

# Update on identity federation



Romain Wartel, CERN

July 2015 GDB

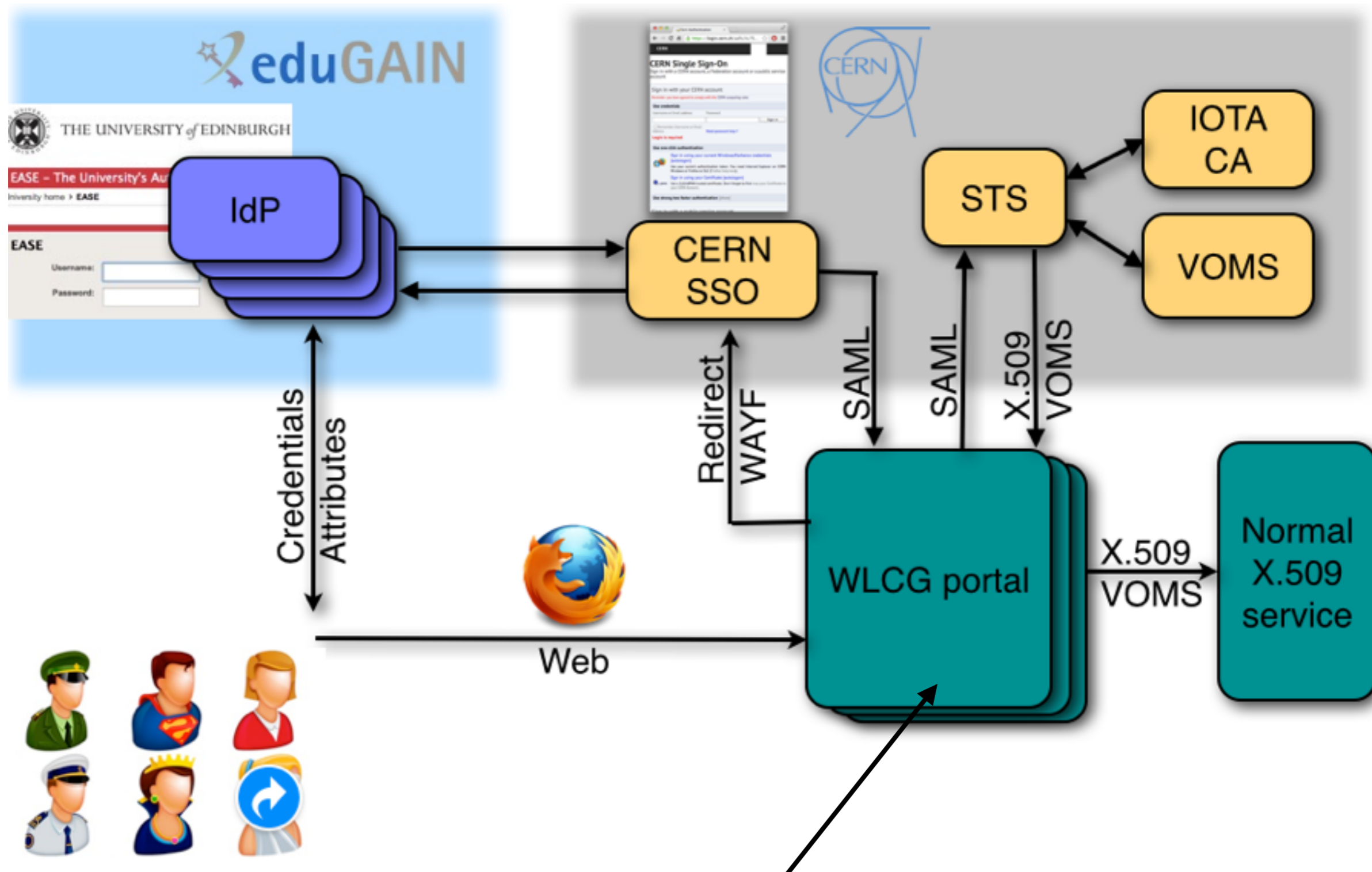


# Brief AARC / Sirtfi update

- AARC started
  - Kick-off meeting complete
  - Main tasks started
  - Work plans are being finalised
  - Partners who committed to AARC are being identified & actioned
- Sirtifi
  - Working group on incident response for federations
  - Significant US involvement, links with FIM4R and REFEDS
  - Current work
    - Register security contact information in EduGAIN
    - Express compliance in metadata with Sirtfi trust framework
    - Test this with a few key identity and service providers in EduGAIN (CERN, InCommon, LIGO, Surfeit, Sunet)
    - Continue work on the trust framework



# WLCG pilot



Are there other VOs interested in participating?



# User identity mapping

© MARK ANDERSON

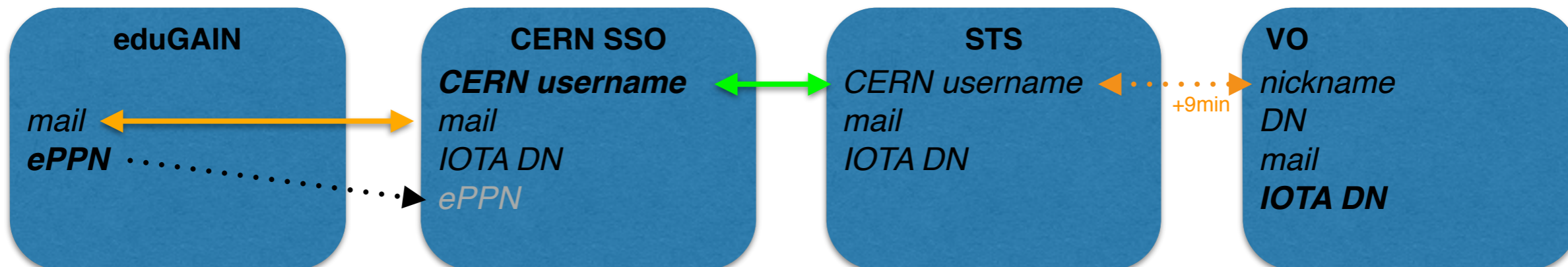
WWW.ANDERTOONS.COM



"I'm here about the details."



# User identity mapping



- **eduPersonPrincipalName? (ePPN)**

*A single value of the form user@domain, where domain is (typically) a DNS-like subdomain representing the security domain of the user (e.g., "osu.edu") and user is generally a username, NetID, UserID, etc. of the sort typically assigned for authentication to network services within the security domain. [...] the possibility for recycling/reassignment does still exist within the domain of a given identity provider. Note that at some Identity Providers a user can freely change their local account name (in the case of a name change due to marriage, for example), and the corresponding EPPN will typically change as well. This can cause a loss of service until name changes propagate throughout every application storing the value. For a less dynamic identifier, see also the eduPersonTargetedID attribute.*

—> No guarantee the eppn will be unique for each user over time

- **eduPersonTargetedID?**

*A single string value [...] that uniquely identifies a user in an opaque, privacy-preserving fashion.*

—> A hash generated via ePPN and SP entityID. Unique per service. Not released by many IdPs anyway.

- **eduPersonUniqueID?**

*A long-lived, non re-assignable, omnidirectional identifier suitable for use as a principal identifier by authentication providers or as a unique external key by applications.*

—> Perfect! But nobody implements this!

<https://www.incommon.org/federation/attributesummary.html#eduPersonPrincipal>



# Attributes

eduPersonTargetedID



SWITCH

SWITCH [CH] https://attribute-viewer.aai.switch.ch/aai/ Romain

## AAI Attribute Viewer

There are more than 30 [attributes defined for SWITCHaai](#). Not all of attributes can be released by [all participating organisations](#) and not all of them are available for every AAI user. What you should see below is:

- **8 SWITCHaai core attributes**, released by the user's home organisation and must be available for all users
- 0 or more **other SWITCHaai attributes**, released by the user's home organisation and are optional to implement for users
- 0 or more **local/bilateral attributes**, released by the user's home organisation and are used only by one or a few organizations
- 5 or more **Metadata attributes**, set by the Shibboleth Service Provider from the user organisation's metadata. [Find out more ...](#)
- 8 or more **Shibboleth attributes**, set by the Shibboleth Service Provider if a user has a valid session.

Also check if CERN is passing the [Interfederation Attribute Check](#) to allow its users access to research and education services world-wide available via [eduGAIN](#).

Attributes	Values
<b>persistent-id</b> SAML2 Attribute Name: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	https://cern.ch/login!https://attribute-viewer.aai.switch.ch/shibboleth!C3T9739D3CNPrNLnj7s7LN7OMsv+BbDJw0GPRwm13bk=
<b>uniqueID</b> SAML2 Attribute Name: urn:oid:2.16.756.1.2.5.1.1.1	rwartel@cern.ch
<b>givenName</b> SAML2 Attribute Name: urn:oid:2.5.4.42	Romain
<b>surname</b> SAML2 Attribute Name: urn:oid:2.5.4.4	Wartel
<b>mail</b> SAML2 Attribute Name: urn:oid:0.9.2342.19200300.100.1.3	Romain.Wartel@cern.ch
<b>homeOrganization</b> SAML2 Attribute Name: urn:oid:2.16.756.1.2.5.1.1.4	cern.ch
<b>homeOrganizationType</b> SAML2 Attribute Name: urn:oid:2.16.756.1.2.5.1.1.5	others
<b>affiliation</b> SAML2 Attribute Name: urn:oid:1.3.6.1.4.1.5923.1.1.1.1	member
<b>cn</b> SAML2 Attribute Name: urn:oid:2.5.4.3	Romain Wartel
<b>displayName</b> SAML2 Attribute Name: urn:oid:2.16.840.1.113730.3.1.241	Romain Wartel
<b>principalName</b> SAML2 Attribute Name: urn:oid:1.3.6.1.4.1.5923.1.1.1.6	rwartel@cern.ch
<b>schacHomeOrganization</b> SAML2 Attribute Name: urn:oid:1.3.6.1.4.1.25178.1.2.9	cern.ch
<b>schacHomeOrganizationType</b> SAML2 Attribute Name: urn:oid:1.3.6.1.4.1.25178.1.2.9	urn:schac:homeOrganizationType:ch:others



# Attributes

Haka Attribute Test Service

The mandatory attributes in the schema are *cn* (*urn:oid:2.5.4.3*), *sn* (*urn:oid:2.5.4.4*), *displayName* (*urn:oid:2.5.4.42*), *eduPersonPrincipalName* (*urn:oid:1.3.6.1.4.1.5923.1.1.1.6*), *schacHomeOrganizationType* (*urn:oid:1.3.6.1.4.1.25178.1.2.10*) and *schacHomeOrganization* (*urn:oid:1.3.6.1.4.1.1466.115.121.1.15*).

### Instructions

#### Icons

The following icons are used to represent the status of each attribute:

- ✔ Attribute was released and it has reasonably correct value.
- ✘ A mandatory attribute was not released or the attribute's value is not within the accepted value range.
- ⬇ An optional attribute was not released.

#### End-users

In case the attribute values are incorrect or a attribute was not released, please contact your local user administration. They are able to add/modify attributes to your user account, this attribute test service only displays the attributes that given to it from your authentication server. Note that the allowed attribute values are displayed as regular expressions so they do not represent the value shown to user.

#### Haka system administrators

If attributes are not displayed/released correctly, please contact [haka@csc.fi](mailto:haka@csc.fi).

### Released attributes

Your Identity Provider's entityid is <https://cern.ch/login>  
 You were authenticated using method: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

Attribute URN/OID	Value	Required Value
✔ urn:mace:dir:attribute-def:eduPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6	rwartel@cern.ch	.*@.*
✔ urn:mace:dir:attribute-def:eduPersonScopedAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9	member@cern.ch	^(student faculty staff employee member affiliate alum)@.*;(student faculty staff employee member affiliate alum)@.*)*\$
✔ urn:mace:dir:attribute-def:eduPersonAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.1	member	^(student faculty staff employee member affiliate alum);(student faculty staff employee member affiliate alum)*\$
⬇ urn:mace:dir:attribute-def:eduPersonEntitlement urn:oid:1.3.6.1.4.1.5923.1.1.1.7		
⬇ urn:mace:dir:attribute-def:eduPersonTargetedID urn:oid:1.3.6.1.4.1.5923.1.1.1.10		
✔ urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	9GwVHPSqtmWDBTUj/sVs4QF0wrYDaEGscl2L6CfOFTI=!!https://cern.ch/login!!https://rr.funet.fi/attribute-test	

eduPersonTargetedID



# Attributes

Interfederation Attribute Test

SWITCH [CH] <https://attribute-viewer.aai.switch.ch/interfederation-test/test/>

Romain

## SWITCHaai

### Interfederation Attribute Test

For [interfederation support](#), an Identity Provider **SHOULD** be able to release all recommended [international attributes](#). This page checks whether all those attributes and values are present.

If interfederation support was already enabled for your organisation, please also ensure that the Identity Provider is configured following the legal recommendations as described on the page [Legal Templates for SWITCHaai](#). In particular, it is recommended to deploy a user attribute consent module like [uApprove](#).

#### Recommended eduGAIN/Interfederation Attributes

Attributes	Values
principalName	rwartel@cern.ch
mail	Romain.Wartel@cern.ch
cn	Romain Wartel
displayName	Romain Wartel
affiliation	member
scoped-affiliation	member@cern.ch
schacHomeOrganization	cern.ch
schacHomeOrganizationType	urn:scsh:homeOrganizationType:ch:others
persistent-id	<a href="https://cern.ch/login!https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth!jsWYKBS6114D1VlmMNeQHOrjoen7lgppKJxpsT/hbyA=">https://cern.ch/login! https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth! jsWYKBS6114D1VlmMNeQHOrjoen7lgppKJxpsT/hbyA=</a>


#### Test Verdict

### Congratulations!

All recommended attributes for Interfederation-support are present and their values passed the above basic tests. This is a first and important step to become Interfederation-enabled!

What this means is that your Identity Provider should now be able to communicate with most interfederated services provided it has the necessary attribute release policies configured for them and provided your IdP consumes the interfederation/eduGAIN metadata.

A final check to see if your Identity Provider is correctly configured for interfederation is to [access an interfederation service like the eduGAIN Wiki](#)



## Interfederation Attribute Test Passed





# Next steps

- Use the CERN username as the unique identifier, and push the IOTA DN in VOMS automatically
- Add support for more applications and/or experiments
- Address ongoing policy and trust issues
  - See next talk from Dave
- Use “ePPN” or better at a later stage, when the pilot is functioning
- Lobby for the implementation of the eduPersonUniqueID