Mapping SAML attributes to OIDC Claims

- Introduction
- OIDC schema <-> SAML eduPerson mapping
- Orphaned SAML attributes

Introduction

This pages show compatible (or not) mappings between OIDC claims and eduPerson SAML attributes. Several claims have direct matches, for some claims/attributes an attribute is available, but an implementation choice must be made.

OIDC schema <-> SAML eduPerson mapping

GREEN = Good Match, YELLOW = Matchable, RED = Problems

		Strong match	**Weak match**	**Remark**
OIDC				
OIDC Scope	**OIDC name**	**eduPerson name**		
profile	sub		eduPersonPrincipalName eduPersonTargetedID /NameID eduPersonUniqueId	See 'Identifier' Claims mapping tab
	name		cn displayName	Multi value issues?
	given_name	givenName		
	family_name	sn (surname)		
	middle_name			
	nickname	eduPersonNickname		EduPersonNickname not really used (?)
	preferred_username	displayName		
	profile	labeledURI	description	labeledURI not really used (?)
	picture	jpegPhoto		jpegPhoto not really used (?)
	website			
	gender			
	birthdate			optionally: schacYearOfBirth, schacDateOfBirth, but are these used?
	zoneinfo	l (localityName)		l (localityName) not really used (?)
	locale	preferredLanguage		
	address			
	updated_at			Use SAML session info here? LDAP modify timestamp?
email				
	email	mail		
	email_verified			Can we assume an institution email with the domainname of the institution is verified?
address				
	address	postalAddress	street	
		postalCode		
		postOfficeBox		
phone				
	phone_number	mobile, telephoneNumber	homePhone	

	phone_number_verified			Can assume an institution phone nr provided by the IdP is verified? How would you know this is the IdP?

Orphaned SAML attributes

Several commonly used eduPerson attributes cannot be mapped at all. It is assumed this is not an issue for most, with the exception of the ones marked below.

eduPersonAffiliation	register at https://www.iana.org/assignments/jwt ?
eduPersonScopedAffiliation	
eduPersonEntitlement	
eduPersonOrgDN	
eduPersonOrgUnitDN	
eduPersonPrimaryAffiliation	single valued variant on affiliation
eduPersonPrimaryOrgUnitDN	
eduPersonPrincipalNamePrior	
eduPersonAssurance	used? compare with AuthnContext
facsimileTelephoneNumber	
homePhone	
homePostalAddress	
initials	
l (localityName)	
manager	
o (organizationName)	used locally
ou (organizationalUnitName)	
pager	
seeAlso	
st	
title	limited use
uid	
uniqueIdentifier	
userCertificate	
userPassword	
userSMIMECertificate	
x500uniqueIdentifier	
IsMemberOf	wide use in internal campus federations
eduPersonOrcid	