

Regionals K-12 IdPs Use Case INITIAL DRAFT Recommendation

Recommendation

The implications of the Regional R&E Network Provider (Regional) K-12 IdP use case were perhaps the most difficult to grapple with during the New Entities Working Group's deliberations. The most complex issue revolved around how to facilitate incorporating K-12 Identity Providers into the federation while protecting InCommon Service Providers from the potential impact of federal regulations regarding underage children. After much further discussion, the New Entities WG recommends that the following actions be taken to support this use case:

1. A new inCommon entity attribute should be defined that specifies that an InCommon Service Provider (SP) is [Children's Online Privacy Protection Act \(COPPA\)](#) compliant.
2. InCommon should provide a mechanism for InCommon SPs to self-assert that they are COPPA-compliant and wish to add the attribute to the InCommon metadata. The attribute will only be present in the metadata if the Service Provider has self-asserted that the site is COPPA compliant.
3. The Participation Agreement that is signed by the Regionals K-12 Identity Providers includes language that prohibits these IdPs from releasing any unique or persistent attribute about any individual who is subject to COPPA unless the SP asserts the COPPA-compliant attribute in the InCommon metadata. A bilateral contract between the IdP and SP can also be used to meet the requirement of this section 3 without the presence of the SP COPPA-compliant entity attribute.
4. MACE-DIR should be asked to define a new eduPerson attribute that can *optionally* be used by any IdP to state that the individual being authenticated is known *not* to be subject to COPPA. There are anticipated applications where this type of attribute will be useful and enable Service Providers to act differently for younger children. This group recommends that MACE-DIR consider making the optional nature of this attribute part of the definition to ensure that SPs know to always act in a COPPA-safe way unless the attribute is present. We expect that some K-12 IdPs will not have the data needed to properly assert the attribute and that others may choose to limit its use to cases where a bilateral contract is in place.

Rationale

The New Entities Working Group focused on how to best enable new types of metadata entities while protecting and minimizing the impact of the new entity types on the existing InCommon members. The question "What does an existing InCommon IdP or SP need to know and/or do if we place this new type of entity in the InCommon metadata?" was a key part of our working group's process.

1. Items #1, #2, and #3 above ensure that existing InCommon Service Providers do not unknowingly ~~start to~~ violate COPPA. For example, a service provider that accepts an authentication and then asks for name/email as part of an auto-provisioning process might violate COPPA without these provisions in place.
2. We had earlier discussed placing more requirements on the existing Service Providers to examine a new COPPA person attribute but that appeared to be problematic both for existing InCommon SPs and for ~~the new~~ K-12 IdPs which might or might not have the needed information available. The new process places all of the burden of avoiding accidental COPPA violations on the new entity Regionals/K-12 IdP operators. InCommon SPs that wish to provide services to K-12 IdPs will need to either assert the new attribute or have a contract in place with the IdP operator.
3. The request to MACE-DIR is to define a new eduPerson attribute that positively states that the individual is not subject to COPPA is to provide a mechanism for SPs to act differently when they know that they are not dealing with underage children. The group felt that the COPPA-safe attribute definition was preferable to specifically populating an attribute that said the individual is subject to COPPA.

Next Steps

The above language was developed by a subgroup - the next step is a review with both the Regionals-InC-Federation and New Entities working groups.