Schema Board Work Item Portfolio

Open Items

Work Item 6	Protocol specific markup
Date Added / **Date Completed**	Discussed on Schema Editorial Board Notes, 7 February 2020, Schema Editorial Board Notes, 12 March 2020
Description	Reformat the specification to include new markup that would make it easier to extract mechanically extract the examples into a protocol appropriate set
People	Proposed by Alan Buxey
Approved by the Schema Board	Given the work already under way to split the core spec from protocol-specific documents, this item is largely overtaken by events. We will mark it closed in case tools are developed in the future that might make this easier. Discussed on 24 May 2021 Schema Board call.

Work Item 8	Update the SCHAC Schema
Date Added / **Date Completed**	21 April 2021
Description	The community has identified schacGender as problematic, being very limited in definition. An informal survey went out to determine if and where this is being used. That survey indicated inquired about all SCHAC attributes. It looks like many of the attributes in SCHAC are not in common usage. The SEB should take a look at the schema overall and consider where and how it might be revised.
People	
Approved by the Schema Board	

Closed Items

Work Item 1	Change the opening paragraph in section 1.2 before the "glossary" style portion discussing identifier concepts to the following (it splits the text apart and inserts a discussion of protocol-specific IDs in the middle)
Date Added / **Date Completed**	Proposed on 28 March 2019 3 June 2019

Description	"Among the most common and useful personal attributes are identifiers. An identifier is an information element that is specifically designed to distinguish each entry from its peers in a particular set. While almost any information in an entry may contribute to differentiating it from similar entries, identifiers are intentionally designed to do this. It is common for entries to contain several different identifiers, used for different purposes or generated by different information sources. Note that while the eduPerson specification includes a number of generic identifier attribute types, it is increasingly common for individual security protocols such as OpenID Connect and SAML to define their own "standard" subject identifiers and related functionality. In some cases (e.g., SAML) this material has been explicitly informed by, and is a reaction to, problems or limitations arising from the application of the eduPerson-defined identifiers to federated authentication. In most cases, it is advisable to defer to a particular protocol's specifications to understand what constitutes best practice in that particular context. It may often be reasonable to map usage of eduPerson identifiers into a protocol, but there may be subtle differences to account for in doing so. Identifiers have a number of characteristics that help to determine appropriate usage. The following comments are offered to help clarify some points of definition for these various identifiers. These concepts are also referred to in various attribute descriptions."
People	Proposed by Scott Cantor
Approved by the Schema Board	The following change was approved by the Schema Board on the 3 June 2019 call: **1.2. Identifier Concepts** Among the most common and useful personal attributes are identifiers. An identifier is an information element that is specifically designed to distinguish each entry from its peers in a particular set. While almost any information in an entry may contribute to differentiating it from similar entries, identifiers are intentionally designed to do this. It is common for entries to contain several different identifiers, used for different purposes or generated by different information sources. Note that while the eduPerson specification includes a number of generic identifier attribute types, it is increasingly common for individual security protocols such as OpenID Connect and SAML to define their own protocol-specific subject identifiers and related functionality. In some cases (e.g., SAML) this material has been explicitly informed by, and is a reaction to, problems or limitations arising from the application of the eduPerson-defined identifiers to federated authentication. In most cases, it is advisable to defer to a particular protocol's specifications to understand what constitutes best practice in that particular context. It may often be reasonable to map usage of eduPerson identifiers into a protocol, but be aware that there may be subtle differences to account for when mapping to multiple protocols such as SAML and OpenID Connect. Identifiers have a number of characteristics that help to determine appropriate usage. The following comments are offered to help clarify some points of definition for these various identifiers. These concepts are also referred to in various attribute descriptions.

Work Item 2	Adding an Identifier Concept to the set in section 1.2
Date Added / **Date Completed**	Proposed on 28 March 2019 5 July 2019
Description	Comparison Rules Identifiers may define specific rules for comparing values, principally whether case matters in alphabetic characteristics. Historically this was not explicit in parts of eduPerson because of the conflation between rules for searching LDAP data and actual comparison of values for the purposes of unique identification. A mix of case-matching approaches can be observed across different identifiers. This is exacerbated by the fact that many applications assume case-insensitive matching, ironically as a result of an erroneous understanding of the matching rules for email addresses (which are in fact unspecified in this regard). It is, practically speaking, dangerous to rely on identifiers that require case-sensitive matching due to this fact.
People	Proposed by Scott Cantor
Approved by the Schema Board	The following change was approved by the Schema Board on the 5 July 2019 call: **Paragraph 4, Section 1.2:** Identifiers have a number of characteristics that help to determine appropriate usage. The following comments are offered to help clarify some points of definition for these various identifiers. These concepts are also referred to in various attribute descriptions. Deployers are urged to carefully consider the characteristics (e.g., case sensitivity, reassignment) for each identifier. **Subsection "Uniqueness", Section 1.2:** Unique identifiers are those which are unique within the namespace of the identity provider and the namespace of the service provider (s) for whom the value is created. A globally-unique identifier is intended to be unique across all instances of that attribute in any provider. Identifiers may define specific rules for comparing values, principally whether case matters in alphabetic characteristics. A mix of case-matching approaches can be observed across different identifiers. Many applications assume case-insensitive matching. It is therefore a security risk to rely on identifiers that require case-sensitive matching.

Work Item 3	Changing the text under "Notes" for eduPersonPrincipalName
Date Added / **Date Completed**	Proposed on 28 March 2019 29 August 2019
Description	"Values of eduPersonPrincipalName are often, but not required to be, human-friendly, and may change as a result of various business processes. They may also be reassigned after a locally-defined period of dormancy. As a result, eduPersonPrincipalName is NOT RECOMMENDED for use by applications that provide separation between low-level identification and more presentation-oriented data such as name and email address. Common identity protocols provide for a standardized and more stable identifier for such applications; failing this, the eduPersonUniqueId attribute may be an appropriate "neutral" form."
People	Proposed by Scott Cantor
Approved by the Schema Board	The following change to eduPersonPrincipalName note section was approved by the Schema Board on the 29 August 2019 call: Values of eduPersonPrincipalName are often, but not required to be, human-friendly, and may change as a result of various business processes. They may also be reassigned after a locally-defined period of dormancy. As a result, eduPersonPrincipalName is NOT RECOMMENDED for use by applications that provide separation between low-level identification and more presentation-oriented data such as name and email address. Common identity protocols provide for a standardized and more stable identifier for such applications, and these protocol-specific identifiers should be used whenever possible; where using a protocol-specific identifier is not possible, the eduPersonUniqueId attribute may be an appropriate "neutral" form. Syntactically, ePPN looks like an email address but is not intended to be a person’s published email address, or to be used as an email address. Consumers must not assume this is a valid email address for the individual.

Work Item 4	Adding a prominent note to the top of the eduPersonTargetedID definition
Date Added / **Date Completed**	Proposed on 28 March 2019 29 August 2019
Description	"NOTE: eduPersonTargetedID is DEPRECATED and will be removed from a future version of this specification. Its equivalent definition in SAML 2.0 has been replaced by a new specification for standard Subject Identifier attributes [Ref TBD], one of which ("urn:oasis:names:tc:SAML:attribute:pairwise-id") is a direct replacement for this identifier with a simpler syntax and safer comparison rules. Existing use of this attribute in SAML 1.1 or SAML 2.0, and the equivalent <NameID> Format of "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" should be phased out in favor of the new Subject Identifier attributes."
People	Proposed by Scott Cantor
Approved by the Schema Board	The following changes to eduPersonTargetedID notes were approved by the Schema Board on the 29 August 2019 call: *NOTE: eduPersonTargetedID is DEPRECATED and will be marked as obsolete in a future version of this specification. Its equivalent definition in SAML 2.0 has been replaced by a new specification for standard Subject Identifier attributes [http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd03/saml-subject-id-attr-v1.0-csprd03.pdf], one of which ("urn:oasis:names:tc:SAML:attribute:pairwise-id") is a direct replacement for this identifier with a simpler syntax and safer comparison rules. Existing use of this attribute in SAML 1.1 or SAML 2.0 should be phased out in favor of the new Subject Identifier attributes."*

Work Item 5	Adding a Notes section to the eduPersonUniqueId definition
Date Added / **Date Completed**	Proposed on 28 March 2019
Description	"For SAML 2.0 applications, it is RECOMMENDED that the SAML Attribute "urn:oasis:names:tc:SAML:attribute:subject-id" [SAML V2.0 Subject Identifier Attributes Profile Version 1.0] be used in scenarios in which this attribute might be suitable. While the syntax rules for this attribute are somewhat different from the SAML Attribute, in most cases existing values of this identifier are likely to be compatible with the SAML Attribute's rules, though the inverse is not as likely."
People	Proposed by Scott Cantor

Approved by the Schema Board	The Schema board does not accept this change at this time. Further discussion is required to determine how much SAML-specific (versus LDAP or OIDC) information should be included in the specification. This change needs to be considered in a broader context. A new release of the schema can go forward without this change. It is worth noting that allowing the SAML-specific recommendation for eduPersonTargetedId is a different situation, in that we are deprecating that attribute and guiding people to a new one, as opposed to this case where we are suggesting SAML-specific recommendation for an attribute that will otherwise remain in the specification.

Work Item 7	Expand Attribute Values
Date Added / **Date Completed**	Discussed on Schema Editorial Board Notes, 7 February 2020, Schema Editorial Board Notes, 12 March 2020 Committee was closed September 2020 - see eduPersonAffiliation subcommittee
Description	Check for some possible notes from Internet2's Tech Ex 2019. Affiliations, in particular, could use potential expansion (though maybe groups are a better way to handle the many variances of affiliation possibilities). This is something we should explore with the community to figure out what they need us to do. Some federations have done this on a federation-specific level. Board must reach out to learn more about what federations that are doing this on a local level are doing and why.
People	Proposed by Miro Milinovic
Approved by the Schema Board	Alan Buxey and Heather Flanagan will put together a schema subcommittee to discuss and come up with a proposal

Work Item 8	AcademicID
Date Added / **Date Completed**	Discussed on Schema Editorial Board Notes, 7 February 2020, Schema Editorial Board Notes, 12 March 2020
Description	Consider adding AcademicID to a schema (the way we have ORCID). Maybe this belongs in SCHAC?
People	Proposed by Miro Milinovic
Approved by the Schema Board	The Schema Board does not accept this proposal at this time. **The group consensus is to deal with requests for new unique identifiers on a case by case basis; will reconsider if we see a number of requests coming in.**