User-Managed Access, Privacy, and Public Policy

Eve Maler

Kantara P3WG meeting

4 Nov 2010

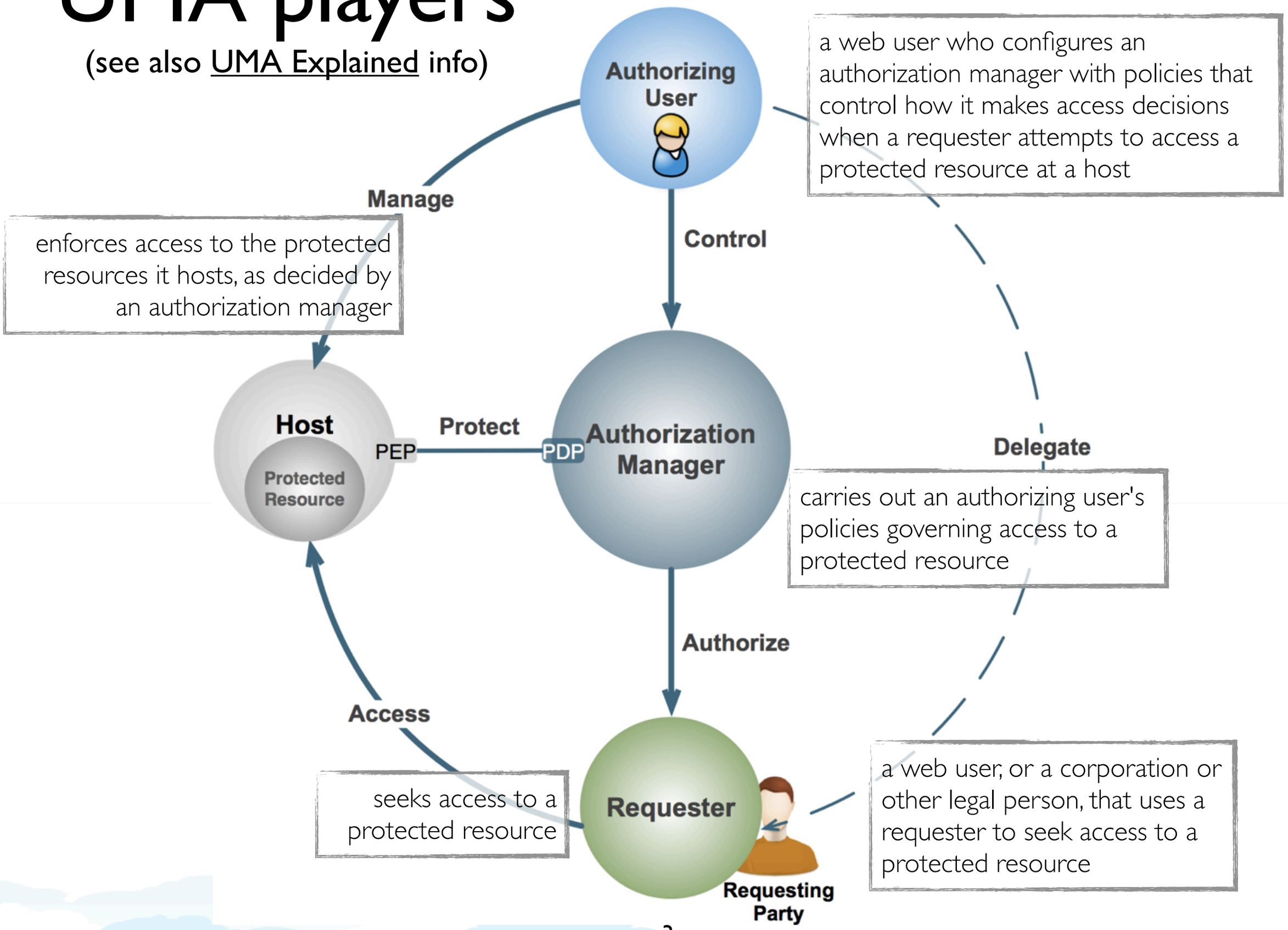
From *privacy* to *selective sharing*

> The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be"
>
> – Ann Cavoukian, Information and Privacy Commissioner of Ontario, **Privacy in the Clouds** paper

Make it easier to share selectively, with greater confidence that your expectations will be met

UMA players

(see also UMA Explained info)



Selected UMA design principles and requirements

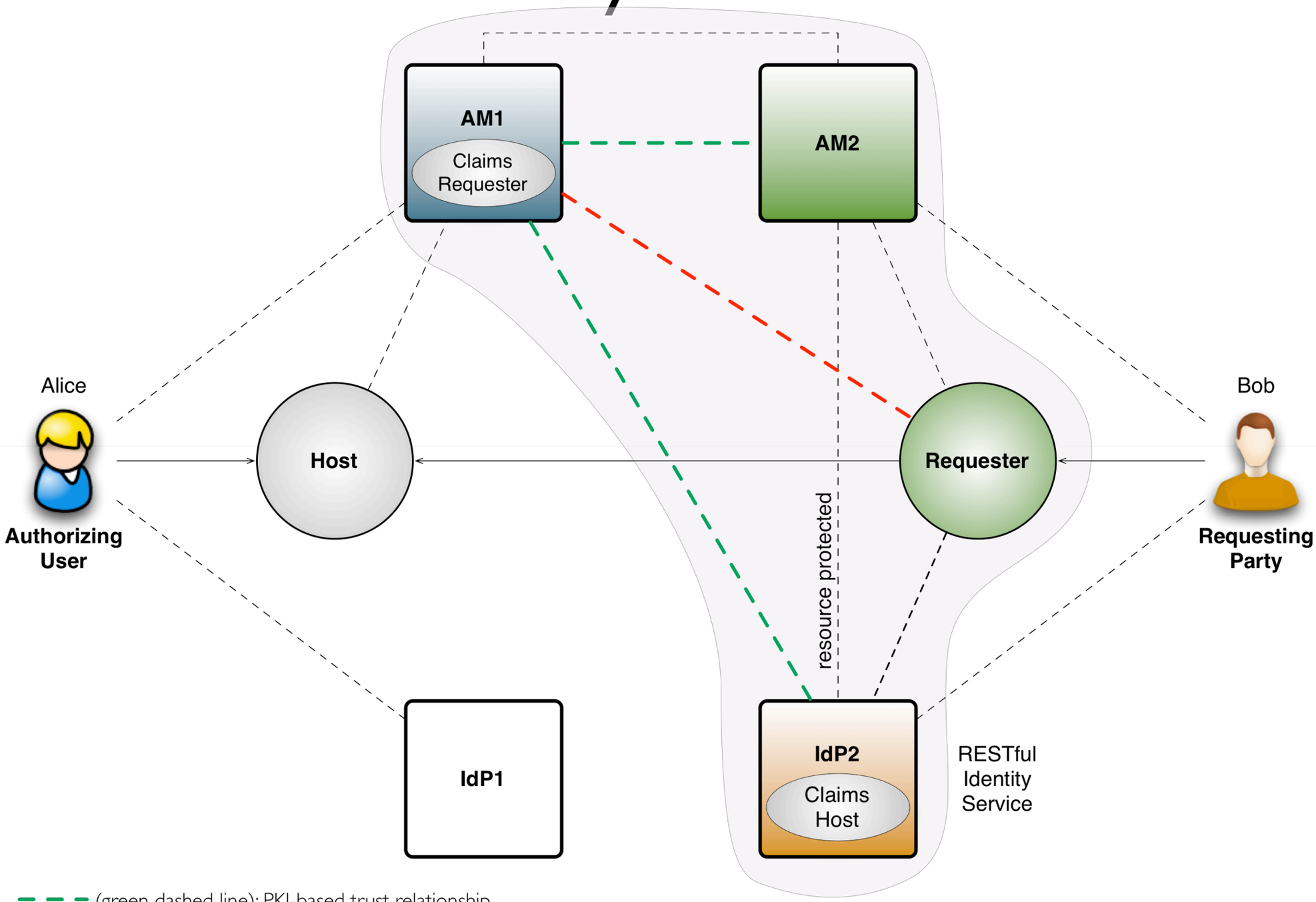
- "ID-agnostic": don't depend on some global notion of an identifier namespace (like OpenID)
- Protect the privacy of the authorizing user (not necessarily other parties)
- Prevent correlation of authorizing user's activity across multiple hosts
- Allow separation of hosts and authorization manager
- User-driven policies and terms for sharing/access (authorizing user can make initial offer vs. just consenting)
- Authorizing user can audit and stop sharing/access relationships

Practical data usage control issues

> UMA is making a run at the problem of privacy-enhanced selective sharing on several fronts, but is counting on synergies with many other efforts (ongoing, planned, and speculative) to take full advantage of the opportunities presented, including, for example:
>
> - Trust frameworks in concert with identity assurance and attribute assurance schemes
> - Standardized policy expression and evaluation frameworks
> - Standardized privacy policies, data portability policies, and information sharing agreements
> - Standardization around web APIs and the scopes that apply to them
> - Dynamic registration of OAuth clients at dynamically discovered authorization servers
> - Customer-centric “fourth-party” brokering services
>
> – Oct 2010 W3C workshop paper on **Controlling Data Usage with UMA**

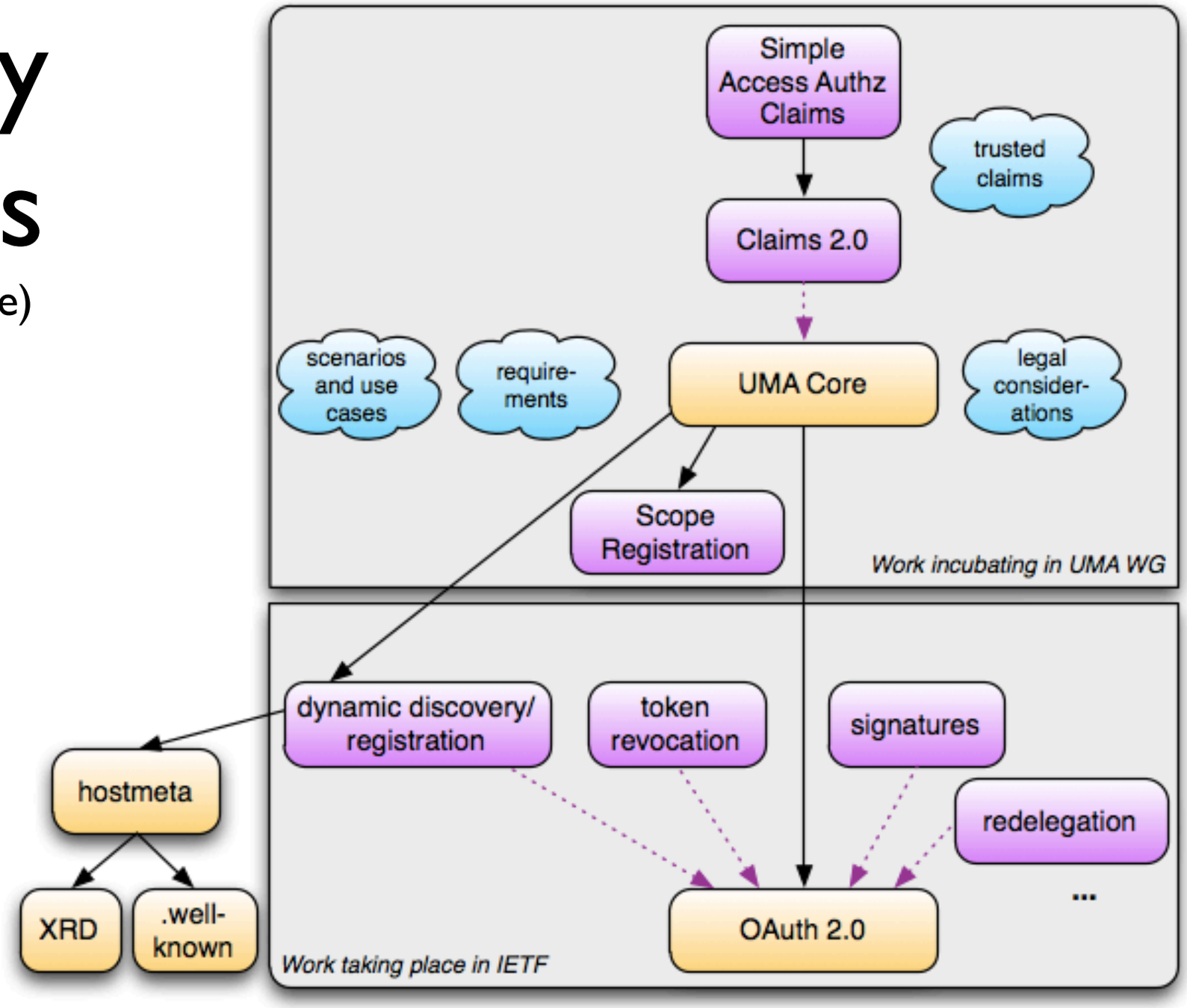
Changing the offer/acceptance cycle for terms of access is *hard*

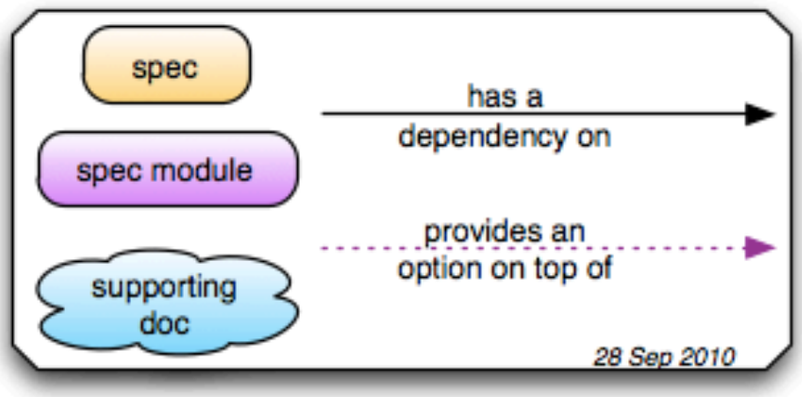
UMA-protected "trusted claims" could be wielded to gain access to UMA-protected arbitrary resources



State of play of the specs

(see also Working Drafts page)





Newcastle University

leeloo