Business Models

Business Models

The reason it's a "BLT sandwich" is not just because, Bacon!!!, but because business comes first. Everything flows from this. The draft NIST Privacy Risk Management Framework notes, very sensibly, that you must start with a business goal.

We have discussed in the legal subgroup that #1 means an individual and their data are beholden to some enterprise. #2 means the data never even enters the sphere of the enterprise; it stays in its native environment, the way data can stay on a phone. We agreed to focus first and foremost on #2 because it meets important UMA goals, requires legal support, and appears to be the critical model required for the IoT.

These models can be viewed as being on a continuum. In #1, the AS legal entity has access to the RO's data, in #2, the AS legal entity (as such) has no access to RO's data, and in #3, the AS legal entity can be considered "the same as" the RO because the RO built the AS. Alice goes from fully disempowered vs. fully empowered with respect to the terms of the contract she can forge with the AS. (We have also discussed how a modular approach to UMA Legal outputs can support the technical dynamicism present in #3 versus #2.)

1. Narrow ecosystem / Organizational consumer-facing access federation

Similar to the corporate consumer-facing identity federations of today. Enterprise E serves as both AS and IdP to its end-user customers, who are the ROs. RqPs might be customers as well, or also users with a more tenuous relationship to enterprise E. The RS's and clients might be run by enterprise E, or possibly also by some partners P, who have been well vetted in advance and whose service and app relationships were set up statically. Each RO experiences the AS as covering the authorization of some fairly limited set of resources in their "online world" (e.g. vertical- or vendor-specific), rather than a potentially comprehensive set. The federation might or might not cross jurisdictional boundaries.

Example:

- Government-to-citizen attribute-sharing and delegation platform with a single government-run AS.

2. Medium ecosystem / Industry access federation

Somewhat similar to the social login identity federations of today. A variety of services and products SP find it valuable to standardize on a method of outsourcing authorization, and a few authorization players A have arisen that are willing to play the AS role, such that end-user ROs are able to choose, by (something approximating) free-market action, the AS they would like to use when engaging with each SP. However, there may be market forces that restrict the choices A presented at each SP among which an RO could choose, producing a "NASCAR effect". Options that are "RO-built/bought/run" are, as today, much less likely to be viable in the market, but there is no structural reason that they would be excluded. The environment is fairly heterogeneous, with any AS/RS/client matchup possibly representing three different organizations, but each required pairwise relationship is likely established in a static fashion, as today.

Example:

- Consumer IoT marketplace with a few popular AS platforms to choose from (imagine WeMo etc.).

3. Wide ecosystem / Free-love access federation

An analogue to the Platonic ideal of identity federation oft-imagined today. All parties can meet and establish trust dynamically as required; for example, an UMA client can acquire OAuth client credentials at an AS at the moment of need, and so can an UMA RS, with any business concerns such as execution of terms of service handled dynamically. ROs can freely choose, build, buy, or run their own AS.

Example:

- The desired end-state of the global healthcare market, with IoT and consumer elements mixed in.