Evaluating External Identity Providers

This page captures relevant criteria upon which External ID providers can be assessed, along with quick assessments of major identity providers. The individual criteria are defined at the end of this page.

Service	Reassign	Pwd Policies	MFA	ID Proof	Attributes	Attr Stability	Release	Consent	Consent Expr	MFA Expr	Directed vs. Static	Mission	Stability	
Yahoo!	Yes. Accounts may be re-assigned.	Password rules are well defined. https://help.yahoo.com/kb/password-requirements-sln5681.html	Yes. Code sent via SMS or Voice.	No.	Name, date of birth, email, contacts.	Unstable. User controlled w/ little or no validation.	Some information can be made private and requires user authorization.	Consent required for 3rd party release. Some application privacy settings.	Implied through availability. Seems to be explicitly granted.	No.	Static.	Public. NYSE: YHOO Web portal, search engine, and related services.	Stable.	htt ya /le /ya /te
Facebook	"user_id" (numeric, directed identifier) is not reassigned?	Six characters. Some complexity reqt or minimal dictionary check; specifics not clear.	App or SMS.	Limited to people with large numbers of followers.	ID; Name(s); gender; locale; timezone, link (to profile); Email; Friends (that also use this App) Others; is_verified; birthdate; age_range	Many are user-managed	Release generally by bundles. Apps request groups of data.	Granular at the "bundle" level. [Some elements also controlled by profile visibility settings in FB]	Lack of consent expressed with OAuth exceptions? Receipt of data implies consent.	Not expressed ?	Directed (older APIs versions=static)	For profit; social networking.	Reasonably strong	[ht w. co /te] Sta us pr ac ide inf (ev wh ve
Amazon [1]	"user_id" - permanent and unique	min 6, max 128 case sensitive (other wise not clear)	Yes, SMS	n/a	user_id, email, name, postal_code	user_id will not change, others user managed	3 levels of release. profile ro: user_id } , profile: user_id user_id } , postal_code): postal_code}	triggered on first use with external service, always triggered for postal_code bundle		na	static	Public: NASDAQ: AMZN Online retail. Utility Computing (AWS).	Its Amazon.	ne he
Twitter	Yes, accounts can be reassigned. This depends on if they were deleted, deactivated, or suspended but it is possible. Your twitter numeric ID however does not changed.	Must be at least 6 characters. No specific requirements for special characters, capitalization, or numeric.	Yes. 2 Options: SMS Code, or challenge to Mobile App (Accept / Deny).	Limited to "highly sought after users." They "do not accept requests for verification from the general public".	Username, Language, TimeZone, Short Bio, Location, Website Link, Profile Photo, Verification Status,	Unstable. User controlled w/ little or no validation.	Bundled.	Controlled through application privacy settings. All or nothing / followers only.	Implied through availability.	No.	Static.	Public. NYSE: TWTR Social Networking. Micro blogging.	Stable.	htt r.c
LinkedIn	Depends. Login is based on e-mail address which can be changed. They have a targeted identifier which does not get re-assigned.	Must be at least 6 characters. No requirements for special characters, capitalization, or numeric. Recommendations are made.	Yes. Code sent via SMS.	No.	Depends on privacy settings but many are available: id, first name, last name, email, location.	Unstable. User controlled w/ little or no validation.	Bundled.	Controlled through application privacy settings.	Implied through availability.	No.	Static.	Public. NYSE: LNKD "Professional" Social Networking.	Stable.	htt .lin co /us ag

Microsoft	If account is closed, email address or user name (not the Microsoft account itself) may be recycled and assigned to another user.	User can opt to force password change every 72 days. passwords 8-character minimum, case sensitive. May not reuse last password.	Phone app, Text msg. or phone call for accessing sensitive account information such as password change. Two step verification can be set up when signing in on a new device. Security code to app, phone or alternate email address.	None, except to verify control of 3rd party email address.	Display name; Birthdate; Gender; Country/region; Time zone; email address; telephone/text	User controlled	Bundles. Varies depending on service being accessed.	Subject to privacy practices for each app accessed.	Implied through availability.	?	Static	Public: NASDAQ: MSFT designing, manufacturing, selling devices, and online advertising to a global customer audience.	Strong	htt ws mi co /wi /m se ag

Note: Google, Google Apps for Education, and UnitedID were originally intended to be assessed but were not, due to time restrictions.

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?

References

Twitter

https://support.twitter.com/articles/101299-why-can-t-i-register-certain-usernames#

https://support.twitter.com/articles/14609-changing-your-username#

https://www.schneier.com/blog/archives/2013/08/twitters_two-fa.html

https://support.twitter.com/articles/119135-faqs-about-verified-accounts#

LinkedIN

"we do not have a reliable system for identifying and counting duplicate or fraudulent accounts"http://investors.linkedin.com/secfiling.cfm?filingID=1271024-14-34

https://developer.linkedin.com/documents/profile-fields

Yahoo

https://developer.yahoo.com/yql/guide/authorization.html

https://developer.yahoo.com/faq/#permission

Microsoft

Microsoft Account Home