# External Identities Working Group Report

(Final Release 5/27/2015)

**Table of Contents**



---

## Executive Summary

Integration of External Identities into internal systems, either single Service Providers or institutional identity and access management systems, can afford multiple benefits, for example:

- Leverage users' existing Identities, obviating the need for assignment of Internal Identities.
- Allow users the convenience of using Authenticators they already have.
- Associate additional Authentication Mechanisms with Internal Identities for use in situations requiring a lower or higher level of trust than is provided by internal Authentication Mechanisms.
- Provide mechanisms for reset / recovery of internally-issued passwords.
- Outsource management of Authenticators (e.g., passwords). For many populations, this may be the largest benefit.

This is the final report of the External Identities Working Group, formed in August of 2014 by the InCommon Technical Advisory Committee to examine these benefits and "...move the community of knowledge towards the goal of making external identities useful and sufficiently trusted in a variety of campus-based use cases."

We open with definitions of common terms used in discussion of External Identities and then characterize updated use cases from the previous Social Identities Work Group along three dimensions: scope, longevity, and risk.

We then address the trustworthiness of external identities as it relates to the trustworthiness of internal identities. There is no hard line between what is be considered "internal" or "external;" it must be determined from the point of view of the relying party, and the same is true when determining trustworthiness. For a specific identity, trustworthiness is determined by a number of criteria, possibly including formal assurance profile certification, which apply to both external and internal identities. We provide risk assessment criteria that should be considered for both internal and external identities. We also discuss strategies for enhancing trustworthiness by linking external and internal identities.

The next section addresses architectural patterns and infrastructure elements required for various uses of external identities, before we close with a list of business and technical criteria to be considered when selecting an External Identity Provider.

---

# Defining Some Terms

## Identity

An Identity is a collection of information about a person, generally within the context of some organization (an application, a university, Google). That collection may or may not be associated with one or more Authentication Mechanisms.

### Internal vs. External Identities

Internal Identities are those that are managed by your organization, while External Identities are Identities that are not managed by your organization. Which Identities are considered Internal vs. External will depend on the nature of your organization:

- An Service Provider operator at a campus may consider campus Institutional Identities as Internal Identities because of a close trust or operational relationship.
- Campus Service Providers operated by vendor under contract may consider ALL Identities to be External Identities.
- Some Service Provider operators may consider all Identity Providers within a federation or an entity category as providing Internal Identities.

### Common Types of Identities

- Internal Service Provider Identity
    - An Identity that is managed within a single Service Provider. It is known only within the Service Provider, and any linking to other Identities is done by the Service Provider. This Identity would always be considered an Internal Identity.

- Institutional Identity
    - An Identity that is managed within the local institution's identity and access management system. Frequently considered Internal Identities by Service Providers operated by the same institution. Identities tracked internally by virtual organizations are also Institutional Identities, although virtual organizations are likely to leverage External Identities and identity Linking to a greater degree.
- Federated Identities
    - A federation is a group of providers that agree upon a standard of operations, interactions, frameworks, goals, etc. This federation can be point-to-point or via a formal federation framework (such as the InCommon Federation in the U.S.) This is the type of Identity most familiar to academic institutions, and is often considered an External Identity.

- Social Identities
    - There are many social networking sites, the most popular include: Facebook, Google, and Twitter. These providers offer users self-service creation of Identities, which can then be used to access other services. For the purposes of this document, these are almost always considered External Identities.
- Other Commercial Identities
    - We are starting to see providers getting into the business of providing strong identity services. PayPal and Verizon are examples of this. Also, organizations like UnitedID are starting to provide strong authentication services, although perhaps with weaker identity proofing and registration.

## Attributes

The individual pieces of information maintained about a person are often referred to as Attributes. Typical Attributes are name, electronic mail address, affiliations, group membership, entitlements, in addition to those used specifically as Identifiers (see below). Multiple organizations may store Attributes, according to each organization's needs, describing the same individuals. These Attributes can be duplicative, complementary or in conflict across different organizations.

## Identifier

Identifiers are Attributes that uniquely reference an Identity. Such Identifiers may be globally unique, or they may be unique only within the scope of the administering organization. Also, it is possible for an Identity to have multiple associated Identifiers. Examples include:

- eduPersonPrincipalName
- UID
- eduPersonTargetedID

In many ways, Identifiers are just Attributes with specific properties. Identifiers are called out in this document for two reasons:

- They are required for effectively Linking Identities (see below)
- Some identifiers are "directed" or "targeted", and have special implications for Linking.

“Directed” or “targeted” Identifiers are scoped to specific Relying Parties, so that different Identifiers are presented to different Relying Parties for the same Identity. Such Identifiers are generally intended to inhibit correlated tracking of user activity across Relying Parties. Support for targeted Identifiers will vary from provider to provider. For example Google provides a single Identifier that is asserted to all Relying Parties, while Facebook and LinkedIn Identifiers are targeted/directed and so are specific to the Relying Party receiving the assertion.

## Authentication Mechanism

A mechanism used by an Identity Provider to determine who the current user is, such as verification of username and password or proof of possession of a software or hardware token. Different Authentication Mechanisms may mitigate more or different risks and so are appropriate for different circumstances.

Identities are not required to have associated Authentication Mechanisms. For example, organizations have traditionally managed Authentication Mechanisms for their Institutional Identities, but it is possible to Link Identities to enable users to leverage their External Identities’ Authentication Mechanisms for their Institutional Identities. This is often referred to as “Bring Your Own Identity.”

Assertions may not communicate all relevant details of the mechanism used to authenticate an individual, even when supported by the protocol. Unless specific conventions are defined and followed, the Relying Party may have no way to determine specifics of the actual authentication events.

## Authenticator

An Authenticator is something a person can use to prove control of an Identity electronically through use of one of the Identity’s associated Authentication Mechanisms. The strength of that proof is dependent on the Authentication Mechanism, issuance and management practice, identity proofing practice, among other factors. Examples of Authenticators are:

- username/password pairs
- software or hardware tokens
- thumbprints

The term “Authenticator” in this document is used similarly to the definition of the term “Credential” in the InCommon IAAF 1.2 and the term “Token” in NIST 800-63-2.

## Linking

External Identities can be used by themselves to grant access to services or they can be Linked to Internal Identities. Linking establishes a mapping from an Attribute asserted by an External Identity provider to an Internal Identity. This allows a Relying Party to leverage the External Identity’s Attributes, its Authentication Methods, or both, and also to supplement that information with Attributes (e.g., campus affiliation) and Authentication Methods (e.g., MFA) managed for the Internal Identity. This can be done to outsource the management of user passwords, to provide convenience for the end user, or to acquire Attributes describing the user from the External Identity. The use cases and implications of such linkages are discussed in greater detail in later sections of this document.

## Identity Provider

An Identity Provider is a network service that asserts identity information about the community of people it represents. While “Identity Provider” has a specific meaning for specific protocols, such as SAML, we use this more general definition in this document, unless noted otherwise.

## Service Provider

A Service Provider is a network service that provides services to people. As with Identity Provider, this document does not use a protocol-specific definition of Service Provider, unless noted specifically.

## Relying Party

A Relying Party is a network service that receives identity information from an Identity Provider. An Relying Party may be a Service Provider, an Identity Provider or both (in the case of “gateway” implementations).

---

# Characterizing External Identity Use Cases

The work group began its work by examining several use cases, many of which had earlier been identified by the Social Identities Working Group. Those use cases have been collected in the External Identities Working Group’s wiki space.

While there are many use cases, they can be categorized along the following dimensions, which in turn affect the criteria that an institution should consider in evaluating sources of External Identities.

- Scope: Linking to a single Internal Service Provider Identity vs. an Institutional Identity
- Longevity: Longevity of the Linkage to an External Identity
- Risk: Risk associated with use of the External Identity

The following sections discuss each of these dimensions in greater detail.

## Linking to an Internal Service Provider Identity vs. an Institutional Identity

External Identities can be linked with a scope limited to a single Service Provider, or linked broadly within the institutional Identity and Access Management (IAM) system making them available to multiple Service Providers. The choice between these two scenarios will be made on the basis of issues such as resource allocation, policy, and organizational responsibility. Note that there is not always a clear line between these two scenarios, as campus IAM systems may offer identity services for local Service Providers without formally adding the Service Provider's users to the IAM system itself. Examples of each approach include:

- Linking to Internal Service Provider Identity:
  - A wiki can link a Social Identity administered by Google to its Internal Service Provider Identity (user record), allowing the user to login with a Google username and password. The wiki can also acquire the user's name and electronic mail address from this Identity.
- Linking to Institutional Identity:
  - A campus can create Institutional Identities for its students' parents and link those Identities to Facebook Social Identities to avoid the need for administering parents' passwords.
  - A faculty member could link a UnitedID Identity to her Institutional Identity to enable password resets with UnitedID's multi-factor authentication.

## Longevity of the Linkage

Some use cases involve "one shot" relationships between a relying party and the user, often because the service itself is very short-lived (e.g., authentication for WiFi at a conference). If the service is used on more than one occasion by the same person, it is not necessary to correlate those occasions or recover state from earlier uses of the service. In this case, the External Identity does not need to be stable over time; Identifiers and Attributes can change without serious impact on the relying party. Also, the External Identity Provider can re-assign Identifiers to other people, as the relying party will not confuse the new user with some previous user who used the service earlier.

If the use case requires maintenance of information about people over time, however, then:

- The stability and re-assignment of the External Identities must match the use case's need for longevity.
- Criteria such as password and MFA key management practices may also rise in importance, depending on the associated risk of the use case.
- The stability of the company/organization acting as the External Identity Provider should be considered, to avoid users needing to reclaim their user records from another Identity.

## Risk Associated with the Use of the External Identity

There are multiple risks to an authentication event. For example:

- User passwords and other Authenticators can be shared, lost, or stolen, either through technological means, or by users themselves.
- The authentication process may fail to return the correct user due to various threats, such as man-in-the-middle attacks.
- The person who has been issued an Authenticator may not be the person he or she claims to be.
- The mechanism or assumptions used by the External Identity provider (session length, etc.) to authenticate the user may not meet the criteria that the Relying Party would prefer.

The impact of these risks on a particular use case must be considered to determine the importance of the following criteria when selecting External Identity Providers:

- Password policies
- Support for multi-factor authentication (MFA) and the ability to determine if MFA was used for the current authentication event
- Identity proofing practice and the ability to determine what identity proofing practice was applied for the current user
- Operational and business practices, including audits and certifications

It is also possible to apply other mitigations at the local level to address potential concerns of External Identity use. For example:

- Device fingerprinting using an Internal Identity / account
- Combining with local (rather than External Identity Provider) MFA authentication

## A Note about Non-Web Protocols

While much of this document comes from the perspective of web-based protocols, no actual dependency on specific protocols should be assumed, unless specifically noted. Many non-web protocols, however, are not capable of supporting arbitrary external Identity Providers.

## Use Cases That Do Not Involve Authentication

The work group did not consider use cases that are not associated with authentication events. There are, however, use cases involving attribute exchange at other times. For example, a Relying Party may retrieve information from an LDAP directory even at times when there is no active user session. Another example could be use of an ORCID; an asserted ORCID may need to be linked to or looked up from an external ORCID resolver in ways that would not necessarily involve interactive user authentication during the lookup .

We leave such cases and the trust relationships that must exist between the Identity Provider and the Relying Party for future study.

# Trustworthiness of External Identities

Historically, campuses have been hesitant to build their IAM infrastructure with a strong dependence on External Identities. On the other hand, there have also been arguments made that it is a reasonable approach to leverage External Identities in conjunction with Institutional Identities, where the External Identities can be seen as “External Authentication Mechanism Providers”. Some External Identity Providers may be more likely to detect and respond to compromised Authenticators than a local IT staff would be able. Relying on such Identity Providers’ Authentication Mechanisms, instead of a local password store, could actually be a net security improvement.

In this section, we will discuss issues related to the trustworthiness of External Identities.

Trust in authentication and Attributes from any Identity Provider (internal or external) is based on a number of factors, such as identity proofing practices or Authentication Mechanism strength. (See the “Criteria for Evaluating Identity Providers” section for a more complete list.)

Not all factors are pertinent for all relying parties, but those that are should be considered for both Internal and External Identity Providers. Internal providers will generally be acceptable across all of these factors, but not always, particularly for high-risk services. External providers will generally be more variable across their strengths and weaknesses.

Social providers, for example, may have strong authentication technologies, but weak identification and registration practices. They may have highly mature operational and security practices, but the policies and business practices may lean toward monetization of the information they can collect from authentication events. They may do regular audits, but they may not provide the results of those audits to users, and there may be no legal agreement beyond a click-through agreement with the end user, not the institution.

The appropriateness of Attributes from external providers should be assessed with the same care put to determining the requirements for business processes and technology to support internal Attributes. They may be treated as authoritative information, default values to be updated later, or disregarded entirely.

## Using Information from Multiple Providers to Increase Trustworthiness

It may be possible to leverage information from multiple Identity Providers to increase trustworthiness. For example:

- An external provider that supports multi-factor authentication, but weak identification and registration practices, can be linked to Institutional Identities with an appropriate registration process to enable multi-factor authentication for the institution.
- A distributed institution with difficulty implementing strong identification practices for geographically distant members of its community can contract with an external Identity Provider with strong identification practices and link those external identities to its Institutional Identities.

## External Authentication Mechanisms and Account Recovery

When leveraging External Authentication Mechanisms to control access to internal resources the perceived or measured trustworthiness of the External Identity may impact practices around account recovery, especially where External Authentication is leveraged to initially create Institutional Identities; e.g., for generating applicant or other “affiliate” level identities.

When creating institutionally managed Authenticators, a campus will typically perform sufficient identity verification during the user onboarding process to be comfortable managing account recovery processes. When individuals have institutionally managed Authenticators, any authentication leveraging Linked External Identities is largely provided as a user convenience. If the externally managed Authenticator is compromised or lost, the institution can unlink any lost External Identities and use internal Authenticators to authenticate the user sufficiently to re-establish links to additional External Identities.

In cases where Authenticators exist only associated with a user’s External Identity, and no separate verification of the user’s identity is done, the Institution or Relying Party has no information to map the real world individual to her Internal Identity. If she loses access to her external Authenticator, and thus cannot assert her External Identity, the process an institution supports to allow her to regain access to her Internal Identity may be impacted. Questions to consider in these cases include:

- Does the institution trust the External Identity’s Attributes sufficiently to perform its own local “identity proofing” or “External Identity re-linking” against the asserted Attributes as part of an account recovery process?
- If not, what additional user verification must the Institution manage locally for purposes of allowing future account recovery?

---

# Architectural Patterns for Integrating External Identities

In this section, we will describe architectural approaches to integrating External Identities for Relying Parties.

This section describes approaches to implementing External Identity integration. Many of the options listed support some form of “offloading” of elements of the integration from Service Providers onto dedicated institutional IAM services. These services can be implemented in a standalone manner that the Service Providers can invoke directly, they can be deployed via separate “gateway” or proxy services that sit between the application and External Identity Providers, or they can be integrated directly (and typically transparently) into the campus IAM system. As of this writing it is most common to see these functions made available via standalone gateways.

The term “gateway” implies a separate appliance, but any of these gateway functions can also be built into the native IAM infrastructure.

For clarity, each function will be discussed distinctly to call out its specific pros and cons. However many of these services can be, and in practice are, provided together in the same service.

Detailed technical evaluation of each architectural element, such as specific implementation and configuration details, is beyond the scope of this workgroup, but could be a useful area of focus for future workgroups.

## No IAM Services/Direct Integration with External Identities

The most direct approach to integrating with External Identities is to put support for those Identities and providers directly in the Relying Party. The Relying Parties directly connect to/authenticate against External Identity Providers.

- Pros
  - No central infrastructure needed
  - Relying Party has full control over behavior of integration.
  - More direct control by the user of release of data to specific resources.
- Cons
  - Relying Party responsible for all aspects of integration
  - All integration work is scoped to the Relying Party; integration with other Relying Parties must be done independently.
  - Targeted Identifiers will differ across Relying Parties
  - Relying Party responsible for adherence to institutional security policies which may be more stringent than External Identity Providers adhere to

## Protocol Translation

Protocol Translation services provide a gateway or proxy to allow the Relying Party to communicate with External Identity Providers without using the same protocol as that External Identity Provider. The most common current use case is to support a SAML/Shibboleth Service Provider connecting to an OAuth External Identity Provider.

- Pros
  - Simplifies the communication to External Identity Providers for Relying Parties that are configured for a single protocol.
- Cons
  - There can be some loss of functionality or change of semantics from the original protocol in the translation.
  - Protocol translation may not maintain the same fidelity of information (ie data may be absent or ambiguous like multiple email addresses or multiple common names)

## Attribute Mapping

Provide a service to map Identifiers from External Identity Providers into Attribute names and formats that are already known to the Relying Party.

- Pros
  - Relying Party can continue to use familiar Attributes.
  - Shields Relying Party from per-External Identity Provider interpretation issues
- Cons
  - There can be some change of semantics from the original values, due to differences in the protocols, or because the External Identity Provider may have been interpreted and implemented differently. Expected behaviors from original vs. mapped Attributes may not be completely compatible.

## Shared Relying Party Proxy

The Shared Relying Party Proxy approach advertises a single Relying Party entity to the External Identity Provider. By having multiple Relying Parties behind a single proxy, they appear to be one Relying Party to External Identity Providers. Many use cases combine this approach with the institutional account linking service described in the next section.

- Pros
  - Creates a common Identifier in cases where Directed Identifiers are used (e.g., with Facebook or LinkedIn).
  - Prevents tracking of user “on campus” behavior by External Identity Provider.
  - Can provide a common “look and feel” for integration with External Identity Providers.
  - Allows for central monitoring for misuse or compromise of External Identities in a way that is easier than when using the direct integration approach.
- Cons
  - All Relying Parties behind the same endpoint are subject to the same, collective API call limits.
  - Release consent screen from the External Identity Provider will not provide granularity (or perhaps clarity) to user for release consent to specific Relying Party.
  - May be contrary to the Identity Provider’s or federation’s business models by hiding from the External Identifier provider the specific resource(s) being accessed.
  - Attributes released by the External Identity Provider to the Shared Relying Party need to be the union of all attributes needed by all proxied services. The Shared Relying Party is also in control of release of External Identity data to internal Relying Parties.

## Institutional Identity Linking

The IAM can manage account linking between External Identities and Institutional Identities. By itself this service extends the IAM services to allow a user’s External Identities to be linked to the Internal Identities directly, so that given an External Identity a Relying Party can find the appropriate Internal Identity and pull identity information from that Identity.  This pattern is common for virtual organizations.

While such a service could be deployed individually, all cases we’ve seen have combined it with the “Shared Relying Party Proxy” approach listed above.

- Pros
  - Supports the concept of “Bring Your Own Credential”, allowing a user to use an External Identity’s Authentication Mechanism to authenticate their Institutional Identity.
  - Allows Relying Parties to share the same External Identity mappings
- Cons
  - All Relying Parties are subject to the same, collective API call limits
  - A second release consent prompt (separate from the one managed by the External Identity Provider) may be required to allow release of Internal Identity information.
  - In some cases, potential confusion for user/service if a user has the choice to authenticate with an External Identity directly vs. an Internal Identity that is linked to an External Identity.

## External Authorization Services

A rapidly evolving best practice for managing authorization or at least some portion of application authorization is to externalize it into its own service. Commonly this will be done with a service such as Grouper that has its own interface for assigning entities to permission groups.

- Pros
  - Allows a common process for authorization management for both Internal and External Identities.
  - Dedicated authorization systems can support more complex permission management processes than is likely available within a given application, including approval workflows and integration of institutional data sources (HR, SIS).
- Cons
  - All Relying Party are subject to the same, collective API call limits
  - Release consent screen from the External Identity Provider will not provide granularity (or perhaps clarity) to user to permit data release to specific Relying Parties.

The pros of an authorization service are not at all specific to External ID use cases, and can be used for authorization management even when External IDs are not supported. Externalized authorization services are called out because it is a commonly considered approach for managing permissions of External Identities across an institution, especially for “lightweight” or “authorization only” identities that do not have distinct “person” identities in the campus’ IAM system.

## Invitation Services

Invitation Services provide a provisioning workflow to provide access and specific permissions to an External Identity holder. A common use case is to allow students to authorize (invite) their parents to view specific parts of the student’s record (e.g., outstanding balance). The invitation service provides an interface to identify who to invite (a link to the parent’s External Identity) and what permissions to provide the invitee (“view bill”) . The invitation service orchestrates the notification to the invitee, creates any necessary Internal Identity or authorization information, registers the linkage of the External Identity to the Internal Identity and/or authorization information.

- Pros
  - Allows management of permissions in advance of a new user having an Identity on the Relying Party.
  - Allows the “inviter” to identify the “invitee” using known Identifiers (e.g., email address) that may not be part of the final identity assertion for that person.
    - E.g., allows an invite to be mailed to a known email address rather than associated with an unknown and unguessable targeted Identifier.
- Cons
  - New users may not be able to request services directly. They must be invited.

The invitation use case is in contrast to the “Just In Time” or “front-channel” provisioning model, where a system is configured to create an Internal Identity on-the-fly using the Identifier and identity Attributes provided in an authentication assertion. It also contrasts with “back end provisioning”, where provisioning is done out of band and is typically driven by independent business rules.

---

# Criteria for Evaluating Identity Providers

The following criteria were identified by the Working Group as important for assessing External (or Internal) Identity Providers. The relative importance of individual criteria, of course, will depend on the specific use case.

Informal assessments of common External Identity Providers can be found on the External Identities Working Group wiki space: Evaluating External Identity Providers.

## Account Management Policies

- Policies around reassignment of accounts. Specifically, whether the "key” Identifier can be reassigned to different users.
- Password requirements (related to complexity, guessing resistance, etc.)
- Does the vendor offer Multi-Factor support?

## Account Identity Vetting

- 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")
- Related to ID Proofing, what Attributes are collected and how are they proofed.
- Are identities re-vetted periodically?
- Stability of the External ID and Attributes over time

## AuthN Policies

- Attribute release practices, including
    - What Attributes are released?
    - What is the granularity of data release? (Attributes vs. bundles)
- Is there a user consent process before data is released to Service Providers.
    - How does the provider express that user consent was provided for release
- How do they express whether Multifactor has been used?
- Does the External ID provider release a directed (per Service Provider) or static (correlatable across Service Providers) Identifier?

## Operational Concerns

- Protocols supported, including mobile and other non-web protocols
- Protection of Authenticators
    - Are Authenticators protected from disclosure or inspection by any entity other than the Identity Provider or the end user?
- Privacy practices
- Incident response practices
- Reassigned IDs
- Degree to which users “churn” through External Identities
- Global vs. Targeted/Directed Identifiers

## Company Details

- Mission of the company, including:
    - Importance of and motivation for providing quality identities
    - Commercial vs. non-commercial
    - Privacy focus
- Certifications maintained by the company
    - InCommon or FICAM Levels of Assurance (LoA)
    - Industry standard audits
- 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"

## Liability and Legal Concerns

- Indemnification
- State-specific issues for public institutions
- Licensing
    - Impacts on user population
    - On the institution
        - What if licensing model changes? (No proxying?)
    - Concerns about for-profit (e.g., charge per login) models in the future
- Impact on Security and IT audits

## Other Concerns

- Are there terms the External provider applies that are potentially in conflict with general campus policies?
- Is there a cost to the user or the organization to leverage the IDs?
- What 3rd party certifications or audits are available to confirm function of service?
- API limitations (number of allowed authentication per unit time)

---

# Conclusion

Integration of External Identities into internal systems can afford multiple benefits. These benefits do not come without a cost, however: The trustworthiness and other aspects of External Identity Providers’ operations must be assessed, and the External Identity Provider’s technology must be integrated into the local system.