

A Use Case Packet consists of three items:

A background ppt on the enabling legislation or purpose of the activity

A 1-2 page classic use case document

Answers/discussion responding to the architectural issues list

---

...from eve's list of important considerations

login-time attribute transfer

back-channel authz'd access

separate policy decision hub

on-board storage of user data

user-imposed policy

binding of ID(s) to data shared

sources of data

RESTful

co-ownership of shared data

---

## Architectural issues list

1. Requirements for attributes, their meaning and syntax, their representation to users

include distinguishing identity proof versus authn method for classic LOA of identity

2. Assignment of values to attributes

business processes, sources of authority, delegation of authority, LOA (from self-asserted to highly vetted) distinguishing static and dynamic attributes values, logging information about the assignment of value, revocation issues, etc

When is the need to get a yes/no to a query to the source of authority or holder of attributes versus receive attributes at the relying party to make the access control decisions

3. Movement and location of attributes –

where do you expect attributes to be located? What are the static and dynamic aspects in identifying the location of the attributes? How are they to be gotten there? How are they expected to be retrieved from there? What are the criteria for push versus pull? Persistent identity linking requirements or concerns?

4. Legal, privacy and secrecy considerations

protection of data

requirements for user consent or other privacy measures

requirements for or against PII

compliance with federal directives

carrying privacy policies with the data

do we get into the issues of privacy more – or is it reflected in identifier linking, etc...

ala the dresden doc with its terms and negations below:

*Anonymity* of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the *anonymity set*.

*Identifiability* of a subject from an attacker's perspective means that the attacker can sufficiently identify the subject within a set of subjects, the *identifiability set*.

*Unlinkability* of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.

*Linkability* of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not.

*Undetectability* of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.

*Detectability* of an item of interest (IOI) from an attacker's perspective means that the attacker can sufficiently distinguish whether it exists or not.

*Unobservability* of an item of interest (IOI) means

- undetectability of the IOI against all subjects uninvolved in it and
- anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.

*Observability* of an item of interest (IOI) means <many possibilities to define the semantics>.