



Authentication and Authorisation for Research and Collaboration

## Mechanism of Interfederation

Alessandra Scicchitano

AARC NA2 WP Leader, GEANT PDO

Taipei - Taiwan

13th March 2016

- Federated Identity Management
- Interfederation
- EduGAIN
- Example of use of eduGAIN
- Conclusions

# Federated Identity Management

---

**Federated identity management (FIM)** enables identity information to be developed and shared among several entities and across trust domains. Tools and standards permit identity attributes to be transferred from one trusted identifying and authenticating entity to another for authentication, authorization and other purposes.

The difference between Single Sign On (SSO) and federated identity is subtle:

- SSO unifies access management for disparate systems within an organization.
- Federated identity does the same, but across different organizations.

# FIM Components

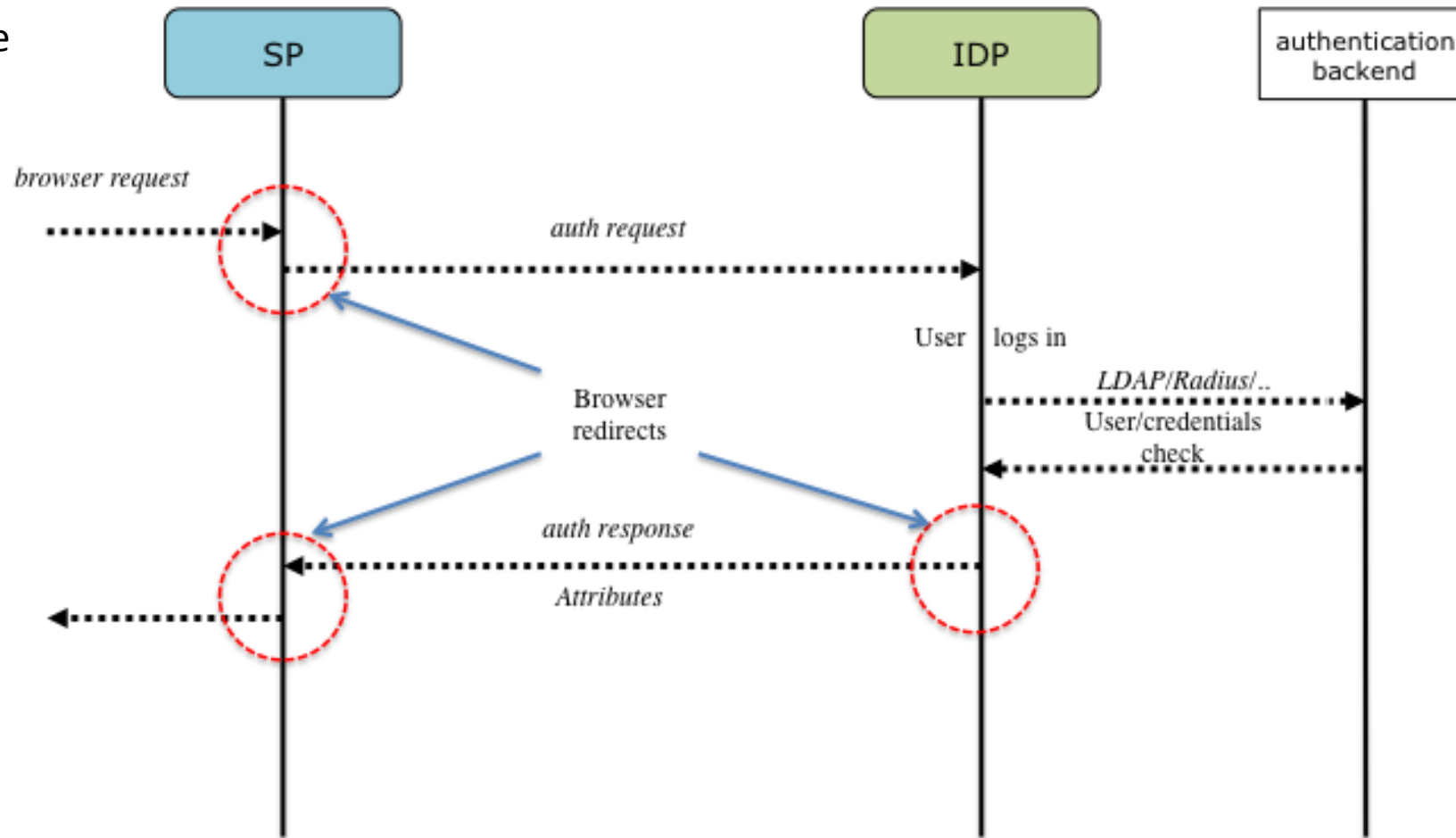
---

There 3 main parties in Federated Identity Management:

- User: Each user is associated with a person. A user is characterized by an identity. A collection of attributes that represent properties about that specific person.
- Identity Provider (IdP): asserts authentication and identity information about the user.
- Service Provider (SP): receives and checks the information to grant authorization to the user to access the service.

# FIM: How it works

Almost all federations currently use the SAML2 protocol



<https://www.openconext.org>

# Federation Identity Management

---

- SPs and IdPs have to trust each other for this approach to work. Typically this trust is made explicit by signing policies and contracts that describe the requirements and responsibilities of the IdPs and SPs. **An Identity Federation** is a collection of IdPs and SPs that have agreed to work together and trust each other.
- An organization may belong to more than one federation at a time
- IdPs and SPs "know" nothing about the federations. They deal with metadata.

# Federation Metadata

---

- An XML document that describes every federation entity
- Contains
  - Unique identifier for each entity known as the entityID
  - Endpoints where each entity can be contacted
  - Certificates used for signing and encrypting data
- May contain
  - Organization and person contact information
  - Information about which attributes an SP wants/needs
- Metadata is usually distributed by a public HTTP URL
  - The metadata should be digitally signed
- Metadata must be kept up to date so that
  - New entities can work with existing ones
  - Old, or revoked, entities are blocked

Credit to Lukas Hammerle - SWITCH for this slide

# Federation Architectures

---

A federation can be built according to either the mesh or the hub-and-spoke principle:

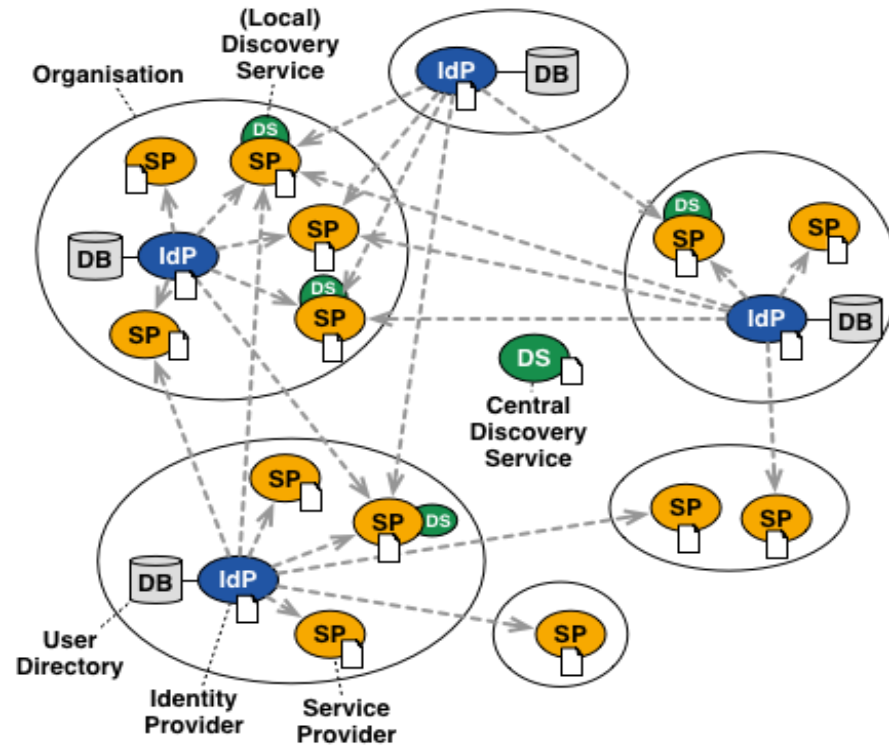
- **Mesh federation:** each entity is responsible for its connections to other entities.
- **Hub-and-spoke federation:** all entities connect to the hub and the hub manages connections between entities on a central location.



# Mesh vs H&S

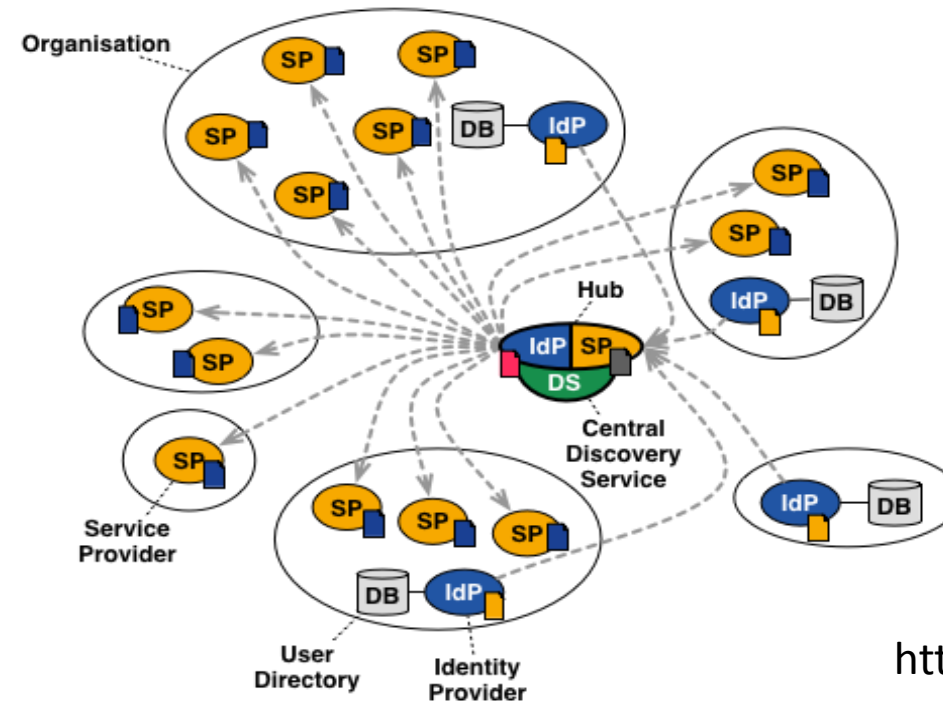
## Full Mesh Federation

~80% of all NREN Federations (June 2013)  
E.g InCommon, UKAMF, SWITCHaai, SWAMID, HAKA, AAF



## Hub-and-Spoke Federation with Distributed Login

~15% of all NREN Federations (June 2013)  
SURFconext, WAYF.dk, SIR, TAAT, Confia



<https://wiki.surfnet.nl>

--> SAML Assertion Flow

Connection to User Directory  
SAML Metadata including all SPs and IdPs

--> SAML Assertion Flow

— Connection to User Directory

■ SAML Metadata including hub's SP

■ SAML Metadata including hub's IdP

■ SAML Metadata including all other SPs

■ SAML Metadata including all other IdPs

# Interfederation

---

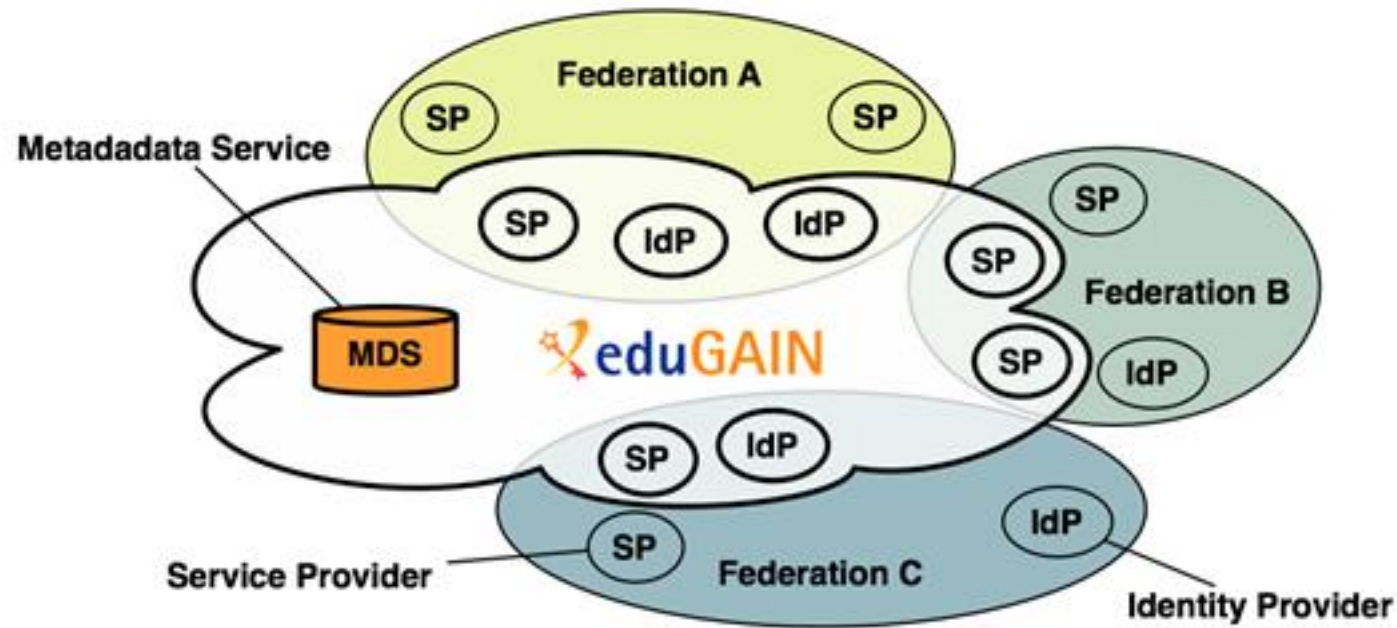
Identity Federations are mostly of national scope but:

- research projects are international
- content publishers' customers are international
- audience of research wikis and blogs is international

Interconnecting national federations → Interfederation

- Interfederation service facilitates international research collaboration
- Content publishers can offer their services without concluding contracts with each single federation

- eduGAIN is a form of *interfederation*. Participating federations share information (metadata) about entities from their own federation with eduGAIN. Next, eduGAIN bundles these metadata and publishes it on a central location.



# Some benefits

---

- Enables trustworthy exchange of information between federations without many bilateral agreements
- Reduces the costs of developing and operating services
- Improves the security and end-user experience of services
- Enables service providers to greatly expand their user base
- Enables identity providers to increase the number of services available to their users

# Some issues

---

- Federated incident handling: Concerns of major science service providers that if they go the federated route, they need to be notified by IdP's of compromised accounts relevant to the service provider.
- Attribute release is proving very problematic.
- Metadata is increasing in size and complexity.

# Example: TCS

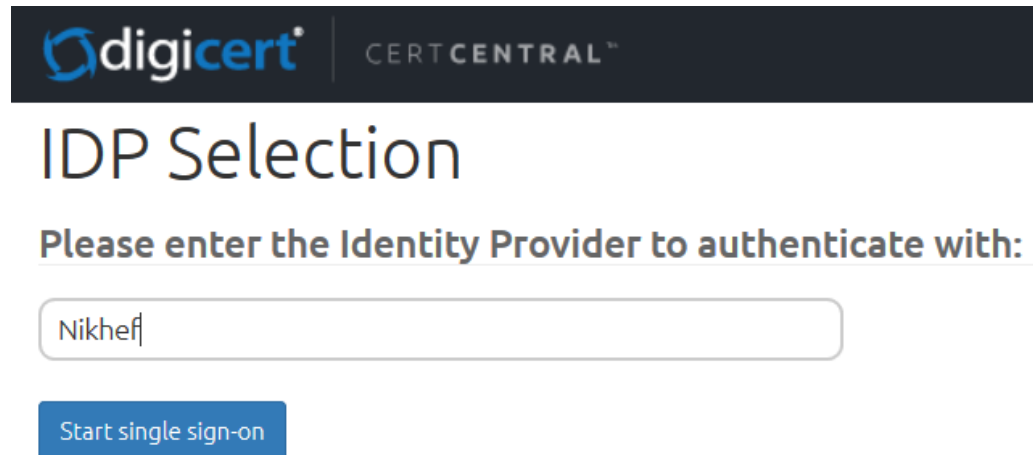
---

## Trusted Certificate Service (TCS):

- Since July 2015 with a new Supplier: Digicert
- And two portals: CertCentral and the SAML portal
- The SAML consumes the eduGAIN metadata

# SSO SAML portal hosted by DigiCert

- Scope: **client certificates**
- DigiCert itself is a SAML2Int Service Provider  
`<md:EntityDescriptor entityID="https://www.digicert.com/sso">`
- visible to Federations and IdPs via the eduGAIN metadata
- DigiCert knows about all IdPs in eduGAIN (via eduID.at – Austrian Federation)



The screenshot shows the DigiCert CERT CENTRAL IDP Selection page. At the top, there is a dark header with the DigiCert logo and the text "CERT CENTRAL™". Below the header, the title "IDP Selection" is displayed in a large, dark font. Underneath the title, a prompt reads "Please enter the Identity Provider to authenticate with:". Below this prompt is a text input field containing the text "Nikhef". At the bottom of the form, there is a blue button with the text "Start single sign-on".

Thanks David! 😊

# How to get the SAML SSO service enabled

---

Who can get client certs via Federated SSO? Users of all IdPs that are:

- part of a subscriber that:
  - has signed up to TCS via their NREN
  - has its IdP data published in the eduGAIN metadata  
*looks like*  
`<md:EntityDescriptor  
entityID="https://sso.nikhef.nl/sso/">`
- where the very same subscriber has:
  - registered and validated at least one organisation,
  - a SAML2Int IdP that releases schacHomeOrganisation, and that is linked to that organisation via the CertCentral portal by an admin
- and the requesting user has the proper eduPersonEntitlement



# Attributes released (for David...)

SURF  
CONEXT

My Profile

My Apps

Exit

EN | NL | HELP

SURFconext Apps

You have given permission to share profile information with the following services:

Service/App	EULA	Support URL	Support email
▶ <a href="#">CERTcentral   Digicert</a>		<a href="#">Support pages</a>	

The following attributes are released to this Service Provider:

Attribute	Value
<b>Surname</b>	Groep
<b>E-mailaddress</b>	davidg@nikhef.nl
<b>First name</b>	David
<b>Entitlement</b>	<ul style="list-style-type: none"><li>urn:mace:terena.org:tcs:personal-admin</li><li>urn:mace:terena.org:tcs:personal-user</li></ul>
<b>Institution user ID</b>	davidg@nikhef.nl
<b>Organization</b>	nikhef.nl
<b>Display Name</b>	David Groep

# The benefits for TCS

---

- 29 NRENs are customers of TCS
- Most of them run their own federation
- All of which have institutions and organizations that belong to their federation
- They can all get TCS client certificates using their own personal credentials via one single portal...

# Conclusions

---

- FIM makes life easier getting ready of too many usernames and passwords;
- It protects user information;
- Interfederation enables local federations to talk to each other;
- EduGAIN is a form of interfederation that is well known and established since years;
- There are clear examples of how interfederation enables international collaboration;
- TCS is one of them.

FIM is cool!!



# Thank you Any Questions?

Alessandra.Scicchitano@geant.org



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).