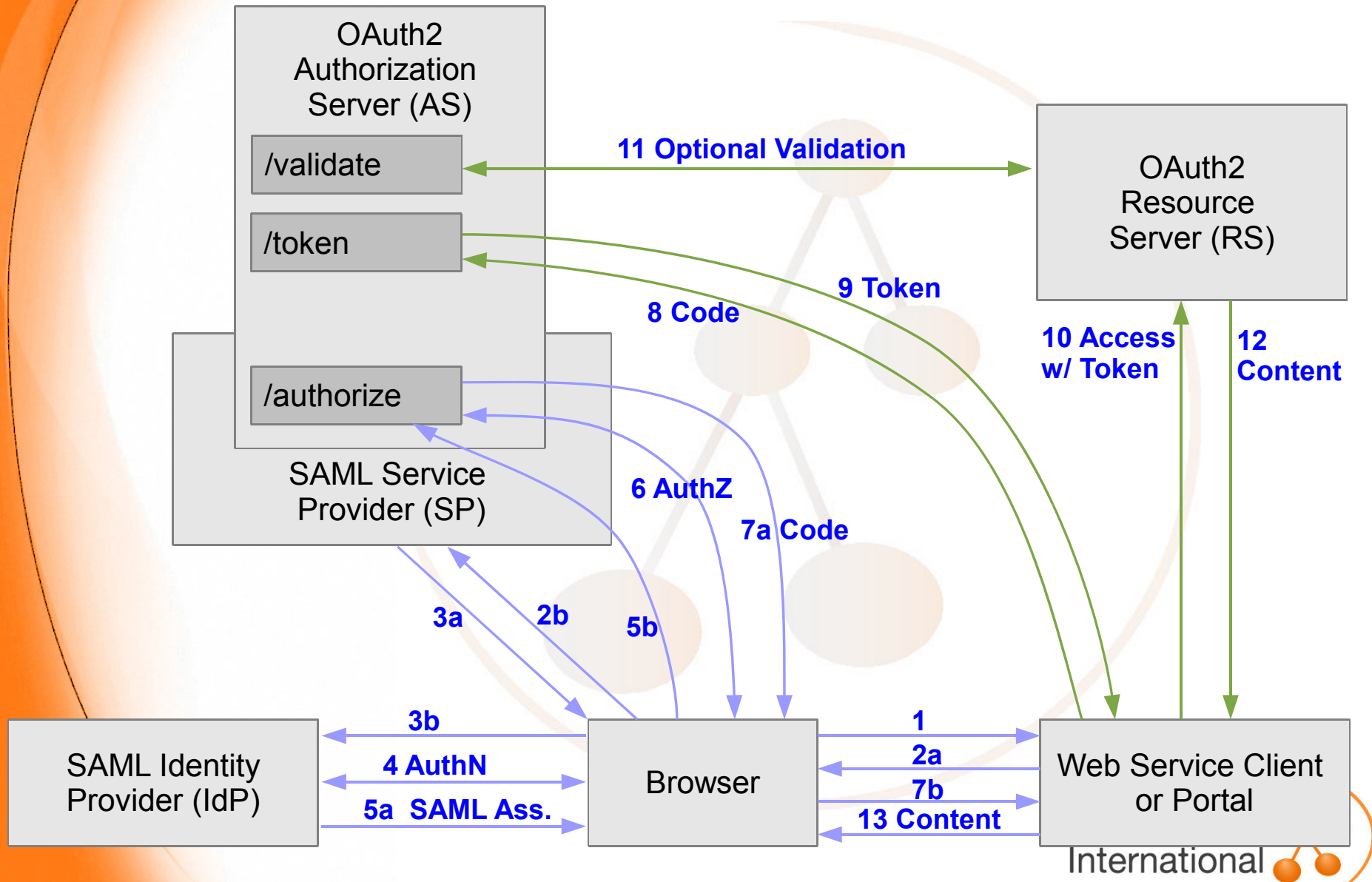
# **Shibboleth**

# Origin

- **Open-Source project, originally developed by Internet2**
- **Now managed by the Shibboleth Consortium**
- **Implementation of**
  - **SAML Identity Provider**
  - **SAML Service Provider**
  - **SAML Discovery Service (Centralized and Embedded)**
- **Origin of the word is Hebrew, see the Bible, Judges 12,6**
- **Current version 2 implements SAML2 and is compatible with SAML1**

# Shibboleth WebSSO
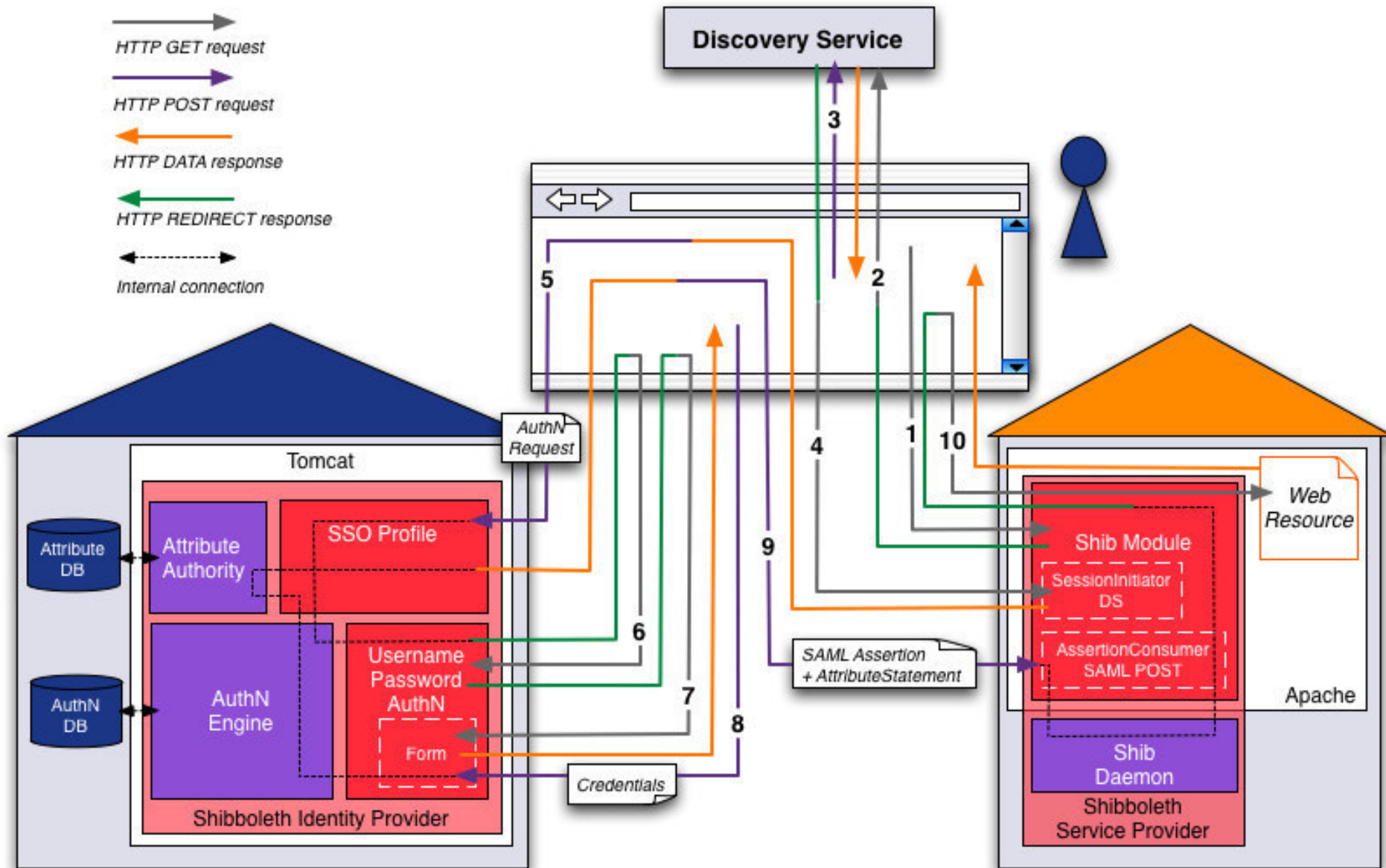
# Identity Provider
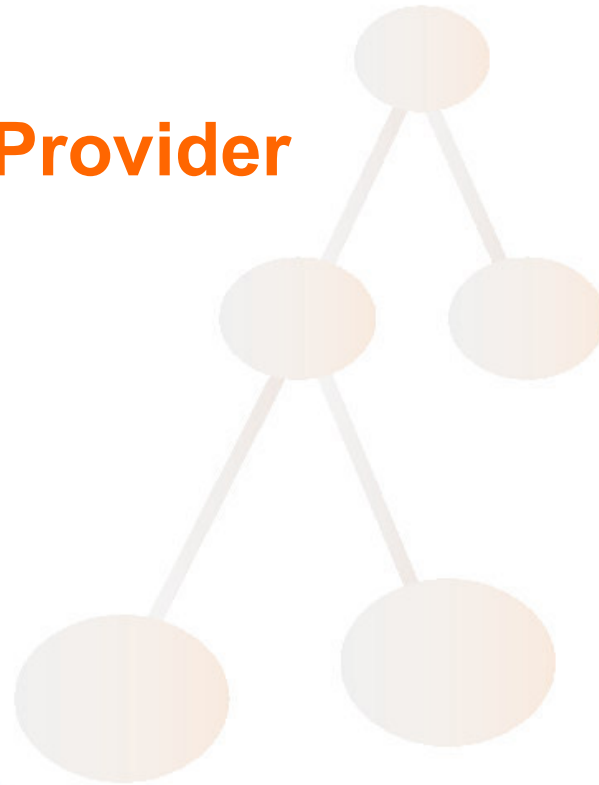
# IdP Basics

➢ **IdP provides users with the possibility to use Web applications that are protected by trusted SPs**

➢ **Unlimited number of "connected" SPs**

➢ **An Organization's IdP can be used for**

- ▪ **Organization internal Single Sign-On**
- ▪ **SSO within a federation**
- ▪ **SSO in multiple federations**

➢ **Authentification of a user is never done at the SP, but always locally in the home organization that the IdP represents → the password is only there!**

# IdP Basics (2)

➢ **After a successful authentication, the IdP sends a SAML Token / Ticket (*Assertion*) to the SP, authenticating the user**

➢ **A reference to the IdP session is saved in the user's Web browser**

➢ **Thanks to the IdP session, any SP can be issued a new Assertion (within session lifetime)**

➢ **Users will not realize following log-ins to further SPs (Single Sign-On) as they are automatically redirected to the IdP (HTTP Redirect, POST) that keeps the session**

# IdP Architecture

- **IdP is a Java Web application**
- **Installation on Windows, Linux, Unix, ...**
- **Runs in Servlet container (Tomcat, Jetty)**
- **Possibly Apache Web server as proxy**
- **Authentication and attribute resolution are separated**
- **Extensible (Spring-based configuration)**
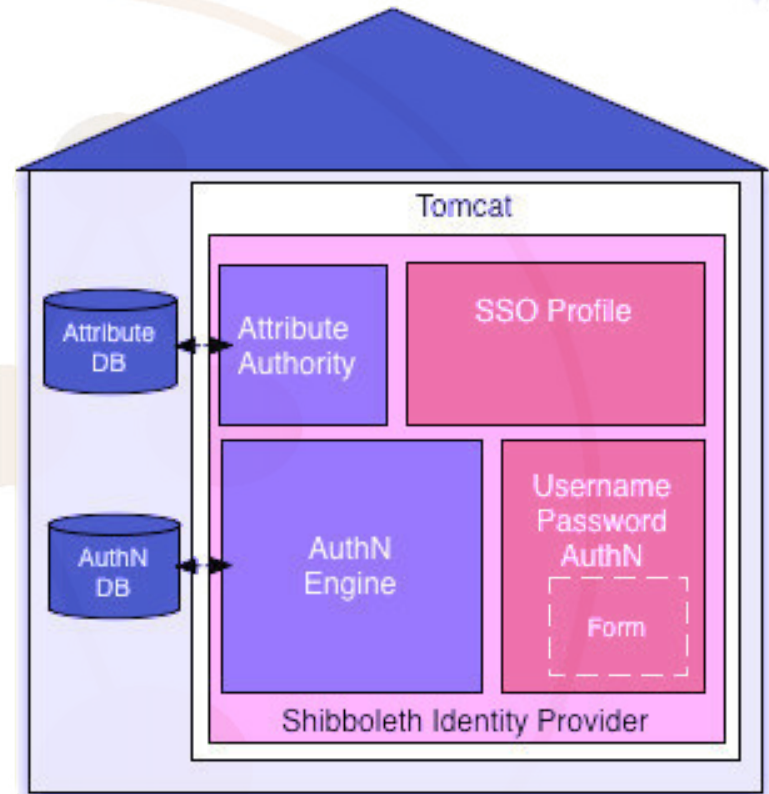
**(c) SWITCH**

# Connection to the IdM

- ➢ **Authentification: IdP can use**
  - ▪ **LDAP, AD, relational Database via JAAS (username/password form)**
  - ▪ **Kerberos domain**
  - ▪ **External SSO (CAS, Pubcookie etc)**
  - ▪ **Remote-User based via the container (Apache, Tomcat)**
- ➢ **Attribute sources: various DataConnectors**
  - ▪ **LDAP, AD, relational Database**
  - ▪ **static Attributes**
  - ▪ **Stored Ids (for pseudonyms) from relational DB**

# Example: connect LDAP via JAAS and Username/Password form

➢ **JAAS configuration**

```
edu.vt.middleware.ldap.jaas.LdapLoginModule required
    ldapUrl="ldap://localhost:389"
    baseDn="dc=dariah,dc=eu"
    tls="true"
    subtreeSearch="true"
    serviceUser="cn=manager,dc=dariah,dc=eu"
    serviceCredential="secret"
    userFilter="uid={0}";
```

➢ **Many more options here, e.g.**
  ▪ **LDAP Failover,**
  ▪ **LDAPS**
  ▪ **Authorization filters**
➢ **Other JAAS modules analogous**

# Interplay with SPs

➢ **Attribute resolver reads attributes from directories, databases, etc. and defines their format on the wire**
  - ▪ **Attributes should be based on standards: e.g. eduPerson eduPersonAffiliation, eduPersonTargetedId, eduPersonEntitlement**
  - ▪ **A particular IdP and SP can arrange bilaterally for custom attributes, additionally**

➢ **Attribute filter defines Attribute Release Policies**
  - ▪ **Shibboleth provides for fine-granular attribute filtering rules (data protection)**
  - ▪ **Complex filters possible**

# Example: Attribute Resolver with an LDAP DataConnector

```
<resolver:DataConnector id="myLDAP"
    xsi:type="dc:LDAPDirectory"
    ldapURL="ldap://localhost:389" useStartTLS="true"
    baseDN="dc=dariah,dc=eu"
    principal="cn=manager,dc=dariah,dc=eu"
    principalCredential="secret">
    <dc:FilterTemplate>
        <![CDATA[
            (uid=$requestContext.principalName)
        ]]>
    </dc:FilterTemplate>
    <dc:ReturnAttributes>
        entryDN mail uid cn sn givenname
    </dc:ReturnAttributes>
</resolver:DataConnector>
```

# Example: Attribute Definition

- ➢ **also in attribute-resolver.xml**

```
<resolver:AttributeDefinition xsi:type="ad:Simple"
        id="email"
        sourceAttributeID="mail">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:mail" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:0.9.2342.19200300.100.1.3"
        friendlyName="mail" />
</resolver:AttributeDefinition>
```

# Example: Custom Attribute Definition

```xml
<resolver:AttributeDefinition xsi:type="ad:Mapped"
        id="fooBarRole"
        sourceAttributeID="entryDN">
    <resolver:Dependency ref="myLDAP" />
    <!-- no SAML1 Attribute Encoder necessary, this is a
        SAML2-only deployment -->
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
            name="urn:oid:1.2.3.4.5.6.7.8.9.1"
            friendlyName="fooBarRole" />
    <ad:ValueMap>
      <ad:ReturnValue>$1</ad:ReturnValue>
      <ad:SourceValue>[^,]+,ou=([^,]+),.*</ad:SourceValue>
      <!-- SourceValue contains user type in DN -->
    </ad:ValueMap>
</resolver:AttributeDefinition>
```

DAASI International

# Attribut-Filter per SP

➢ **Specify which attributes are sent to which SP**
➢ **Data sparseness**
➢ **Configure access rules centrally**
➢ **Allows for uniform SP configurations**
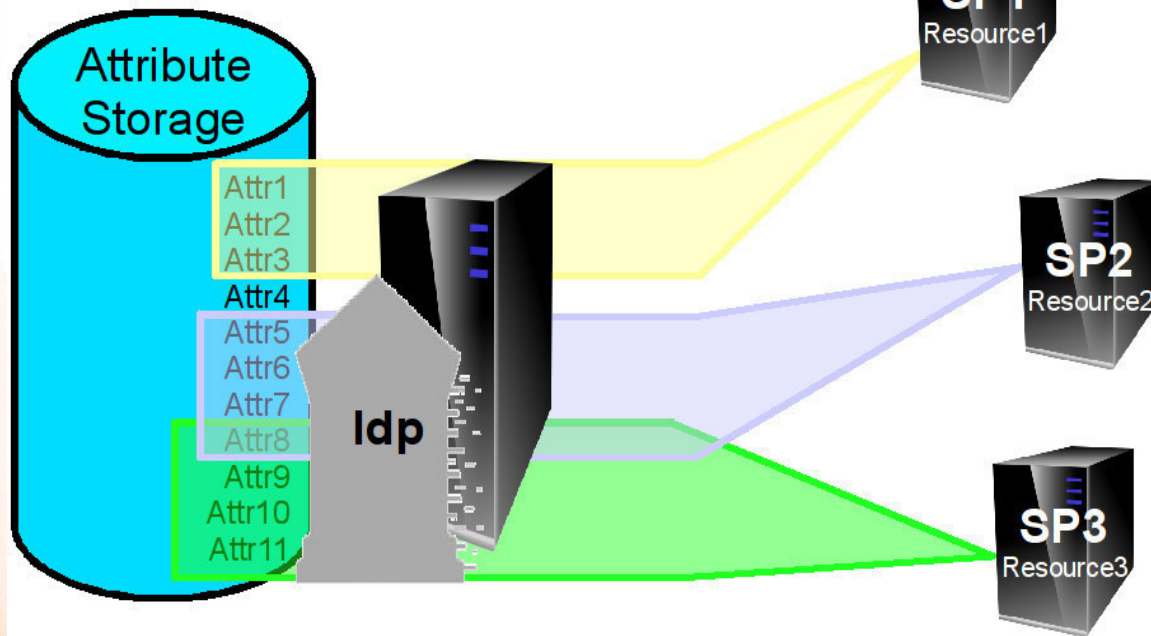
# Example: Attribute Filter

```xml
<afp:AttributeFilterPolicy>
    <afp:PolicyRequirementRule
        xsi:type="basic:AttributeRequesterString"
        value="https://sp1.example.eu/shibboleth" />

    <afp:AttributeRule attributeID="givenName">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>

    <AttributeRule attributeID="fooBarRole">
        <PermitValueRule xsi:type="basic:OR">
            <basic:Rule
                xsi:type="basic:AttributeValueString"
                value="Researchers"/>
            <basic:Rule
                xsi:type="basic:AttributeValueString"
                value="Students"/>
        </PermitValueRule>
    </AttributeRule>
</afp:AttributeFilterPolicy>
```

# IdP Deployment Options
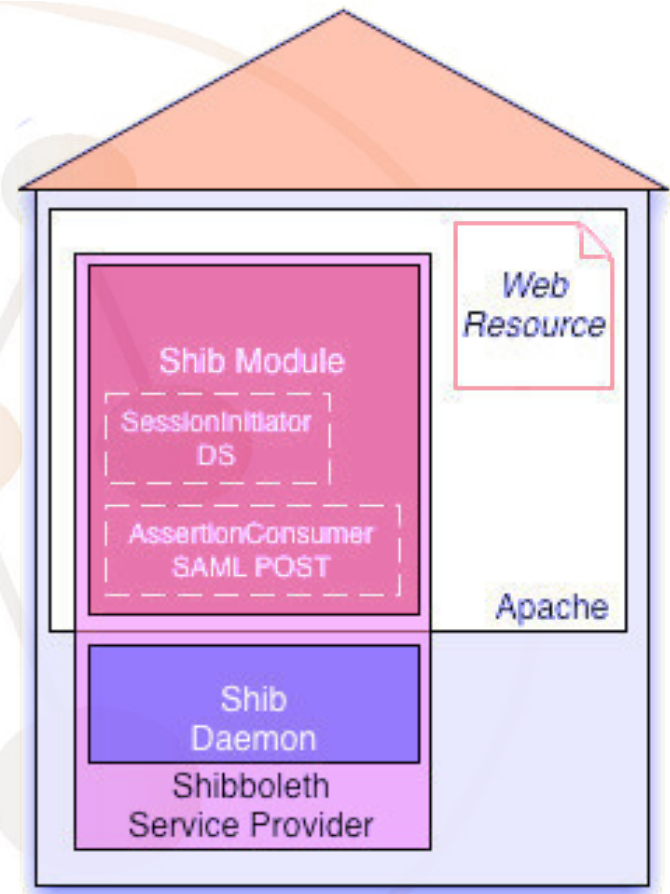
- Standalone Servlet Container or proxied by Apache Web Server?
- Jetty? Which version?
- Tomcat? Which version?
- Which Java Version?
- Clustering?
  - Do not cluster: active and standby instance (needs Load Balancer)
  - Parallel IdPs (stateless Clustering, with a LB and long cookie-based stickyness for SSO), no Artifact and SLO
  - Clustering with Terracotta (using DNS Round Robin or a LB)
  - Clustering with memcached (with LB, short stickyness)

# Service Provider

# Service Provider

- **Supports Apache, FastCGI, Sun/iPlanet and IIS**
- **Application is protected by a Web server module**
- **Status (sessions, etc) is being kept by the Shibboleth Daemon shibd**
- **Binaries for Windows, RPM-based Linuxes, OS X, Sources for other UNIXes**

Web Resource

Shib Module

SessionInitiator
DS

AssertionConsumer
SAML POST

Apache

Shib Daemon

Shibboleth Service Provider

**(c) SWITCH**

**DAASI International**

# SP Configuration files

- ➢ **Apache /etc/httpd/conf/httpd.conf, or in extra files (example for CentOS)**
  - ▪ **conf.d/<servername>.conf**
  - ▪ **conf.d/shib.conf, refernced therein mod_shib_22.so**
- ➢ **Shibboleth itself under /etc/shibboleth/**
  - ▪ **shibboleth2.xml**
  - ▪ **attribute-policy.xml**
  - ▪ **attribute-map.xml**
  - ▪ **xxx-metadata.xml**
  - ▪ **certificates**
- ➢ **Start skript /etc/init.d/shibd**

# Configure vhost

```
...
Listen 443
<VirtualHost _default_:443>

    ServerName          sp123.example.edu
    UseCanonicalName  On

    SSLEngine on
    SSLCipherSuite ALL
    SSLOptions +StdEnvVars +ExportCertData

    SSLCertificateFile /etc/pki/tls/certs/sp.pem
    SSLCertificateKeyFile /etc/pki/tls/private/sp.key
    SSLCertificateChainFile /etc/pki/tls/certs/chain.pem
    ...
</VirtualHost>
```

DAASI International

# shibboleth2.xml

- ➤ **Request Map with XML Access control (only option under IIS)**
- ➤ **Applications vs. ApplicationOverride**
  - ▪ **SP's entityID**
  - ▪ **REMOTE-USER preference sequence**
  - ▪ **Session Information (Timeouts, Protocol Handler, Service Locations und Bindings, Session Initiators → federation DS or default IdP, Logout Initiator)**
- ➤ **Credentials**
- ➤ **Attribute Map and Policy**
- ➤ **Metadata Provider (local files or remote URL)**
- ➤ **See https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPShibbolethXML**

**DAASI**
International

# Filter Attributes in the SP

- attribute-policy.xml
- s. **https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeFilter**
- Examples:

```
<afp:AttributeRule attributeID="sn">
    <afp:PermitValueRule
    xsi:type="AttributeIssuerString"
    value="https://testidp.example.org/idp/shib
    boleth"/>
</afp:AttributeRule>
<afp:AttributeRule attributeID="entitlement">
    <afp:PermitValueRule
      xsi:type="AttributeValueString"
    value="urn:mace:dir:entitlement:common-
      lib-terms" />
</afp:AttributeRule>
```

# Map Attributes

- attribute-map.xml
- Environment variable `REMOTE_USER` receives special treatment in shibboleth2.xml and not here
- Mapping rules examples:

```
<Attribute name="urn:mace:dir:attribute-
    def:eduPersonScopedAffiliation"
    id="affiliation">
        <AttributeDecoder caseSensitive="false"
            xsi:type="ScopedAttributeDecoder"/>
</Attribute>

<Attribute name="urn:oid:2.5.4.20"
    id="telephoneNumber" aliases="telnr tel"/>
```

# SimpleAggregation

- ➤ **Can request attributes from another IdP than the one the user actually logged in to**
- ➤ **Aggregates attributes through SAML 2.0 attribute queries (via SOAP call to the AA) using an identifier derived from the attributes obtained**

```
<!-- use eduPersonPrincipalName, ask for epEntitlement -->
<AttributeResolver  type="SimpleAggregation"
                    attributeId="eppn"
                    format="urn:oid:...1.1.6">
    <Entity>https://ieee.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="...uri"
        FriendlyName="eduPersonEntitlement"/>
</AttributeResolver>
```

DAASI International

# Attribute Checker

➢ **Shibboleth SP >= version 2.5**

➢ **Validates a user's session against a list of required attributes (and optionally values) and**

- **Either returns the user to complete the login process**
- **Or displays an error template (session data available)**

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

➢ **Designed to complement the sessionHook:**

- **Location where user is sent after session creation**
- **HTTP Redirect, params `target` and `return`**
- **Hook must either redirect back to SP or lead elsewhere**

# SP Deployment

➢ **Create server certificates**

➢ **Install the SP on the server where the application is**

➢ **Operating System Choices:**

- ▪ **RPM based: download repository file from**
  **http://download.opensuse.org/repositories/security:/shibboleth/**

- ▪ **Debian based/Ubuntu: use shiny new SWITCH repository for SP v2.5, see**
  **https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.5/sp/deployment/**

- ▪ **Mac, Windows, Solaris: see https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSP{Mac|Windows|Solaris}Install**

# SP (2)

- ➤ **Configure Apache**
  - ▪ **Vhost for the application**
  - ▪ **Apache access rules**
- ➤ **Configure the SP**
  - ▪ **shibboleth2.xml**
  - ▪ **attribute-map.xml**
  - ▪ **(attribute-policy.xml)**
  - ▪ **IdP Metadata**
  - ▪ **(Certificates)**
- ➤ **Protect something (default: <DocumentRoot>/secure/)**
  - ▪ **Some Test Application: e.g. phpinfo()**
  - ▪ **Your Web application**

# Troubleshooting

- ➢ **Log files (CentOS, again :-)**
  - ▪ **/var/log/shibboleth/shibd.log**
  - ▪ **/var/log/shibboleth/transaction.log (z.B. level INFO: IdP, IdP-NameIdentifier, IP address, time, SP sessionID, name of accepted attributes (no value)**
  - ▪ **/var/log/httpd/ssl_access_log**
  - ▪ **/var/log/httpd/ssl_error_log**
- ➢ **Control attributes supplied by the SP using a phpinfo() under /secure/index.php, or**
- ➢ **`https://sp.example.org/Shibboleth.sso/Session`**

# IdP and SPs
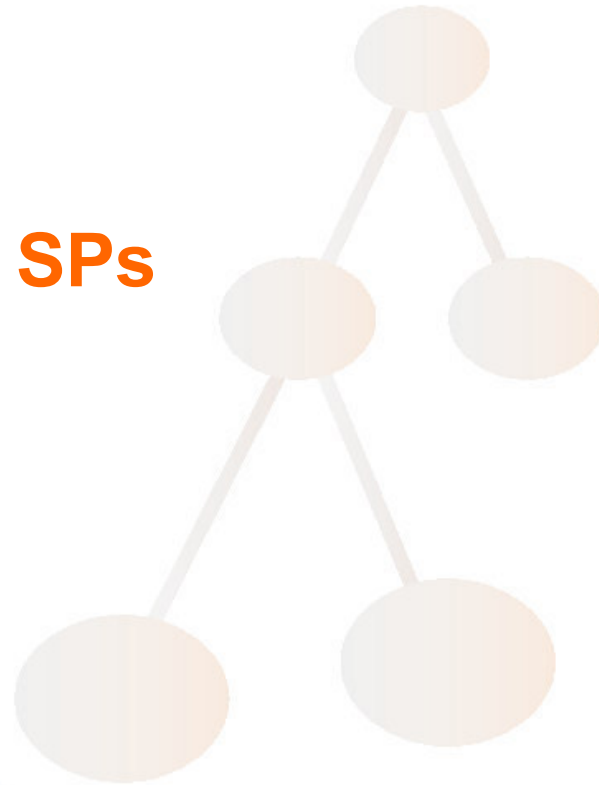
# Metadata

- Metadata must be exchanged: IdP needs SP's, and SP needs IdP's metadata
- Shibboleth SP and IdP have an endpoint for metadata retrieval
- Handler addresses:
    - https://exampleSP.org/Shibboleth.sso/Metadata (always generated with all important info)
    - https://exampleIdP.org/idp/profile/Metadata/SAML (IdP maintainer must keep them current)
- Usually a federation amends the generated information and manages metadata distribution

# Attribute Exchange

- ➤ **Compatibility in a federation: IdPs and SPs need to**
  - ▪ **speak the same language (attribute definitions)**
  - ▪ **and must match what they process (attribute exchange policies)**
- ➤ **Thus the following must match**
  - ▪ **attribute-resolver.xml and attribute-map.xml (SP)**
  - ▪ **attribute-filter.xml (IdP) attribute-policy.xml (SP)**
- ➤ **Ideal world!**
  - ▪ **Only in closed environments possible (but there are lots of such)**
  - ▪ **Many parties involved in a federation (there are lots), so it is hard to keep language and policies in synch**
  - ▪ **Many more parties involved with interfederations (eduGain), so even harder**

# DARIAH Java SP
## (Tobias Gradl)

# Shibbolizing Web Applications

# Recommendations for New Web Applications

➢ **Ideally read-only access to user attributes, then these attributes can be provided by environment variables**

➢ **Use standard the environment variable $REMOTE_USER**

- ▪ **Also supported by Tomcat and Apache**
- ▪ **Can use authentication modules interchangeably**

➢ **Use a service account if there needs to be write access to a database (there's not password with SSO)**

➢ **If the application has public and closed parts: use different URL paths**

➢ **Even easier: protect the whole application with Shibboleth**

# Shibbolizing Existing Applications

➢ **Points to consider (not a recipe)**
- **What is the current authentication method? Apache, Tomcat, LDAP, own mechanism, ...**
- **What is the current resource protection method? Apache, Tomcat, own mechanism, ...**
- **Does the application have an own session management? How does it work?**
- **How does the application's access control work?**
- **Any authorization rules for the application – or for those parts that must be protected specifically?**
- **User data: From where, What for?**
- **Can Shibboleth SP provide these data as attributes?**
- **Can IdPs provide them?**

**(inspired by Bernd Oberknapp, UB Freiburg)**

**DAASI International**

# Shibbolizing an Existing Application

➢ **Single Sign-On: the art of removing control of the user password from an application**

➢ **Only Web applications**

➢ **No authN against a local (at the SP!) data source**

- ▪ **Application only sees attributes (read only)**
- ▪ **Any user password remains at the IdP**
- ▪ **A privileged system account could be used for local read and write data**

➢ ***Protect* the Login Path with Shibboleth, and allow for Shibboleth *control* of the rest (to see the attributes)**

➢ **Web Server *can* (not required!) allow for access control to the application based on SP attributes**

# Authentification

➢ **Existing application assumes AuthN by Web server or servlet container?**

- ▪ **Easy to shibbolize**
- ▪ **SP Web server module (mod_shib) populates environment / CGI variables**
- ▪ **Just exchange AuthN method (e.g. Basic Auth, LDAP) in Apache configuration with *shibboleth***

➢ **SP sets special variable REMOTE_USER via a fixed preference list, e.g. „uid eppn persistent-id targeted-id"**

# Authentification

➢ **More difficult if application**
- ▪ **Presents its own login screen and/or**
- ▪ **Assumes to be given login / password**

➢ **Usually need a new module that**
- ▪ **Redirects to the SP Login Handler**
- ▪ **Saves attributes given by the SP into the application session**

➢ **Make that module**
- ▪ **mandatory**
- ▪ **or an alternative, but**
- ▪ **„Dual Log-in" (login/password plus link to DS on the same page) is not recommended due to phishing awareness**

# Access Control

- ➤ **Access control by the Web Server, can be configured in**
  - ▪ **shibboleth2.xml aka *XML access control* (/RequestMap/Host/Path/...)**
  - ▪ **Via Apache directives in httpd.conf or embedded files or via .htaccess files**
  - ▪ **To avoid confusion, should not mix these two mechanisms**
  - ▪ **see https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPProtectContent**
  - ▪ **or https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPContentSettings**
- ➤ **Or application access control (often combined with Lazy Session)**

# Access Control Pros and Cons

| | 1.a httpd.conf | 1.b .htaccess | 2. XML AccessControl | 3. Application Access Control |
|---|---|---|---|---|
| **+** | ▪ Easy to configure<br>▪ Can also protect locations or virtual files<br>▪ Regex Support | ▪ Dynamic<br>▪ Easy to configure | ▪ Platform independent<br>▪ Powerful boolean rules<br>▪ Regex Support<br>▪ Dynamic | ▪ Very flexible and powerful with arbitrarily complex rules<br>▪ Regex Support |
| **-** | ▪ Only works for Apache<br>▪ Not dynamic<br>▪ Not very flexible rules | ▪ Only works for Apache<br>▪ Only works with "real" files and directories | ▪ XML editing<br>▪ Configuration error can prevent SP from restarting | ▪ You have to build it yourself<br>▪ You have to maintain it yourself |

**(c) SWITCH**

# Examples: Apache vs. XML

➢ **Apache Access control in httpd.conf:**

```
<Location /secure>
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    Require entitlement common-lib-terms
</Location>
```

➢ **XML-based in shibboleth2.xml:**

```
<Path name="secure" authType="shibboleth"
    requireSession="true">
    <AccessControl>
        <Rule require="affiliation">
            member@example.org
        </Rule>
    </AccessControl>
</Path>
```

# Application Access Control

➢ **SP only provides for attributes from the IdP**

➢ **URL paths must be either under Shibboleth *protection or control***

➢ **Attributes can be used freely by the application for access control, e.g. in a PHP script:**

```
if ($_SERVER['affiliation'] == 'staff')
    { grantAccess(); }
```

➢ **E.g. in a Perl CGI script:**

```
if ($ENV{'affiliation'} eq 'staff')
    { grant_access() }
```

➢ **E.g. in a Java Servlet in Tomcat proxied by Apache**

```
affiliation = (String)
    request.getAttribute("affiliation");
if (affiliation.equals("staff"))
    grantAccess();
```

(c) 2017 DAASI International, DARIAH-DE, AARC

# Lazy Session

➢ **Lazy Session: request Log-in when application needs it**
➢ **Usually used with application access control**
➢ **Shibboleth must *control* (not *protect*) path:**

```
<Location /lazy>
    AuthType shibboleth
    ShibRequestSetting requireSession 0
    Require shibboleth
</Location>
```

➢ **Application requests AuthN by redirecting to:**

```
https://sp.example.org/Shibboleth.sso/Login?
    target=https://sp.example.org/cgi-bin/
    application.php&
    entityID=https://idp.example.org/
```

# Lazy Session:
# alternative Login Mechanism

➤ **This variant does not call the LoginHandler directly**

➤ **Shibboleth *protect* the URL that usually does Log-in for the application and call it**

```
<Location /login>
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    require valid-user
</Location>
```

➤ **At this location, exchange existing password form with**
  ▪ **reading the user attributes from the SP**
  ▪ **saving the login information in the session**

# Example from UB Freiburg

➢ **Shibbolize a Nagios Server using Basic Auth and local Apache accounts**

➢ **(1) Renamed Apache accounts (using the uid from IdP)**

➢ **(2) Defined an Entitlement in the IDM for those users that are allowed to access Nagios (alternative: an LDAP group)**

➢ **(3) Configured IdP such that uid and Entitlement are released to the SP on the Nagios server**

➢ **(4) Configured the SP to use the IdP, accept uid, and provide it as REMOTE_USER**

➢ **(5) Include the SP's metadata into the IdP's local metadata**

**DAASI International**

# Example from UB Freiburg

➢ **(6) Change Apache config from LDAP to shibboleth:**

```
AuthType Shibboleth
    ShibRequestSetting requireSession 1
    ShibRequireAll On
    Require user ~ ^.+$
    Require entitlement https://mylogin.uni-
                        freiburg.de/entitle
                        ment/ub/nagios/admin
```

➢ **What the particular user is allowed to see (authZ) remains in the Nagios configuration**

➢ **Accordingly, Nagios configuration must be touched if such user leaves the university**

# Advanced Techniques

- ➢ **isPassive at the Service Provider**
  - ▪ **Only for SAML2 SPs**
  - ▪ **Allows for Log-in to the application without any user interaction**
  - ▪ **Application must be protected with Lazy Session**
- ➢ **IdP LoginHandler must support it**
  - ▪ **UsernamePassword Handler does**
  - ▪ **RemoteUser Handler does not**
- ➢ **Check via redirect to the IdP, without the user noticing**
  - ▪ **If there's no IdP session, does not present IdP login screen but come back, sending to some default page**
  - ▪ **If there's a session, user comes back authenticated**

# Advanced Techniques

- ➢ **forceAuthn mechanism**
  - ▪ **SAML2**
  - ▪ **Request renewed authN for critical operations at an application**
  - ▪ **Precedes over SSO**
  - ▪ **Must be supported by the IdP (Shibboleth IdP does)**

DAASI
International

# SP Deployment Options

➢ **Full Shibboleth protections or Lazy Session?**

➢ **Access control by container or by application?**

➢ **Personalization via**
- ▪ **pseudonyms**
- ▪ **REMOTE-USER**
- ▪ **Further user attributes**

➢ **One IdP, a few IdPs, or an embedded or central Discovery Service?**

➢ **Which federation(s)?**

➢ **One logical SP (~vhost) or many?**

➢ **Further authN methods besides Shibboleth?**

**DAASI International**

# CLARIN and Shibboleth: Integration into the LAT software stack (Willem Elbers)

# JEE Strategies
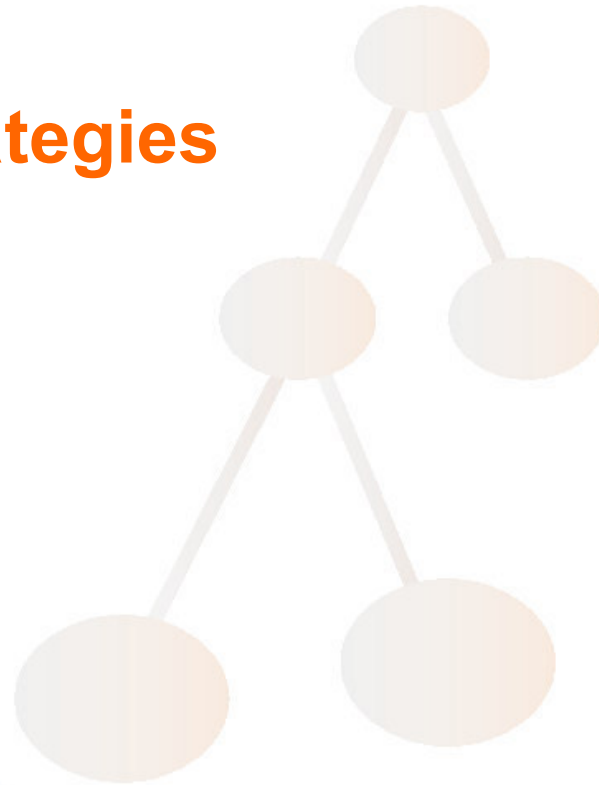
# Java Applications

➢ **Shibboleth SP is a Web server module**

➢ **But J2EE applications run in a Servlet Container (Tomcat, Jetty, ...) or Application Server (JBoss, Geronimo, ...)**

➢ **Solution: Web Server Proxy (e.g. mod_proxy_ajp)**

➢ **Other Options**

▪ **DARIAH Java SP!!!**

▪ **Spring Security Shibboleth Native SP plugin for Grails/Groovy/Java Web applications**

▪ **Non-Shibboleth SAML SP products, e.g. OpenAM, ESOE, OIOSAML.java, (s. http://saml.xml.org/wiki/saml-open-source-implementations)**

# Java Applications (2)

- ➢ **Role concept: the container...**
  - ▪ **sets the User Principal (REMOTE_USER)**
  - ▪ **Assigns principals to Roles, declaratively**
- ➢ **Container Managed Security (web.xml)**
  - ▪ **Translate <security-constraint>s and <web-resource-collection>s into Apache <Location>s**
  - ▪ **Omit <login-config>s und <security-config>s**
  - ▪ **Not recommended for complex roles**
- ➢ **Application Security (servlet filter)**
  - ▪ **request.getRemoteUser() → can be used directly**
  - ▪ **request.isUserInRole(role) → proxy with a HttpServletWrapper**
  - ▪ **Lazy Session: access control per Servlet**

# Application Managed Security: web.xml

```xml
<web-app>
  <display-name>Attribute2Role</display-name>
  <filter>
   <filter-name>Attribute2RoleFilter</filter-name>
   <filter-class>de.sc.Attribute2RoleFilter</filter-class>
  </filter>

  <servlet>
    <servlet-name>ListParameters</servlet-name>
    <servlet-class>de.sc.ListParameters</servlet-class>
  </servlet>

  <servlet-mapping>
    <servlet-name>ListParameters</servlet-name>
    <url-pattern>/ListParameters</url-pattern>
  </servlet-mapping>

  <filter-mapping>
    <filter-name>Attribute2RoleFilter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
</web-app>
```

# Application Managed Security: Filter

```java
public class Attribute2RoleFilter implements Filter {

    @Override
    public void doFilter(  ServletRequest request,
                           ServletResponse response,
                           FilterChain chain) {
        ServletRequest req = new HttpRequestWrapper(
                        (HttpServletRequest) request);
        chain.doFilter(req, response);
    }
}
```

DAASI International

# Application Managed Security: Wrapper

```java
public class HttpRequestWrapper extends
                                HttpServletRequestWrapper {
    private String surname;
    private boolean loser;

    public HttpRequestWrapper(HttpServletRequest request) {
        super(request);
        surname = (String) request.getAttribute("sn");
        String attr = (String) request.getAttribute("loser");
        if ((attr != null) && attr.equals("TRUE"))
                loser = true;
        else   loser = false;
    }
    @Override
    public boolean isUserInRole(String arg0) {
        if (arg0.equals("loser"))
            return loser;
        return false;
    }
    public String getSurname() {
        return surname;
    }
}
```

# Application Managed Security: Servlet

```java
public class ListParameters extends HttpServlet {

    protected void doGet(...)  // call doIt
    protected void doPost(...) // call doIt

    void doIt(HttpServletRequest request,
              HttpServletResponse response) {
    out.println("<html>");

    //...

    out.println("Surname (sn): "+ request.getAttribute("sn");

    if (request.isUserInRole("loser")) out.println("Loser!");
        else out.println("Winner!");

    if (request instanceof HttpRequestWrapper) {
        String surname = ((HttpRequestWrapper) request)
                        .getSurname();
        out.println("cached value): " + surname);
        }
    }
}
```

# Generic Interface
for Applications

# Interface

➢ **In order to switch to SSO easily, an application should request the following methods:**

- ▪ `Boolean is_authenticated ()`
- ▪ `void authenticate ( URL target, String entityID )`
  - • **or alternatively:** `URL get_authentication_URL ( URL target, String entityID )`
- ▪ `void logout ( URL return )`
  - • **or alt.** `URL get_logout_URL ( URL return )`
- ▪ `String get_user_id ()`
- ▪ `Array [String] get_attribute ( String attribute_name )`
- ▪ `Array [ Array [String] ] get_attributes ()`

➢ **Other SSO frameworks have a similar API, e.g. CAS, OpenID etc.**

# Example PHP class
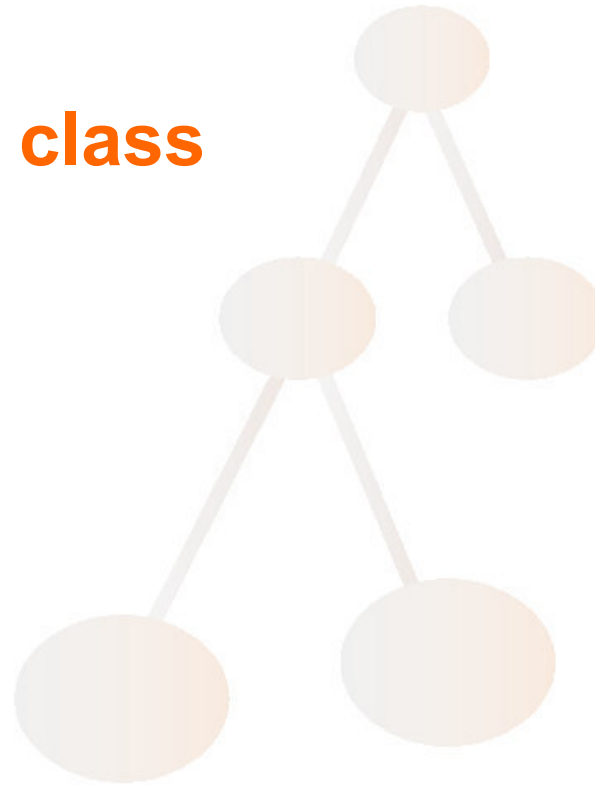
# Interface

```
interface INTERFACE_AUTH
{
  public function is_authenticated ();
  public function authenticate (
      $target_URL, $idp_entity_id );
  public function get_authentication_URL (
      $target_URL, $idp_entity_id );
  public function logout ( $return_URL );
  public function get_logout_URL(
      $return_URL ) ;
  public function get_user_id ();
  public function get_attribute ( $name );
  public function get_attributes ();
}
```

# Initialization

```
class SHIB_AUTH implements INTERFACE_AUTH
{
  private $default_shib_login_handler =
      "/Shibboleth.sso/Login";

  private $default_shib_slo_handler =
      "/Shibboleth.sso/Logout";

  private $default_shib_attributes =
      array ( "sn",
              "givenName",
              "cn",
              "mail",
              "eppn" );
```

# Login Status

```
public function is_authenticated ()
  {
    if (isset ( $_SERVER['Shib-Session-ID']))
      {
 return TRUE;
      }
    else
      {
 return FALSE;
      }
}
```

DAASI
International

# Login

```php
public function authenticate ( $target_URL = NULL,
                               $idp_entity_id = NULL )
  {
    header( 'refresh:0;url=' . $this->get_authentica-
            tion_URL ( $target_URL, $idp_entity_id) );
    flush();
    exit;
  }


public function get_authentication_URL (
            $target_URL = NULL, $idp_entity_id = NULL )
  {
    return $this->shib_login_handler .
      ( $target_URL == NULL ? '' : '?target=' .
$target_URL ) .
      ( $idp_entity_id == NULL ? '' : '&entityID=' .
$idp_entity_id );
  }
```

# Logout

```php
public function logout ( $return_URL )
  {
    header( 'refresh:0;url=' .
        $this->get_logout_URL ( $return_URL) );
    flush();
    exit;
  }

public function get_logout_URL ( $return_URL )
  {
    return $this->shib_slo_handler .
      ( $return_URL == NULL ? '' : '?return=' .
$return_URL );
  }
```

# Attributes

```php
public function get_user_id () {
    return $_SERVER['REMOTE_USER'];
}

public function get_attribute ( $name )
  {
    return explode ( ';', $_SERVER[$name] );
  }

public function get_attributes ()
  {
    $result = array();
    foreach ($this->shib_attributes as $a)
      {
      $result[$a] = $this->get_attribute ( $a );
      }
    return $result;
  }
```

# Use the Class

```
$myUrl = "https://example.org/index.php
include_once ("class.shib_auth.php");
$shibsession = new SHIB_AUTH("shib_conf.php");

if ( isset( $_POST['doLogout']))
  {
    $shibsession->logout( $myUrl . "?
LogoutHint" );
  }
elseif ( isset( $_POST['doLogin']))
  {
    $shibsession->authenticate( $myUrl );
  }
```

DAASI International

# Use the Class

```
elseif ($shibsession->is_authenticated())
   {
   // echo „valid session exists"
   // dump user ID and attributes
   // echo form with logout button
   //      using hidden doLogout field
   }
else
   {
   // give a SSO-logout hint if after logout
   // echo „valid session does not exist"
   // echo form with login button
   //      using hidden doLogin field
   }
```

**DAASI**
International

# Integration Strategies for IdP Discovery (Peter Schober)

# User Experience

➢ **Some SPs (e.g publishers) do not need personal data, a pseudonym suffices for personalization**

➢ **However, many SPs need personal data (e.g. in Research Education) to operate correctly**

➢ **Usually, a federation provides for common metadata, but does not rule attribute release**

➢ **Attribute release is subject to legal restrictions, i.e. privacy and data protection**

➢ **One solution: be liberal in releasing attributes, but let the user decide → IdP Extension *uApprove***

➢ **Another solution: make bilateral arrangements. This influences IdP choice for a service...**

# User Experience

- ➢ **Various possible IdP Discovery strategies for an SP**
- ➢ **A: Central DS of the federation**
  - ▪ **Limited to IdPs in one federation**
- ➢ **B: Embedded DS, filled from that SP's Metadata**
  - ▪ **All possible IdPs**
- ➢ **C: Embedded DS with IdP whitelist**
  - ▪ **Only a set of specific IdPs available**
- ➢ **From a user experience point of view, A and B can lead to unwanted results:**
  - ▪ **User chooses home IdP and logs in successfully**
  - ▪ **However, that IdP might not „know" the SP**
  - ▪ **Thus no required attributes released**
  - ▪ **Thus authorization error**

# User Experience

➢ **Approaches A + B show all IdPs**

- ▪ **Need special error treatment in the application**
- ▪ **However, this is the chance to change something:**
  - • **Display IdP name and logo,**
  - • **Tell the concrete reason: which attribute is missing**
  - • **Display IdP contact details to request for attribute exchange with this SP**
- ▪ **→ User can ask at the right place, i.e. at the IdP**

➢ **Approach C shows only 'known good' IdPs**

- ▪ **IdP list is harder to maintain**
- ▪ **Less disappointing for users**
- ▪ **But: If „my" IdP is not in the list, there's no easy way for me to request this (as the SP is the wrong address)**

**DAASI International**

# User Experience

- ➤ **New construct: Code of Conduct (CoC)**
  - ■ **SPs assert that they adhere to privacy protection**
  - ■ **SPs describe what personal data they process**
- ➤ **Technical implementation: SAML entity attributes**
  - ■ **SAML metadata extension**
  - ■ **http://www.geant.net/uri/dataprotection-code-of-conduct/v1**
  - ■ **Give PrivacyStatementURL**
  - ■ **List required and optional RequestedAttributes**
- ➤ **IdPs can base attribute release policy upon these entity attributes → bilateral arrangements are not required anymore, IdP maintenance is easier**

# DARIAH Authorization Framework

# Authorization

- Many frameworks and standards exist for Authentication (= logging users in): Basic AuthN, LDAP, SAML, X.509, ...
- Only few standards for Authorization (=granting access to some resource): XACML, RBAC and ...?
- Two possible ways to do the actual authorization decision:
    - Every service / application using own set of rules
    - Centrally managed service containing access rules and all services must ask this service for access decision
- Proposed a mixture of both possibilities
    - Basic authorization is stored centrally (access groups in DARIAH LDAP
    - However, it is upon the service to honor these attributes and to authorize the user upon their presence and/or content and other attributes

# Motivation

- ➢ **Challenges:**
  - ▪ **CoC has not arrived fully in today's federations yet**
  - ▪ **DARIAH SPs need some personal data: mail, surname, givenname, organization, eduPersonPrincipalName**
  - ▪ **Users' Home („Campus") IdPs do not provide these**
  - ▪ **Service Authorization: DARIAH central LDAP directory maintains list of user groups that regulate access to e.g. the DARIAH Wiki**
  - ▪ **Aim: also allow services protected by SAML SPs to base their Authorization decisions upon such group membership**
- ➢ **Developed AAI concept satisfying these issues**
- ➢ **We're not the first ones: see http://www.switch.ch/aai/downloads/20090908-JRA3-SAML-VO-Platform.pdf**

**DAASI International**

# Introducing DARIAH SP Blueprint

➢ **„Blueprint": solution for each SP in the DARIAH AAI that allows for authentication by Campus IdPs**

➢ **Basic idea:**

- ▪ **User tries to access DARIAH SP**
- ▪ **Authentication at Campus IdP (front channel)**
- ▪ **SAML Attribute Request at the DARIAH IdP (back channel without user interaction), providing:**
  - • **Attributes not given by Campus IdP**
  - • **Group memberships**

➢ **There is one „registration" page upon first time access**

- ▪ **Protected by an SP**
- ▪ **Complementing required attributes**
- ▪ **Approval of DARIAH Terms of Use**

# DARIAH AAI Infrastructure

DARIAH LDAP
- ou=people
- ou=shibpeople
- ou=groups

DARIAH IdP

Registration SP

Campus IdP

Attributes + Entitlements

ePPN

Permissions

write Attributes

Redirect2

Aggr. Attr. Resolver

Resource SP

AttributeChecker

Redirect1

Admin Portal

DARIAH Resource
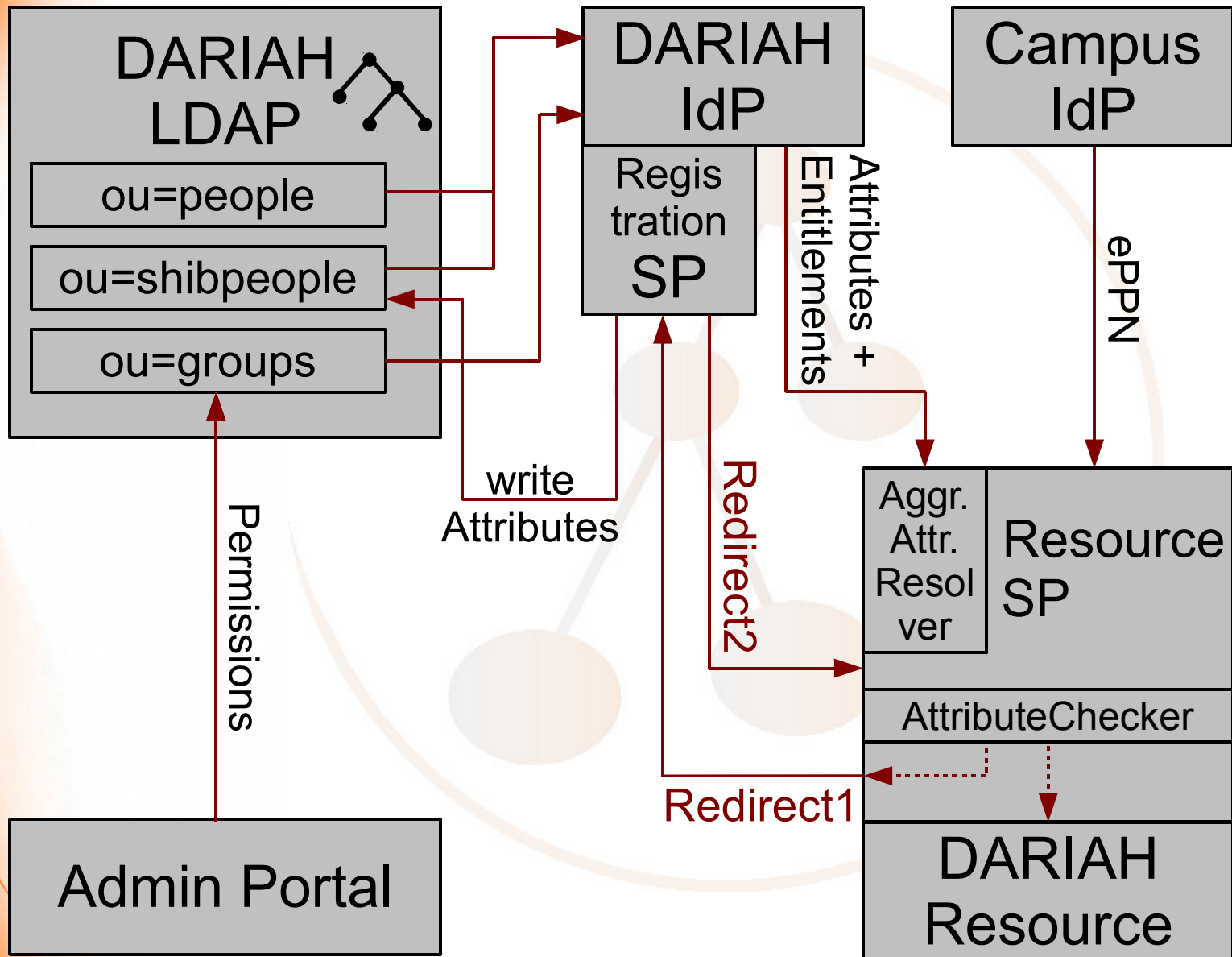
# Premises

- ➤ **Usage of a federated AAI, e.g. DFN-AAI or eduGAIN**
- ➤ **Account at either Campus IdP or DARIAH homeless IdP**
- ➤ **If Campus IdP: need at least one Identifier (ePPN) at the SP**
- ➤ **DARIAH LDAP, containing**
  - ▪ **Homeless users branch (attributes and passwords)**
  - ▪ **Federated users branch (only attributes, provided by the Campus IdP and/or by the user)**
  - ▪ **Authorization groups branch, with members referencing the other two branches**
- ➤ **A resource / DARIAH service, protected by a Shibboleth SP which takes part in the federation**
- ➤ **Management of authorization groups by the Admin Portal**

**DAASI International**

# AAI Flow (1)

- ➢ **User wants to access some resource protected by an SP**
- ➢ **Resource SP sends the user to their Campus IdP for authentication and creates a session upon return**
- ➢ **Resource SP resolves user attributes from both the**
  - ▪ **Campus IdP: eduPersonPrincipalName**
  - ▪ **DARIAH IdP: eduPersonEntitlement based on the user's group membership, and other personal data**
- ➢ **The received attributes are checked**
  - ▪ **Enough attributes? Grant access to resource**
  - ▪ **Not enough attributes? Continue on next slide.**

# AAI Flow (2)

➢ **Delete Session at SP and redirect to registration web form**
- ▪ **Form ist protected by an SP as well**
- ▪ **Form receives HTTP GET attributes**
  - • **User's Campus IdP EntityID, for automatic log-in (SSO)**
  - • **URL of the resource the user initially wanted to access**
- ▪ **Attributes provided by the Campus IdP are presented read-only**
- ▪ **Input fields for missing attributes are provided**
- ▪ **Checkbox for the DARIAH Terms Of Use**

➢ **On form submission, these details are entered into the DARIAH LDAP branch for federated users**

➢ **HTTP Redirect back to the requested resource. Continue on previous slide.**

DAASI
International

# Limitations

- ➢ **Works with ECP, but missing attributes are filled in interactively, so need WebSSO profile for first time access**
- ➢ **Campus IdP should release same set of attributes to a DARIAH Resource SP as to the Registration SP**
- ➢ **DARIAH LDAP knows federated user IDs only after their first login**
  - ▪ **Adding users via Admin portal to groups only possible after registration**
  - ▪ **But: there are other ways to pre-populate groups in LDAP**
- ➢ **Not yet a usable concept for Attribute *updates* at the Campus IdP and their inclusion into the DARIAH LDAP once registration was finished**

# Blueprint: Implementation

**in /etc/shibboleth/shibboleth2.xml:**

```
<ApplicationDefaults ...targeted-id"
  sessionHook="/Shibboleth.sso/AttrChecker">

...

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

        <AttributeResolver type="SimpleAggregation"
                attributeId="eppn"
                format="urn:oid:...1.1.1.6">
          <Entity><DARIAH-IDP></Entity>
        </AttributeResolver>
```

DAASI International

# Blueprint: Implementation

in */etc/shibboleth/attrChecker.html*:

```
<html><head>
    <meta http-equiv="refresh" content="3;
      URL=https://ldap-dariah.esc.rzg.mpg.de/
        Shibboleth.sso/Login
          ?target=
            /secure/UserAttributesCompletion.php
              %3ForiginalURL%3D<shibmlp target/>
            &entityID=<shibmlp entityID/>
        "/>
  <title>Insufficient Information</title>
</head><body>
    <h2>Insufficient Information</h2>
    Your home organisation did not provide
    sufficient attributes to this service.
    Therefore, you are now being redirected to the
DARIAH central user registry. Details:...
</body>
</html>
```

DAASI International

# Blueprint: Implementation

in **/etc/shibboleth/attribute-policy.html:**

```
<!-- deny attributes, except from Dariah IdP -->
<afp:AttributeFilterPolicy>
   <afp:PolicyRequirementRule xsi:type="NOT">
      <Rule xsi:type="basic:AttributeIssuerString"
          value="<DARIAH-IDP>" />
   </afp:PolicyRequirementRule>

   <afp:AttributeRule attributeID="*">
      <afp:DenyValueRule xsi:type="ANY"/>
   </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

**We need this only because the Shibboleth SP cannot de-duplicate attributes with the same values...**

**DAASI** International

# Blueprint: Implementation

in **/etc/shibboleth/attribute-map.html:**

```
<Attribute
    name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
    id="isMemberOf" />
```

..that's all!

DAASI International

# Thank You!

➢ **Questions?**

➢ **DAASI International**
  ▪ **www.daasi.de**
  ▪ **Info@daasi.de**

**DAASI** International

# AAI@EduHr

## Croatian Research and Education Identity Federation

**Miroslav Milinović**

University of Zagreb, University Computing Centre (SRCE)

<Miroslav.Milinovic@srce.hr>

CESSDA SAW Workshop

*Zagreb, March 1-2, 2017*

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

# Contents

- Identity federations

- AAI@EduHr

- eduGAIN

- AAI@EduHr for SPs / developers

# e-infrastucture



| Information systems and applications |
| Data services (digital archives, repositories, …) |
| **Middleware** (identity federations, AAA, …) |
| Computing resources (servers, storage, HPC, grid, …) |
| Data centers |
| Network services |

# Identity federation model



authenticates user;
provides attributes

consumes attributes;
allows access

IdP

trust

SP

2

1

3

user accesses service

srce
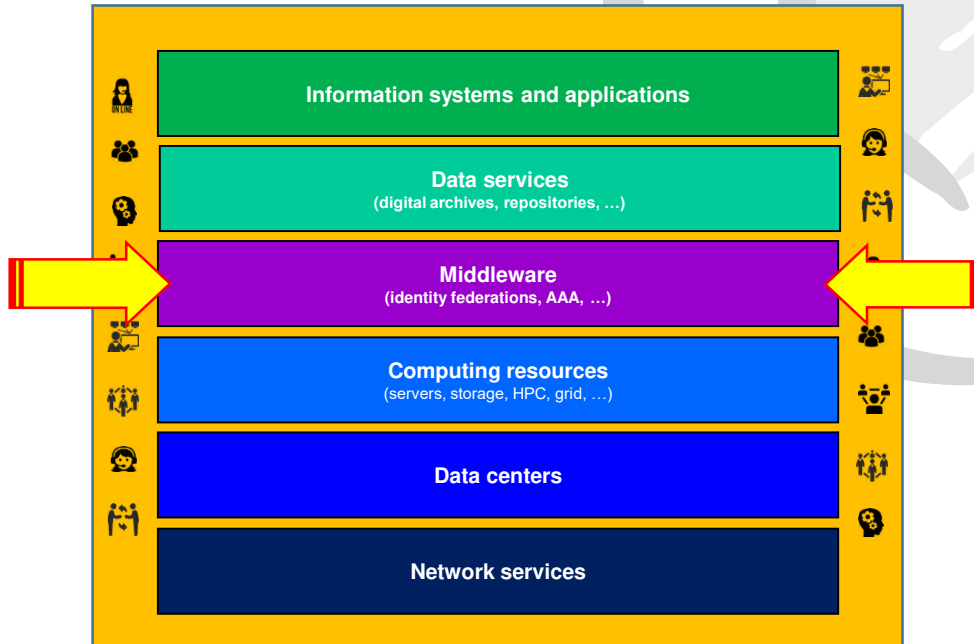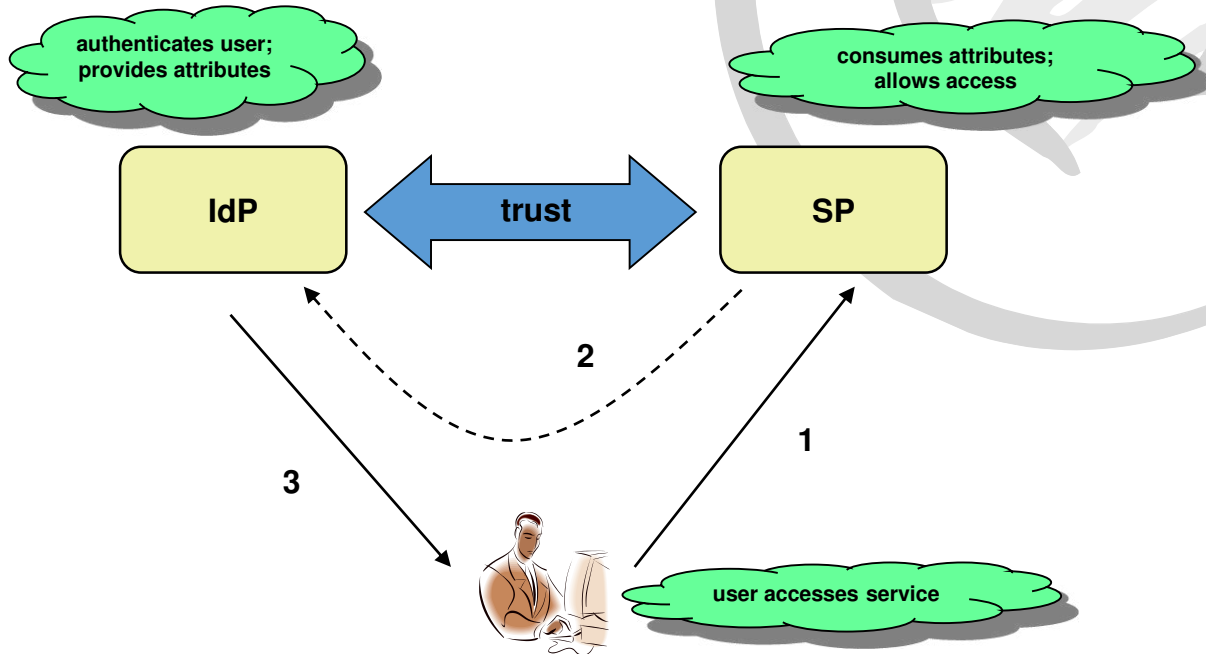
@EduHr

# Mash federation model
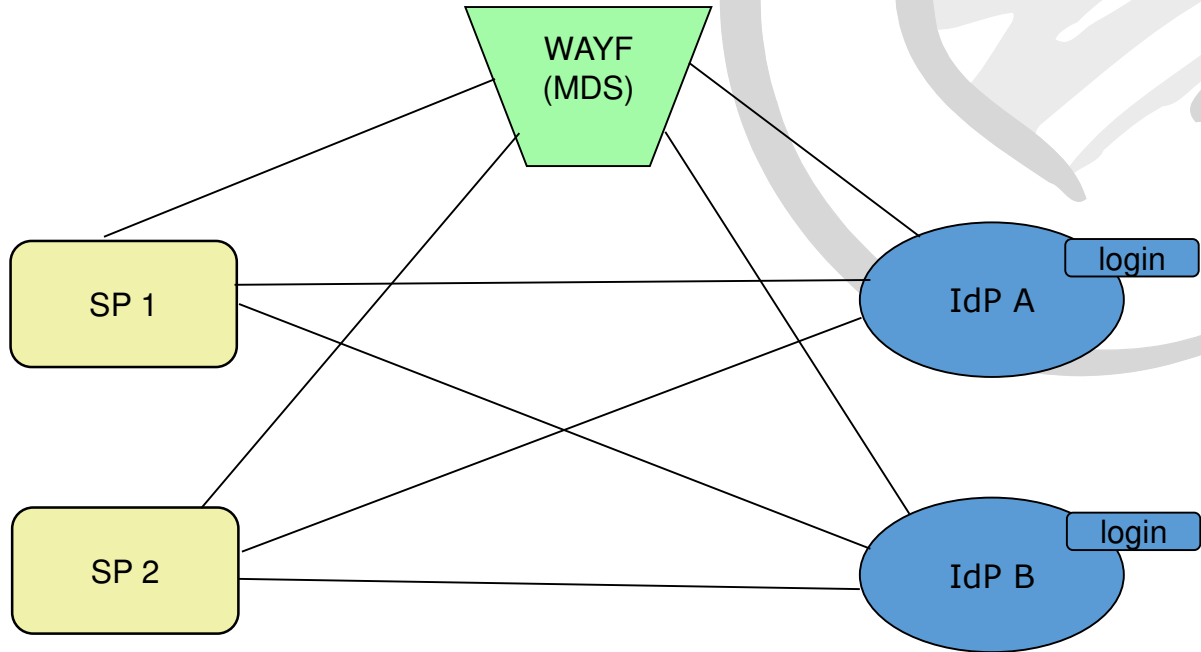
# Hub-and-spoke federation model
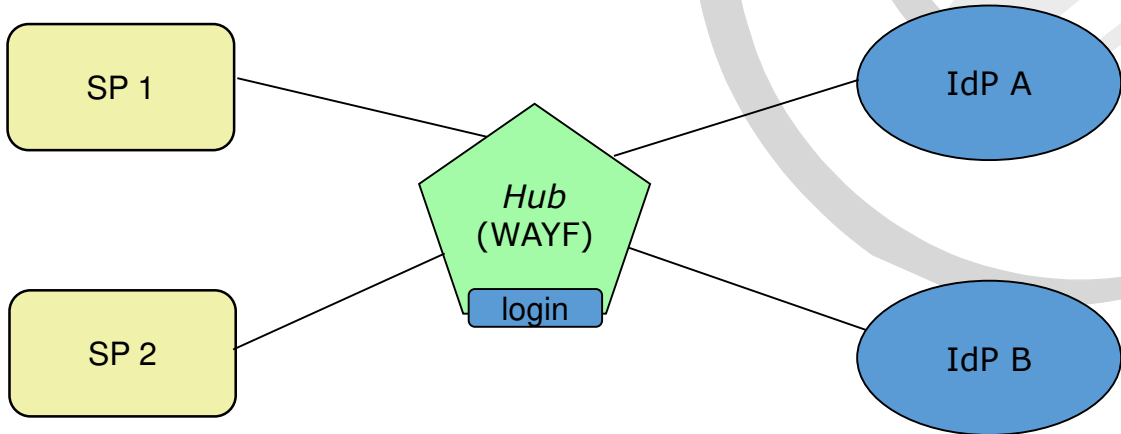
# Virtual Organisations (VOs) / Attribute Authorities (AAs)
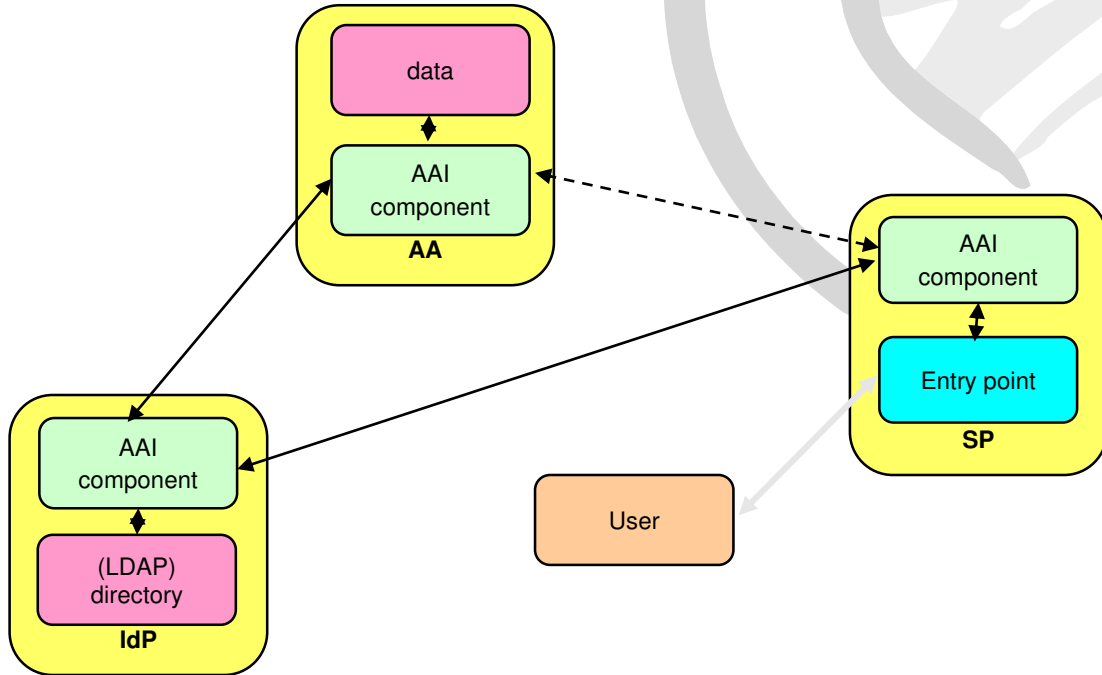
# AAI@EduHr: Croatian R&E Identity Federation

- *Autentikacijska i autorizacijska infrastruktura znanosti i (visokog) obrazovanja u RH*
- in production since March 1, 2006
- *hub-and-spoke* architecture
- Policy document: Pravilnik o ustroju, ver.1.3.1 (http://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf)
- March 1, 2017:
  - 229 IdPs
  - 603 SPs
  - 878.173 e-identites
  - connected to:
    - global services: eduroam  and eduGAIN
    - National e-gov service: NIAS (e-Građani)
- Web: http://www.aaiedu.hr
  (notice: most of the documentation is in Croatian language only)

srce

# AAI@EduHr in numbers

successful SSO authN
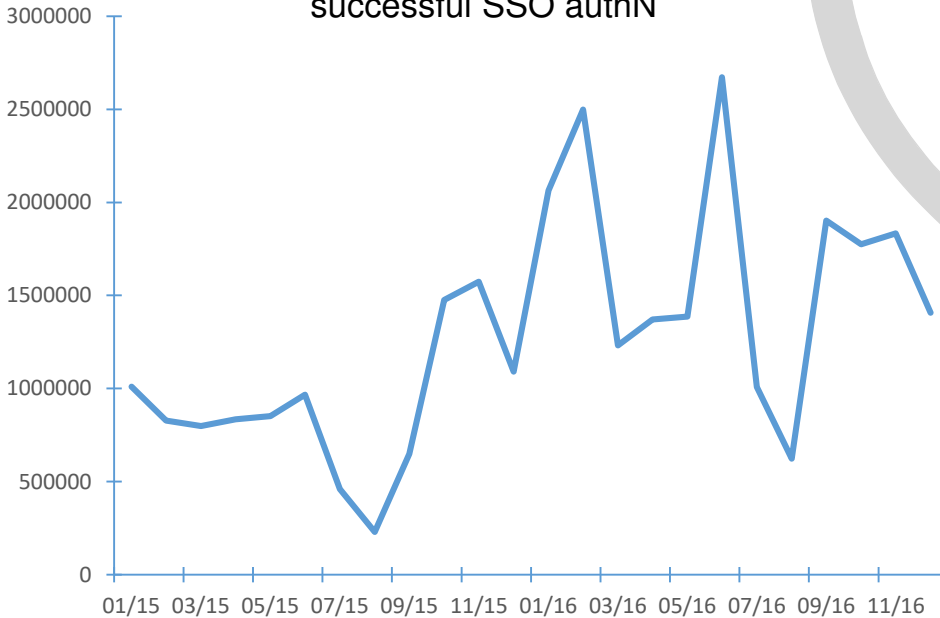


Successful Web SSO authN:
last 30 days: 2.964.140
last 24 hours: 104.587

Successful RADIUS authN:
last 30 days: 14.013.800
last 24 hours: 603.678

(March 1, 2017)

# More statistics …
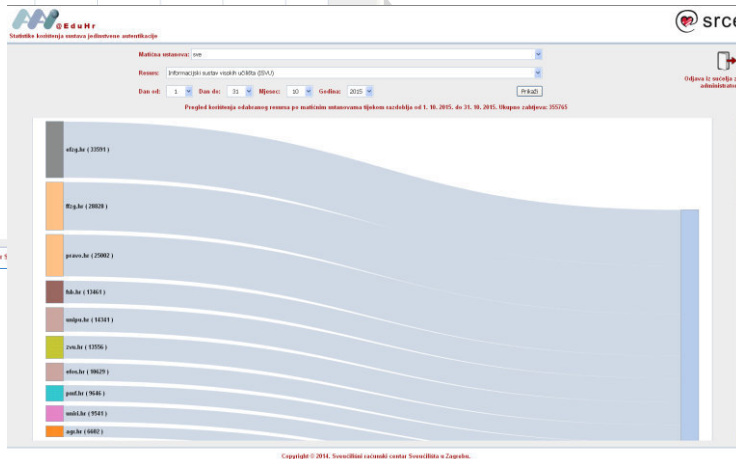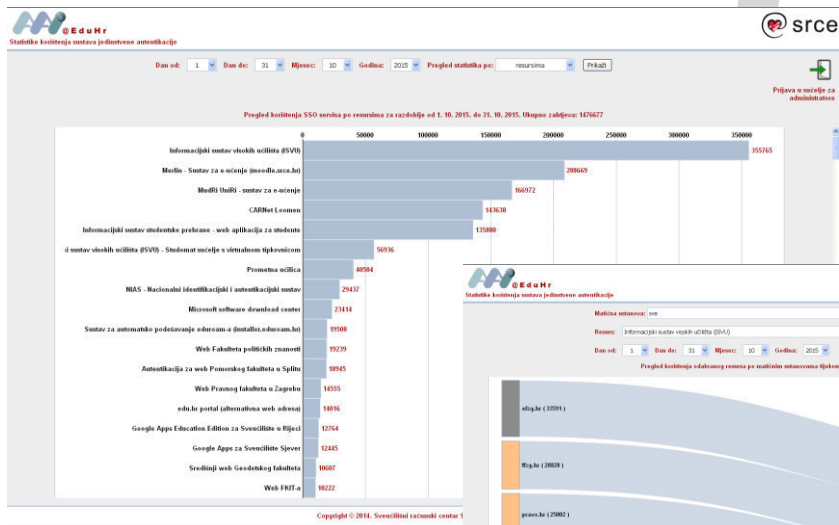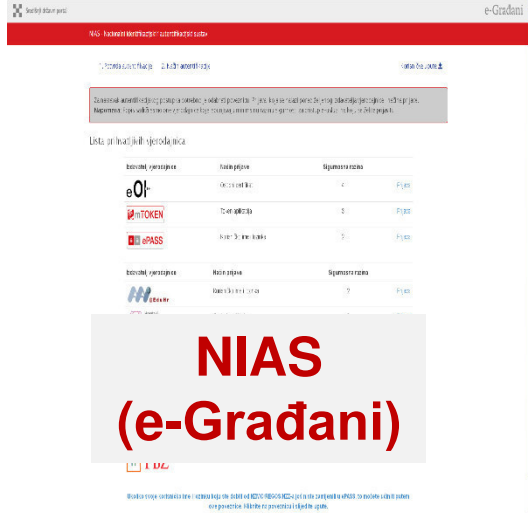
# Connections with other services



www.edugain.org

www.eduroam.org



NIAS
(e-Građani)

srce

@EduHr

# AAI@EduHr: Hub-and-spoke federation



SP 1

SP 2

*Hub*
(WAYF)

login

IdP A

IdP B

Central services
provided by Srce

# AAI@EduHr architecture



social networks

eduroam

NIAS

eduGAIN

OpenID, …

RADIUS

HTTPS / SAML

HTTPS / SAML

RADIUS

HTTPS / SOAP

Central
AAI@EduHr services
(RADIUS proxy, FWS,
MDS, login/SSO, VO/AA)

RADIUS

HTTPS / SAML

AOSI-WS
&
RADIUS server

AAI@EduHr
component

LDAP directory

user uid@realm.hr

entry point

IdP

SP
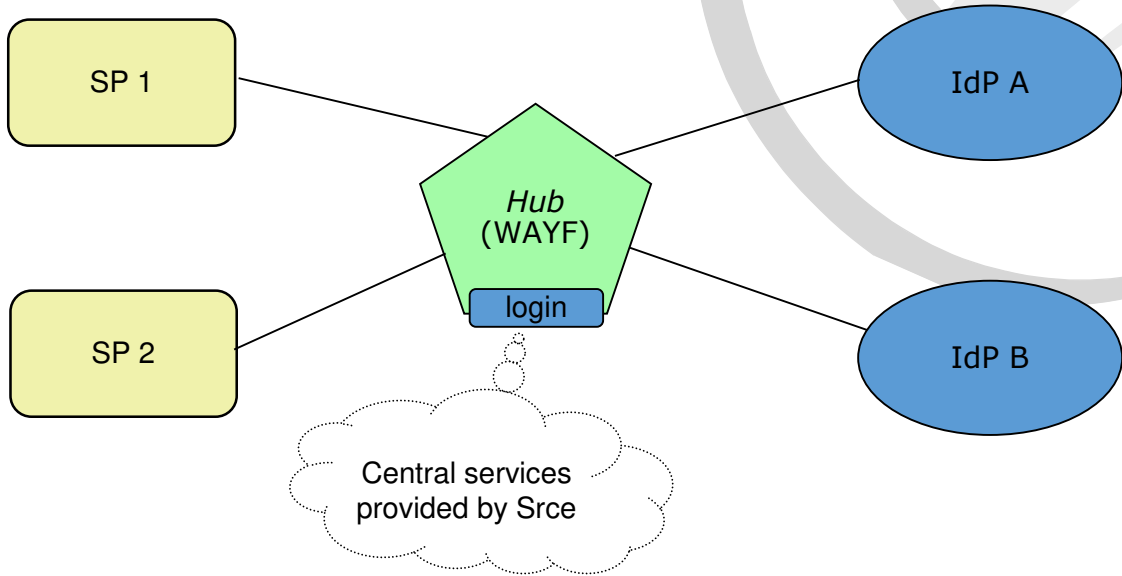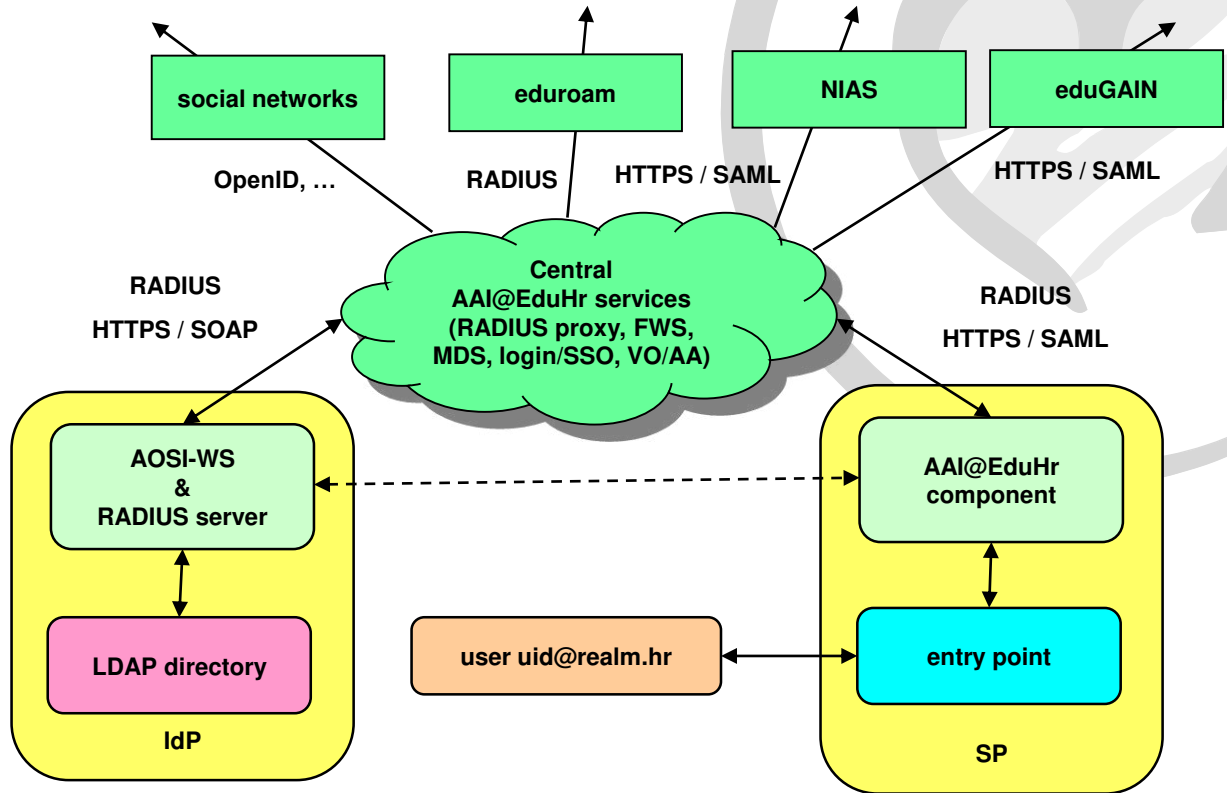
# AAI@EduHr: IdM
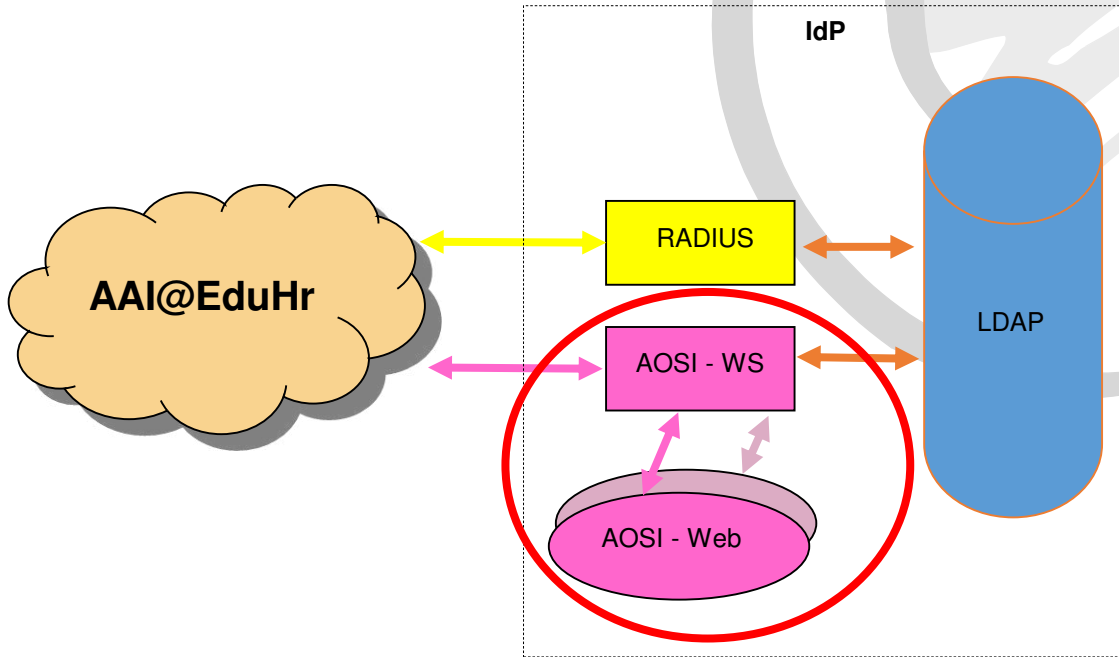
# What is eduGAIN?
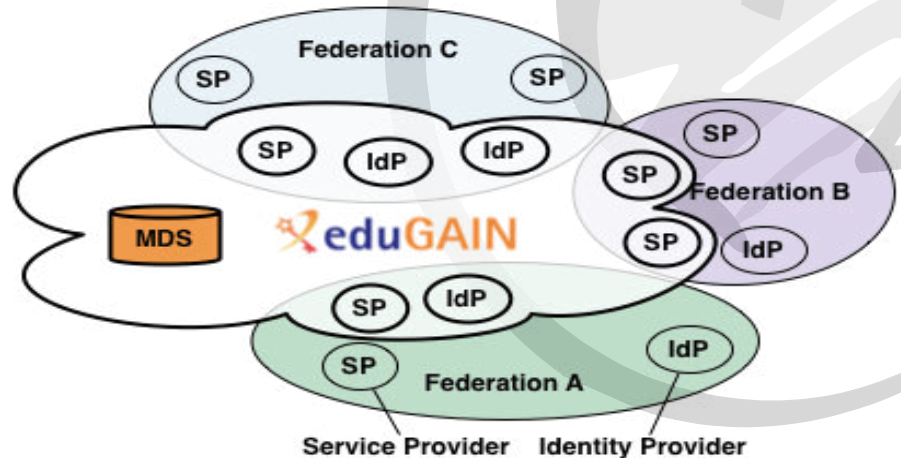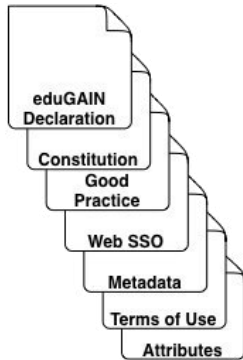


- **edu**cational **G**lobal **A**uthentication **In**frastructure
- basic components:
  - eduGAIN Policy Framework (https://technical.edugain.org/documents)
  - MDS (Metadata Distribution Service; mds.edugain.org)
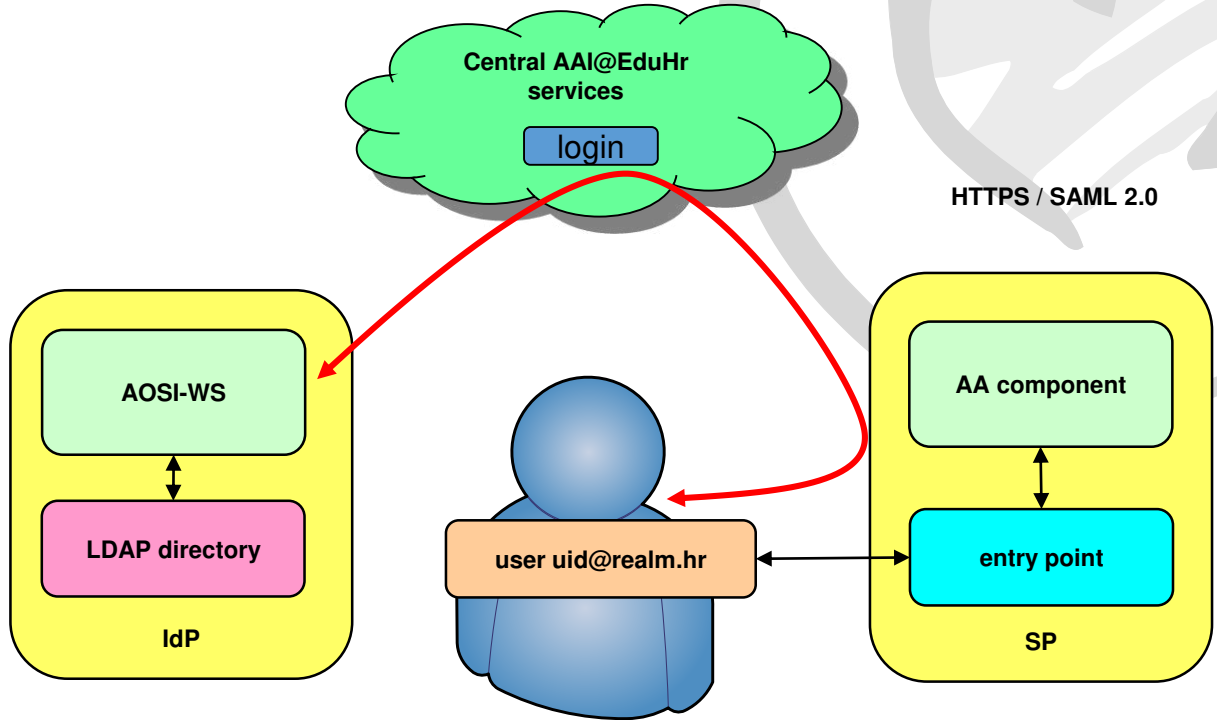
**eduGAIN**

# eduGAIN
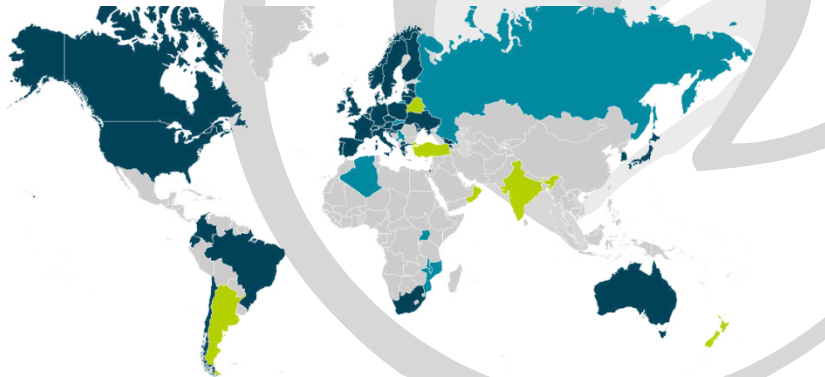


- in production since 2011

- 41 member federations

- www.edugain.org
- technical.edugain.org

**edu**GAIN

# AAI@EduHr in eduGAIN

- AAI@EduHr is eduGAIN member
- Srce represents AAI@EduHr in eduGAIN bodies

- AAI@EduHr entites in eduGAIN:
  - **all IdPs are** automatically **„in"** eduGAIN
    - attribute release based on *eduGAIN Attribute Profile*
    - an IdP can opt-out
  - **all SPs are „out"**
    - an SP has to opt-in (ask Srce to be included)
    - an SP has to fulfill organisational and technical requirements

srce

# AAI@EduHr for SPs (Web SSO scenario)



Central AAI@EduHr services

login

HTTPS / SAML 2.0

AOSI-WS

LDAP directory

IdP

user uid@realm.hr

AA component

entry point

SP

srce

@EduHr

# AAI@EduHr for SPs (Developers)

- supported protocols:
  - SAML 2.0
  - RADIUS (network access, special cases of non-web-based services)

- supported platforms:
  - PHP (simpleSAMLphp)
  - Java (Spring Security SAML, …)
  - .NET (OIOSAML.NET):
  - Python / Django

  - Shibboleth compatible tools/platforms

  - any platform compatible with SAML 2.0

- testing environment: AAI@EduHr Lab

# SP set-up in AAI@EduHr

- study:
  - AAI@EduHr Policy
    ([http://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf](http://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf))
  - documentation for SPs
  - ([http://www.aaiedu.hr/za-davatelje-usluga](http://www.aaiedu.hr/za-davatelje-usluga))

- register your application via resource registry:
  - [www.aaiedu.hr/aairr](www.aaiedu.hr/aairr)
  - indicate special cases: eduGAIN and/or additional login via social networks

- make necessary ajustments in your application:
  - install missing components (e.g. SSP, SAML modules, …)
  - use AAI@EduHr LAB for testing

- AAI@EduHr team provides support via e-mail address aai@srce.hr

# AAI@EduHr and social networks



http://www.unizg.hr/authdemo/

# How to opt-in eduGAIN with your SP?

- let Srce know:
  - we provide support / know-how
  - we publish your metadata / register your app. in eduGAIN

- ajust your service policy:
  - privacy policy / CoCo (see eduGAIN documentation)

- ajust technical components of your service:
  - attribute handling
  - discovery service (login screen / WAYF)
  - metadata handling
  - verify before production
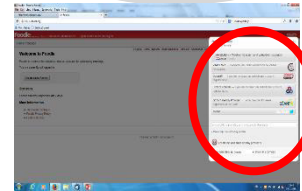
# Discovery service examples



https://foodl.org/
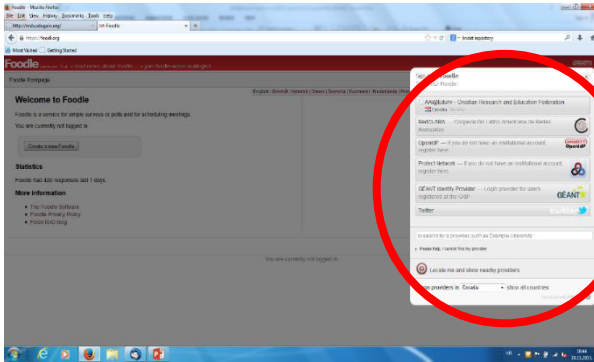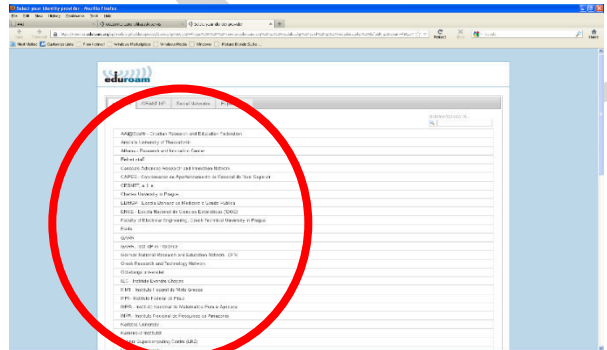


http://monitor.eduroam.org/db_web

# Learning opportunity

- we organize a workshop for SPs / application developers on April 4

- check http://www.srce.unizg.hr/dei/radionice

**AAI@EduHr**

# http://www.aaiedu.hr

**aai@srce.hr**

**edu**GAIN

Sveučilište u Zagrebu
Sveučilišni računski centar

Ovo djelo je dano na korištenje pod licencom Creative Commons *Imenovanje-Nekomercijalno 4.0 međunarodna.*

**www.srce.unizg.hr**     **creativecommons.org/licenses/by-nc/4.0/deed.hr**          **www.srce.unizg.hr/otvoreni-pristup**

srce
otvoreni pristup