Use Case C1 Attribute Aggregation and Single Sign-On

Examples of Usage:

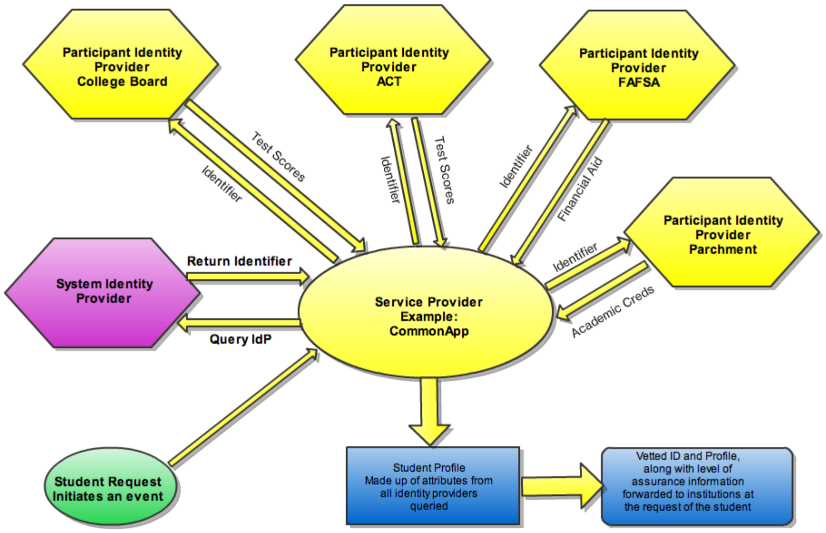
Aggregated attributes:

This system works based upon the ability in SAML to aggregate attributes from multiple identity providers into a single identity. This allows the central identity provider to keep the slimmest minimum amount of information about a student; a unique identifier, name, user name, password, and the facts about various vetting that has been done to verify a student's identity. This allows aggregation across multiple participants to build a picture of the student that is customized specifically to the event the student is trying to initiate. All participants that keep data about students will do so locally, and the only commonality will be the unique identifier provided by the central identity store. When a student logs in to any site using the system credentials, the fact of their successfully logging in will be attached to their unique identifier, which can be sent to one or many specific participant identity providers to harvest other attributes about the student. When this aggregated data arrives at a school, no matter where it comes from, it is all tied together by the matching identifier, solving data matching problems at the school. It also contains one or many instances of the student having had their credentials physically verified by officials of various participants, which will give the university some assurance of the quality of the identity, allowing for the provisioning of local university customized services.

The flow through the system at sign-on:

A student arrives at any site in the system, and is met with a log-in prompt. When the student provides their system credentials, the system identity provider is queried, and if the correct credentials are provided the identify provider will return the student's unique identifier, and possibly the details of any identity vetting that has been done, to the requesting party. The requesting party will then query any identity provider that is required to complete the transaction requested, providing the unique identifier provided by the system IdP. The participant IdP's can verify with the system IdP that the unique identifier was legitimately acquired, and will then return the enriched data about the student to the requesting party. The complete package of aggregated attributes can then be sent out to complete the operation.

Graphical Depiction of the Flow through the system at sign-on:



Participant Identity Provider College Board
Participant Identity Provider ACT
Participant Identity Provider FAFSA
Test Scores
Identifier
Identifier
Test Scores
Identifier
Financial Aid
Participant Identity Provider Parchment
Identifier
Return Identifier
System Identity Provider
Service Provider Example: CommonApp
Query IdP
Academic Creds
Student Request Initiates an event
Student Profile Made up of attributes from all identity providers queried
Vetted ID and Profile, along with level of assurance information forwarded to institutions at the request of the student