Authentication and Authorisation for Research and Collaboration

Architecture

Guidelines for attribute translation from SAML to OIDC

Nicolas Liampotis

CERN

29 November 2016

Current status

- eduPerson (201602) specification: http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html
- Registered OIDC claims: https://www.iana.org/assignments/jwt/jwt.xhtml
- OpenID Connect for Research and Education Working Group (OIDCre): https://wiki.refeds.org/display/GROUPS/OIDCre

SAML-to-OIDC Mappings

SAML authN response element	OIDC scope	OIDC claim	UserInfo endpoint	Introspection endpoint
eduPersonUniqueId	openid	sub (public)	Y	Y
eduPersonPrincipalName	openid	sub (public*)	Y	Y
eduPersonTargetedID (SAML2 Persistent NameID)	openid	sub (pairwise)	Y	Y
displayName	profile	name	Y	N
givenName	profile	given_name	Y	N
sn	profile	family_name	Y	N
mail	email	email	Y	N
AuthncontextClass (multi-valued)	openid	acr (single-valued)	Y	?
eduPersonAssurance (multi-valued)	openid	amr (multi-valued)	Y	?
eduPersonScopedAffiliation	affiliation?	edu_person_scoped_affiliations	Y	?
eduPersonEntitlement	entitlement?	edu_person_entitlements	Y	?
eduPersonOrcid	orcid?	orcid	Y	?

Thank you

Any Questions?

nliam@grnet.gr

https://aarc-project.eu

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).