Account Linking Approaches with Risks

DRAFT

The information on this page is DRAFT. In the end this information was presented in a different format in the workgroup's final report, but this page is left in tact as a record of some of the discussions that led to the information in that final report.

This page summarizes approaches that have been discussed within the workgroup for performing account linking between an *Internal IdP* (e.g., campus-run) and an *External IdP* (run by a third-party) IdP.

Definition: External IdP

An *External IdP* is an IdP that is run by a different organization than the one that runs the campus IdMs; *External IdPs* create and manage identities outside of a campus' direct control. *External IdPs* may provide assertions via SAML or other protocols. Some examples of *External IdPs* for purposes of this discussion include:

- An OAuth/OpenID Connect authentication service provider such as Google or Facebook
- A SAML IdP run by a partner institution
- An IdP Proxy that performs as a SAML-to-OAuth/OpenID Connect gateway (such as the InCommon gateway service)
- An IdP Proxy that performs as a SAML-to-SAML gateway but that generates assertions based on data from "backend" IdPs that are run by external institutions.

Solution Summary

This section gives a very brief outline of the solution approaches. Later sections investigate each solution in detail.

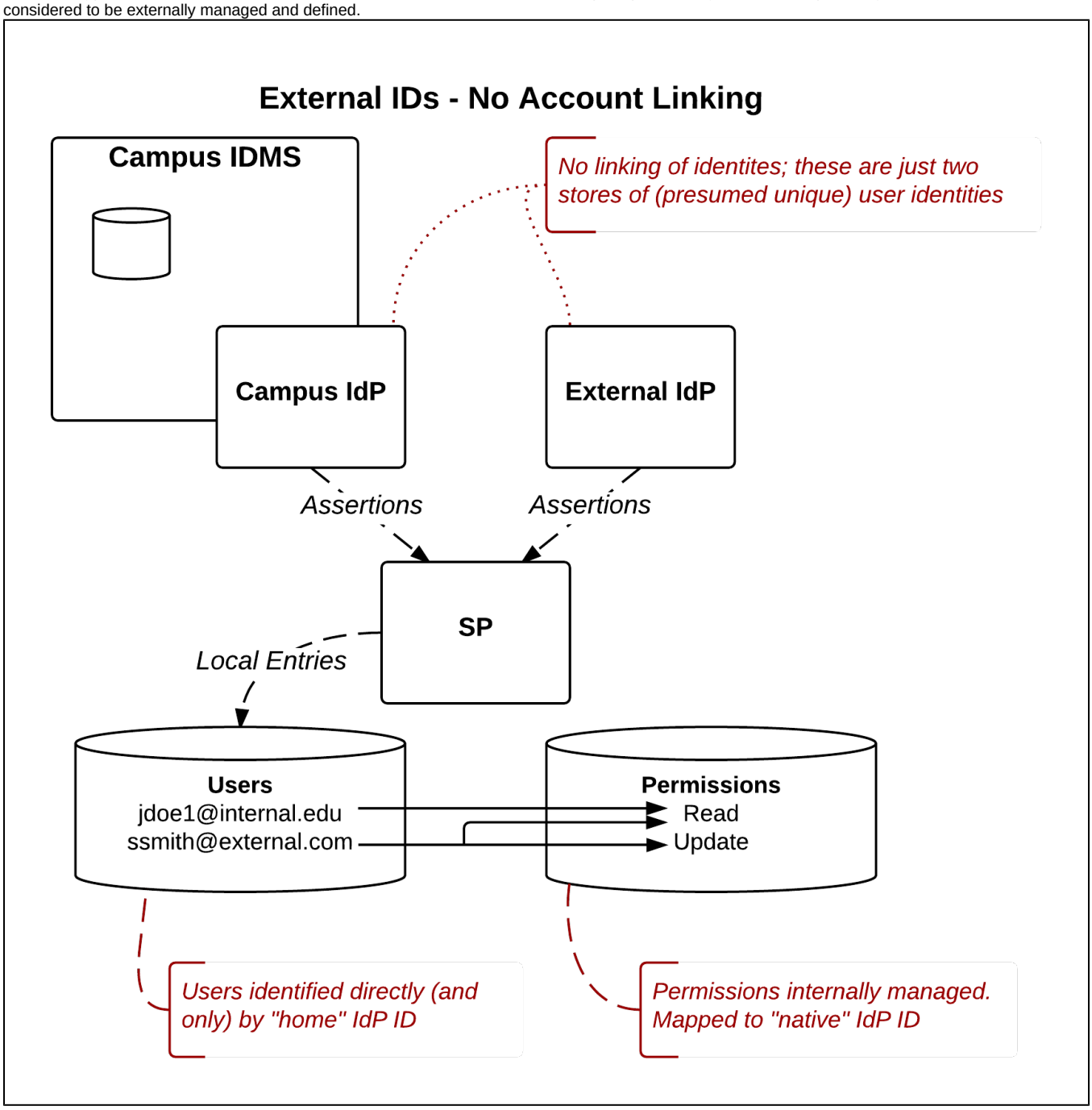
1. **No Account Linking**
   - This describes the currently-typical federation case, where external identities are allowed access to systems, but they are not linked to internal identities in any way. From an Account Linking standpoint, this is a "no support" use case. Note however that several External ID use cases can still be supported, even with no support for account linking.
2. **Account Linking at the SP**
   - In this model, the campus/internal IdMs is unaware generally of the fact that linking is taking place. The SP takes full responsibility to tracking the linking of an External ID (an ID asserted by and in scope of an *external IdP*) to an internal user identity, and linking identities in one SP does not link the identities in another IdP.
3. **Trusted External IdP**
   - In this model, an IdP operated by an external entity is authorized to assert IDs or attributes that are conceptually *internal* IDs of the campus IdP. An External IdP that is allowed to release a "campus Alumni ID" describing the user would fall into this category.
4. **Account Linking at the IdP**
   - In this model, the IdP itself manages the linking of external IDs to internal users. This model hides the fact that an External ID (or external credential) was used from SPs, allowing users to use internal and external credentials interchangeably. It also allows for "Bring Your Own Credential (BYOC)" support with no need for the SPs to perform customized support of account linking.

Solution Details

Approach 1:No Account Linking

Model Description

This is the typical "federation with an external IdP" use case. External IDs are accepted (asserted by External IdPs), but any IDs or attributes asserted are considered to be externally managed and defined.



Responsibility Assessment

- Who does account linking? *N/A*
- Who merges account attributes? *N/A*
- Who authenticates and handles attribute release? *External IdP (for External Ids*)
- Who decides whether a given external ID source is trusted? *SP*

Pros

- Lightweight for SPs, in that they get all external information they need directly from the IdP asserting an identity.
- Only "policy" or negotiated agreement required between SP and External IdP is data release.
- LoA concerns entirely outsourced.

Cons

- Does not provide account linking.

Supported Use Cases

This model can support the following External ID Use Case Categories:

- Anonymous
- Open Affiliates
- Non-business affiliates
- Ad-hoc personal affiliates
- Inbound Affiliate (somewhat)

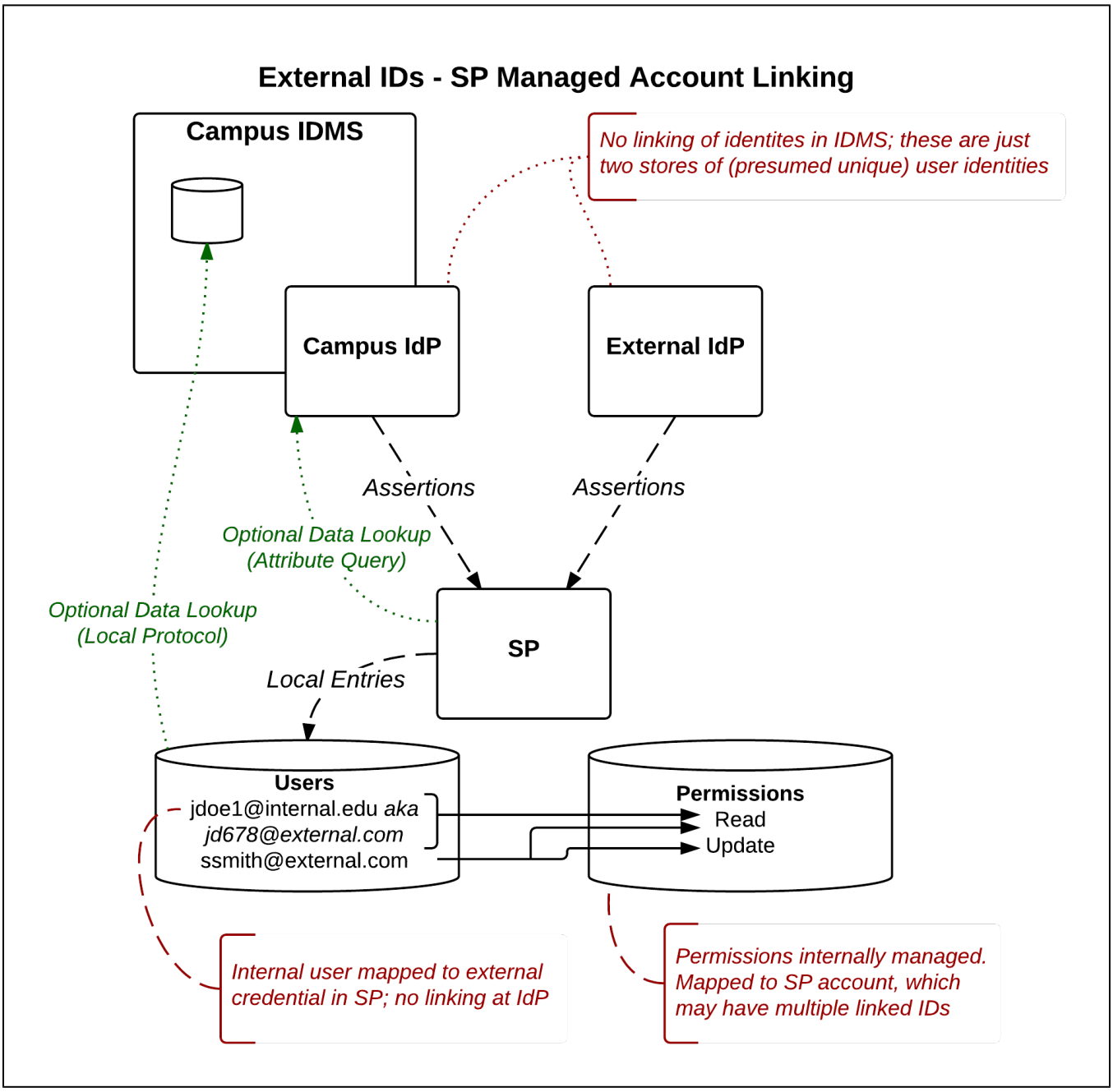
Discussion

While permissions may be granted based on attributes provided in such an assertion, those attributes are still considered to originate from an external source/authority and not to define characteristics of an "internal" person. E.g., eduPerson(Scoped)Affiliation may be used to drive access decisions, but it's clear that a "Student" affiliation asserted by an External IdP describes a "Student" affiliation outside of the campus; external IdPs asserting a "Student" affiliation are not asserting a student *at the local institution.*

Approach 2:Account Linking at the SP

Model Description

In this model, the linking of accounts is handled internally at the SP. The campus/internal IdMs is unaware of the fact that linking is taking place.



Responsibility Assessment

- Who does account linking? *SP*
- Who merges account attributes? *SP*
- Who authenticates and handles attribute release? *Internal IdP/IdMS (for internal attributes)*
- Who decides whether a given external ID source is trusted? *SP*

Pros

- Lightweight for IdMSs; allows SPs to "trailblaze" such a service.
- Implicitly supports selective (on the part of the user) account linking. E.g., "link my IDs for app 1, but not for app 2"

Cons

- User must link identities for each SP individually
- Each SP must create and follow a process for account linking/LoA management.
  - Risk that some SP linking processes will be inadequate, especially if internal and external accounts are at different LoA levels.
- To rely on campus IdMS identity data, SPs must implement additional IdMs lookups
  - Increases workload on the IdMS to access current data

    - Increases risk SP may rely on outdated identity data (if additional IdMS lookups are not implemented)
    - Impacts user release consent, as user consent at the (external IdP) does not limit the amount of information available to the IdP.

Supported Use Cases

This model can support the following External ID Use Case Categories:

- Non-business affiliates
- Business affiliates
- Inbound affiliates
- Outbound affiliates
- Alternate factor (possibly)

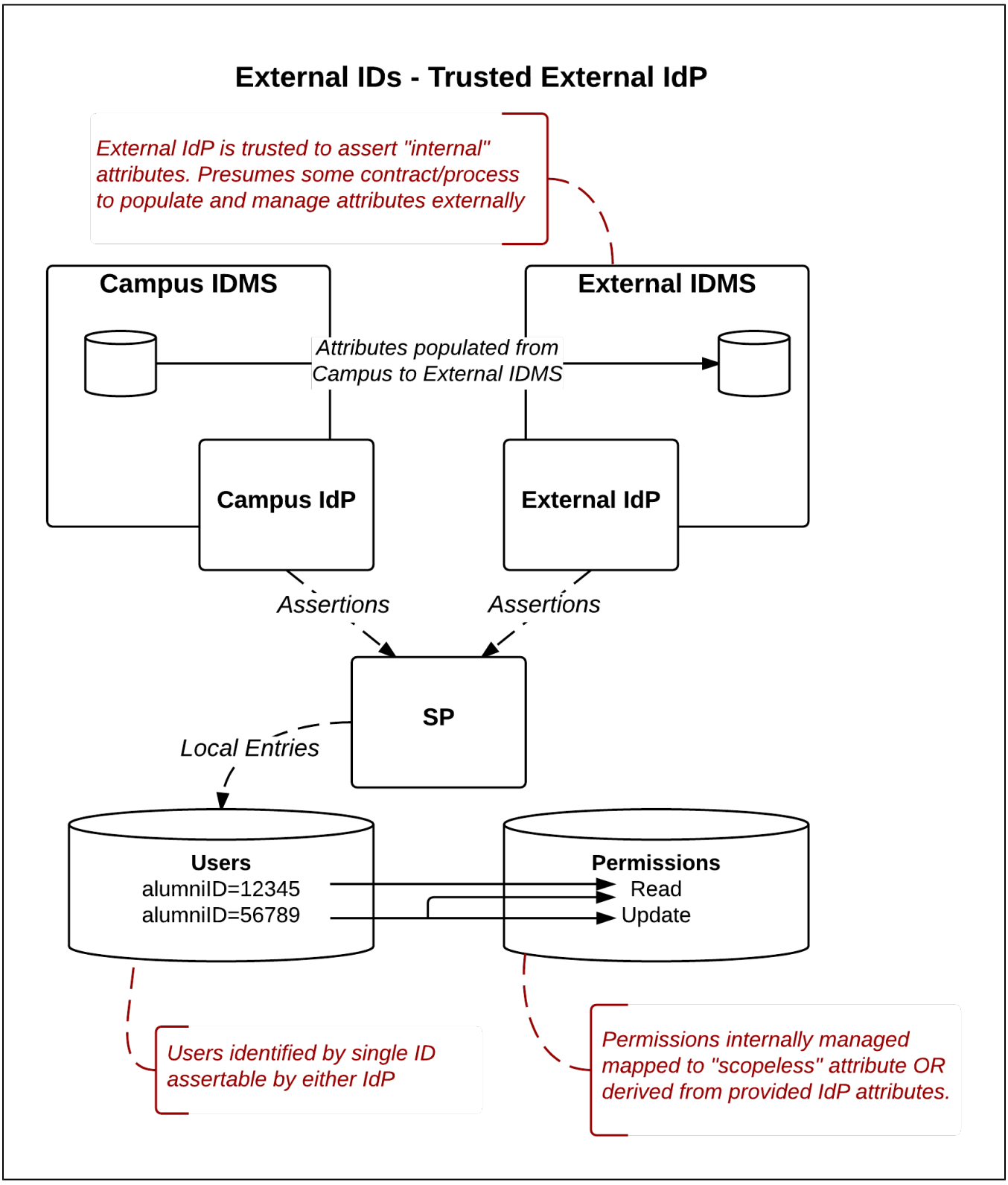
Discussion

Placeholder

Approach 3:Trusted External IdP

Model Description

In this model, an IdP operated by an external entity is authorized to assert IDs or attributes that are conceptually *internal* IDs of the campus IdP. An External IdP that is trusted to release a valid "Student ID" in support of an alumni service (see Use Cases from External ID Workgroup Discussion, alumni use case) would fall into this category.



Responsibility Assessment

- Who does account linking? *External IdP*
- Who merges account attributes? *Internal IdP and External IdP*
- Who authenticates and handles attribute release? *External IdP*
- Who decides whether a given external ID source is trusted? *SP*

Pros

- Lightweight for SPs
- Lightweight for IdPs
- Outsources technical LoA concerns (proofing still an internal IdP concern)

Cons

- Requires some agreement (likely contractual) between Internal and External IdP to define what attributes are to be asserted under what circumstances.
- External IdP data will be "stale" unless ongoing provisioning processes are put in place.
- Linkage might not be trusted for all purposes, leading to policy implications on which SPs can talk to a given External IdP.
    - E.g., if a given External IdP is entitled to assert Student ID for separated students, then it's potentially important that IdP only be leveraged by Alumni services SPs and not (current) Student services SPs.

Supported Use Cases

This model can support the following External ID Use Case Categories:

- Business affiliates
- Outbound affiliates
- Alternate factor (possibly)

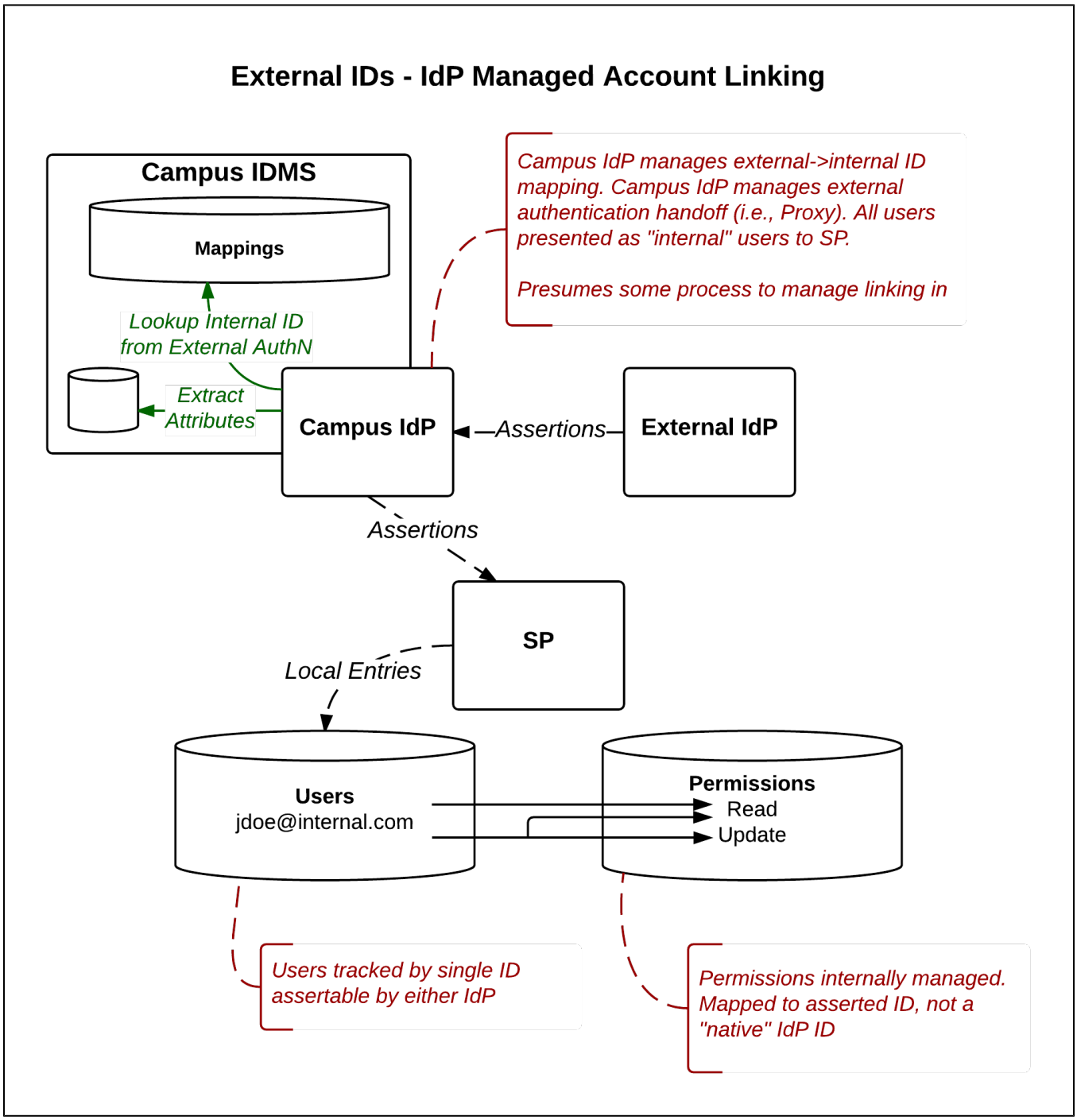
Discussion

If the SP were made responsible for the attribute merging (i.e., performing attribute queries or other lookups to get the "internal" user attributes), this example becames a hybrid of approach 2 and 3.

Approach 4:Account Linking at the IdP

Model Description

In this model, the IdP itself manages the linking of External IDs to internal users. This model hides from the SP the fact that an External ID (or external credential) was used for authentication, allowing users to use internal and external credentials interchangeably. It also allows for "Bring Your Own Credential" support with no need for the SPs to perform customized support of account linking.



Responsibility Matrix

- Who does account linking? *Internal IdP*
- Who merges account attributes? *Internal IdP*
- Who authenticates and handles attribute release? *External IdP*
- Who decides whether a given external ID source is trusted? *Internal IdP*

Pros

- Lightweight for SPs
- Allows user to completely replace internal credential with external credential
  - Linking can be done once for all services
- Linked attributes will not be "stale" at the SP
- Outsources technical LoA concerns (proofing still an internal IdP concern)

Cons

- Heavyweight for IdPs. campus IdPs essentially become IdP Proxies providing data enhancement of all inbound assertions.
    - I.e., External IdP asserts an ID, campus IdP uses that ID to lookup internal Identity and build a campus/internal assertion describing the individual.
- SPs unable to distinguish what credential was actually used
    - Could be rectified by building in additional attributes/authentication context support at the IdP, but any such support would be highly custom to that IdP
    - In a "BYOC" scenario, lack of ability to distinguish may be seen as a feature, but is listed as a con given the expectation of this inability being identified as some level of security risk

Supported Use Cases

This model can support the following External ID Use Case Categories:

- Non-Business affiliates
- Ad-hoc personal affiliates (presuming an internal identity is created)
- Business affiliates
- Inbound affiliates (presuming an internal identity is created)
- Outbound affiliates

Discussion

Discussion above presumes that the mapping done in the Internal IdP is a "global" mapping. It's also possible that the Internal IdP could allow per-SP mapping rules, in which case this case looks functionally much more like approach #2 (Account Linking at the SP), though the responsibility matrix is as shown in this example.