Group Members' Thoughts about the Evaluation Criteria

This page captures relevant criteria upon which External ID providers might be assessed, along with group members' comments. Its purpose was only to structure discussion of the criteria and should not be considered a final product of the work group.

*Should **Required vs. Desired vs. Optional** answers be identified separate from assertions? Note that if so, which answers are Required, etc. will vary based on which solution approach is taken.*

Desired Reponses from...	Reassign	Pwd Policies	MFA	ID Proof	Attributes	Attr Stability	Release	Consent	Consent Expr	MFA Expr	Directed vs. Static	Mission	Stability
Eric Goodman	No reuse/ reassignment ever	Ideally Silver compatible	Ideally	Varies by use case	**Required**: UserID; **Desired**: User knowable UserID; confirmed contact address	Indefinite	Ideally granular	Ideally	SAML Attribute	SAML AuthnContext (and /or attribute?)	Static preferred. In some use cases static is required.	Non-user tracking /privacy preserving is ideal	Always good
David Walker	Non-reassigned identifier available	Silver / LoA-2, but depends on use case.	Yes, but depends on use case	Depends on use case	Non-reassigned identifier, email	Documented	Documented	Yes	Documented	SAML AuthnContext (and /or attribute?)	Documented	Non-user tracking /privacy preserving is ideal	Always good
Mary Dunker	never reassign unique identifier	Comparable to Bronze or Silver - depending on use case	a desirable option	Varies by use case. Important to publish ID Proofing, if any is done	R&S attributes	Document	Document	yes - required	SAML Attribute	SAML AuthnContext (and /or attribute?)	Document	Non-user tracking /privacy preserving is ideal	Good - Document
John Breen	No reuse	Depends on use case. Silver compatible but not necessary if use case does not require.	Support Required	By use case	non-reassigned id e-mail Optional: address, first, last.	Documented	Documented	Case by case. Some attr. no consent (unique id).	SAML attribute	SAML AuthnContext (and /or attribute?)	Documented	Non-user tracking /privacy preserving is ideal	Good - provable via documentation/metrics

Legend

- **Service**: Name of External ID service provider
- **Account Management Policies**
  - **Reassign:** Policies around reassignment of accounts. Specifically, whether the "key identifier") reassigned to different users.
  - **Pwd policies:** Overview of password requirements (related to complexity, guessing resistance, etc.)
  - **MFA:** Does the vendor offer Multi-Factor support.
- **Account Identity Vetting**
  - **ID Proof:** Is there any identity proofing done by the External provider that would allow a campus to trust attributes other than Ext ID-sourced IDs (like "Account Name" and "email")
  - **Attributes:** Related to ID Proofing, what attributes are collected and how are they proofed.
  - **Attr Stability**: Stability of the External ID and attributes over time
- **AuthN Policies**
  - **Release:** Attribute release practices, including
    - What attributes are released?
    - What is the granularity of data release? (Attributes vs. bundles)
  - **Consent:** Is there a user consent process before data is released to SPs.
  - **Consent Expr**: How does the provider express that user consent was provided for release
  - **MFA Expr**: How do they express whether Multifactor has been used?
  - **Directed vs. Static**: Does the External ID provider release a directed (per SP) or static (correlatable across SPs) identifier?
- **Company Details**
  - **Mission:** Mission of the company, including:
    - Private vs. public
    - Privacy focus
  - **Stability**: Stability of the vendor and the service that the vendor offers
    - Likely this is not directly measurable, and would be more along the lines of
    - "how long in business"
    - "how long service has been operational"
    - "how many users using their IDs"
    - etc.
- **Other Concerns**
  - **EULA**: Are there terms the External provider applies that are potentially in conflict with general campus policies?
  - **Cost**: Is there a cost to the user or the organization to leverage the IDs?
  - **Audits**: What 3rd party certifications or audits are available to confirm function of service?