The Three S's Of Distributed Authorization: Safe, Simple, Scalable

Eve Maler, Principal Analyst, Security & Risk

@xmlgrrl, +Eve Maler

MIT Legal Hackathon

January 28, 2013

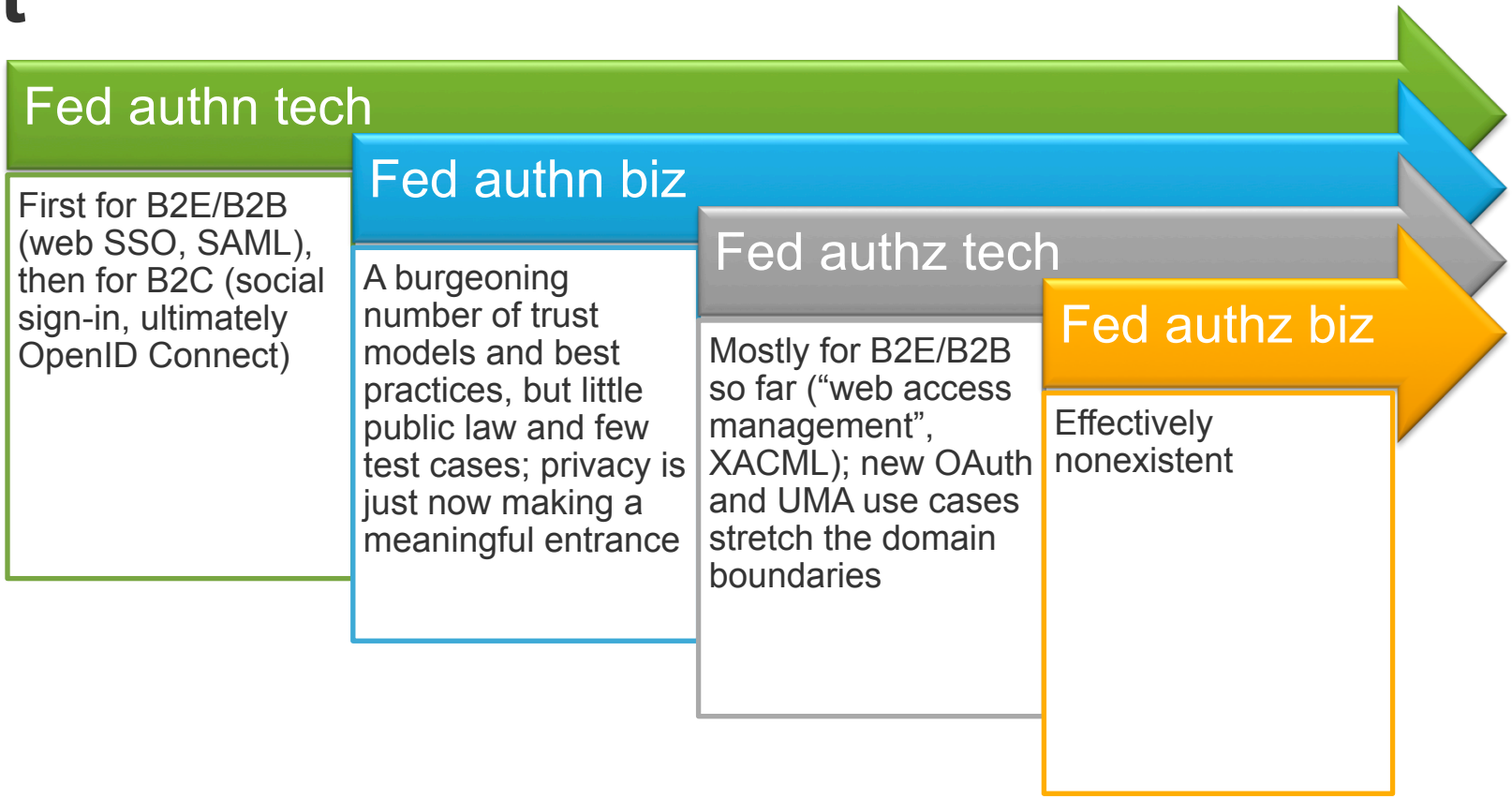
Steve Yegge's rant crystallized a key challenge for data sharing

[Jeff Bezos] issued a mandate that was so out there, so huge and eye-bulgingly ponderous, that it made all of his other mandates look like unsolicited peer bonuses… '1) ***All teams will henceforth expose their data and functionality through service interfaces.****'*

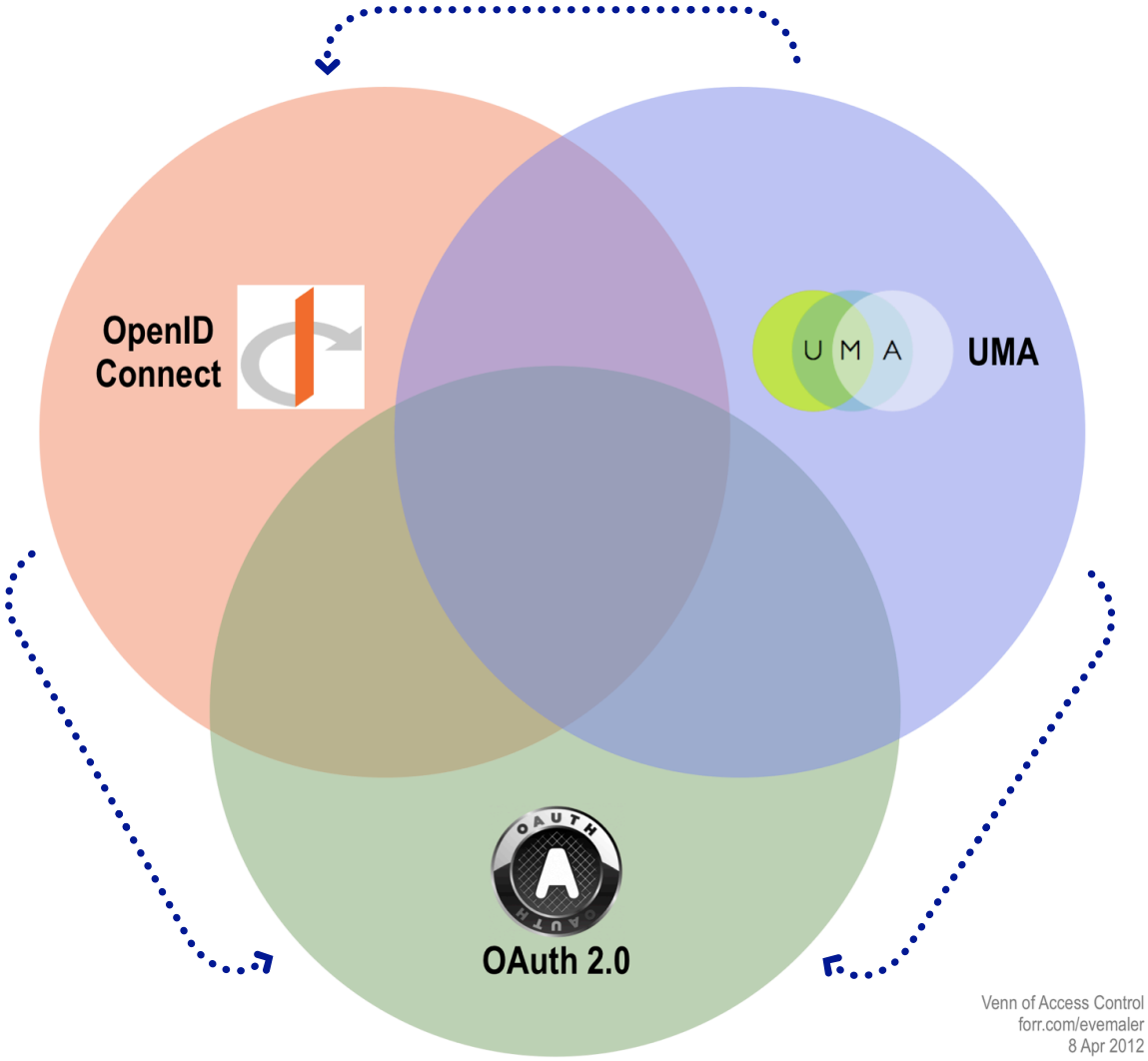
Like anything else big and important in life, ***accessibility has an evil twin*** *who, jilted by the unbalanced affection displayed by their parents in their youth, has grown into an equally powerful arch-nemesis (yes, there's more than one nemesis to accessibility)* ***named security.*** *And, boy howdy, are the two ever at odds.*

But I'll argue that accessibility is actually more important than security because dialing accessibility to zero means you have no product at all, whereas ***dialing security to zero can still get you a reasonably successful product*** *such as the Playstation Network.*

We're finally getting around to loosely coupled identity in steps – but we're often not deeply protected when we do it

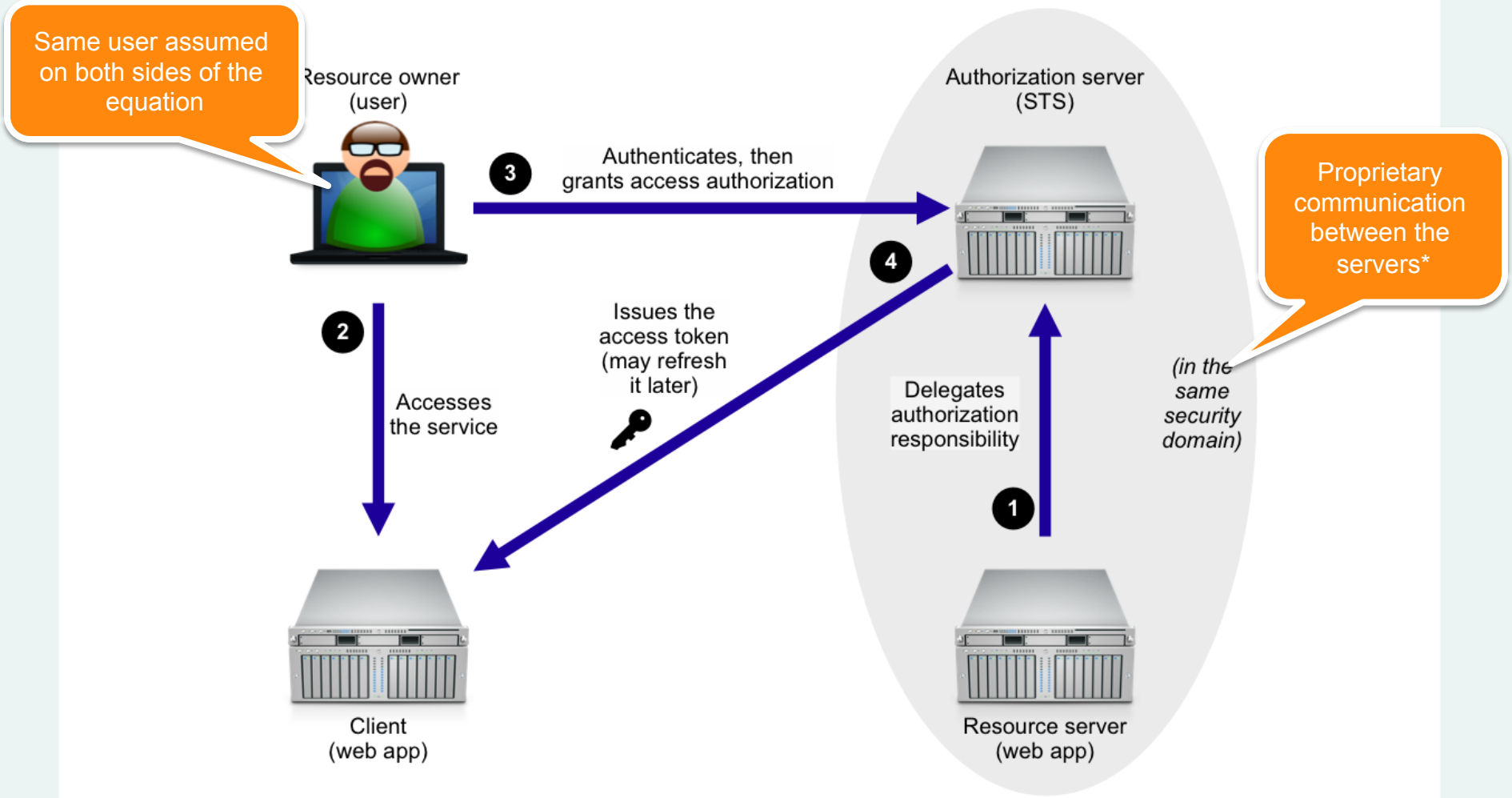


There's a new "Venn" of access control

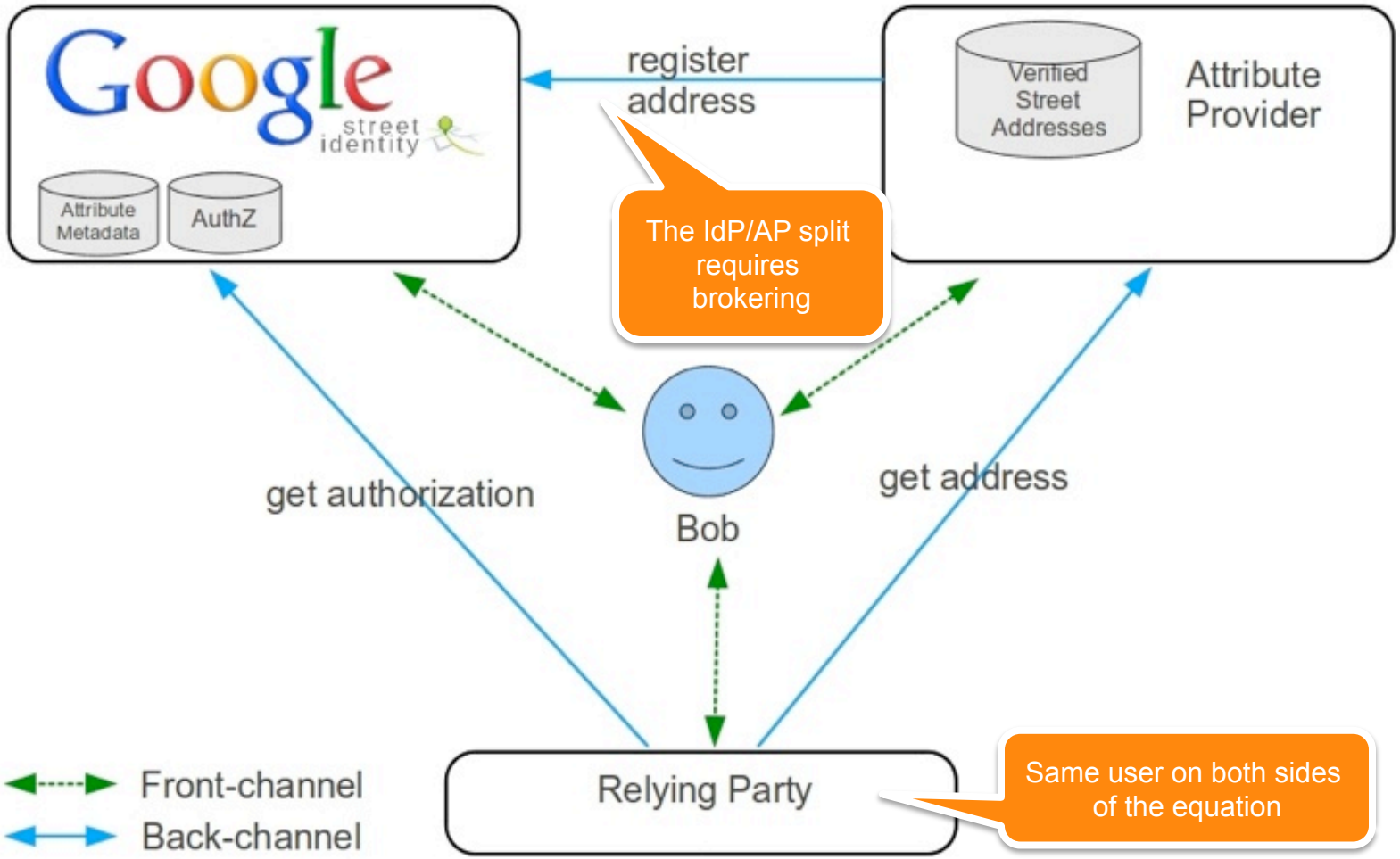


Venn of Access Control
forr.com/evemaler
8 Apr 2012

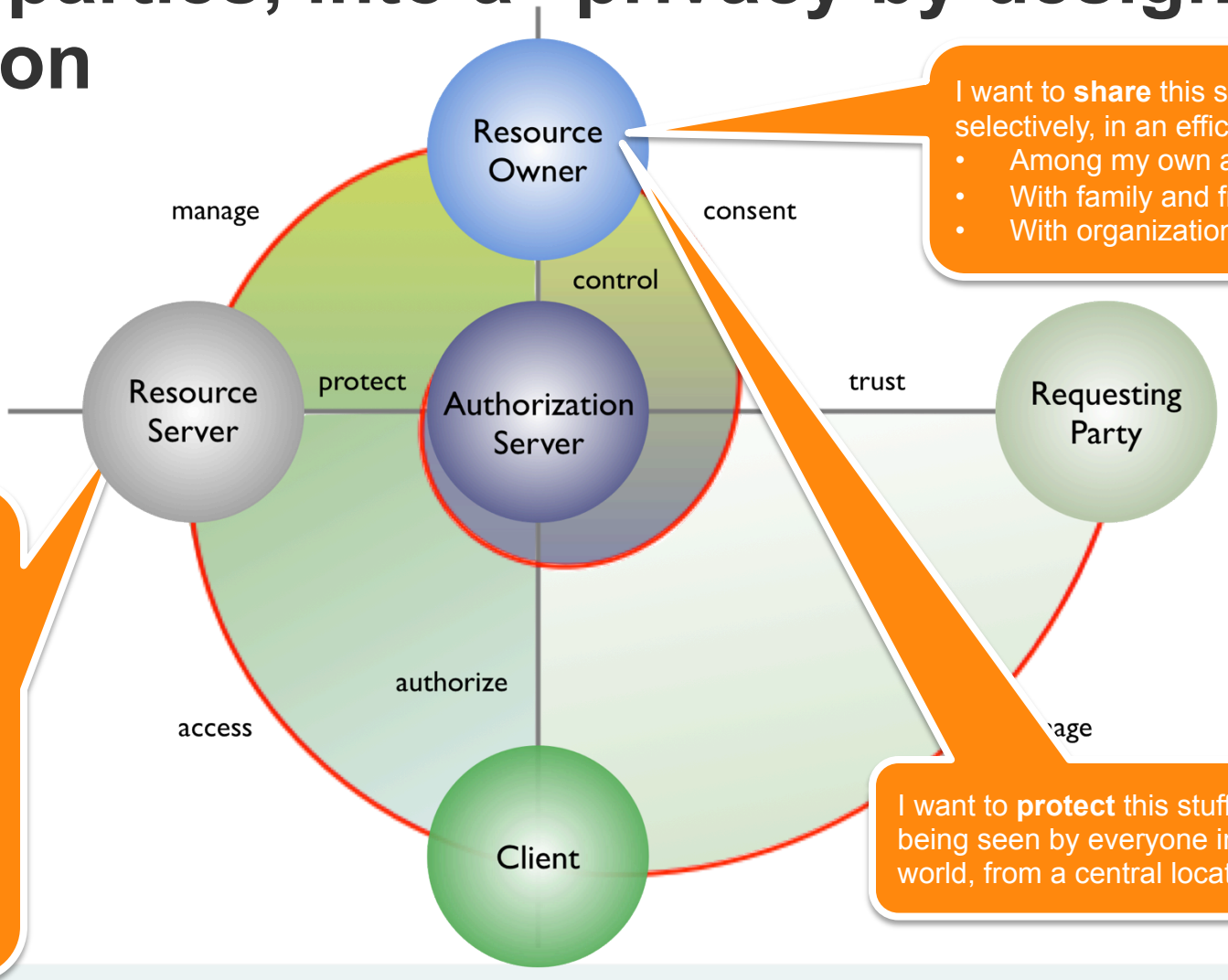
The classic OAuth scenarios enable lightweight web services security



The OpenID Connect attribute provider scenario also has limitations



UMA turns online sharing, with arbitrary other parties, into a “privacy by design” solution



…resulting in opportunities for a true digital footprint control console

Web 2.0 access control is inconsistent and unsophisticated	You can unify access control under one app
To share with others, you have to list them literally	Sharing policies can test for claims like “over 18”
You have to keep rebuilding your “circles” in new apps	You can reuse the same policies with multiple sites
You can’t advertise content without giving it away	You can control access to stuff with public URLs
You can’t get a global view of who accessed what	You can manage and revoke access from one place

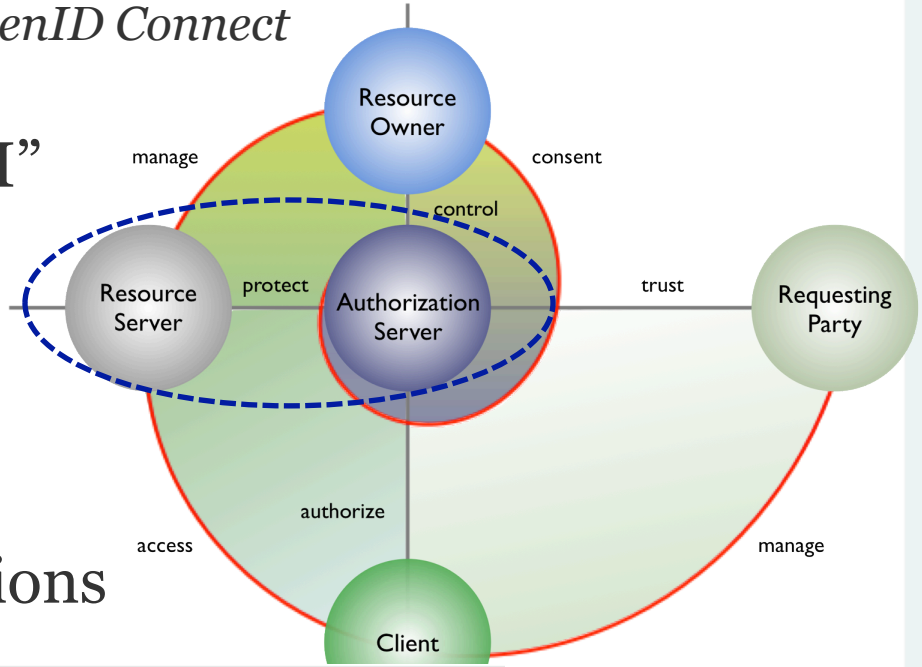
A technical innovation: machine-readable scope descriptions

(now modularized so OAuth and OpenID Connect can potentially use this feature too)

AS presents "protection API"

RS makes calls to it to register resources for protection, along with their scopes

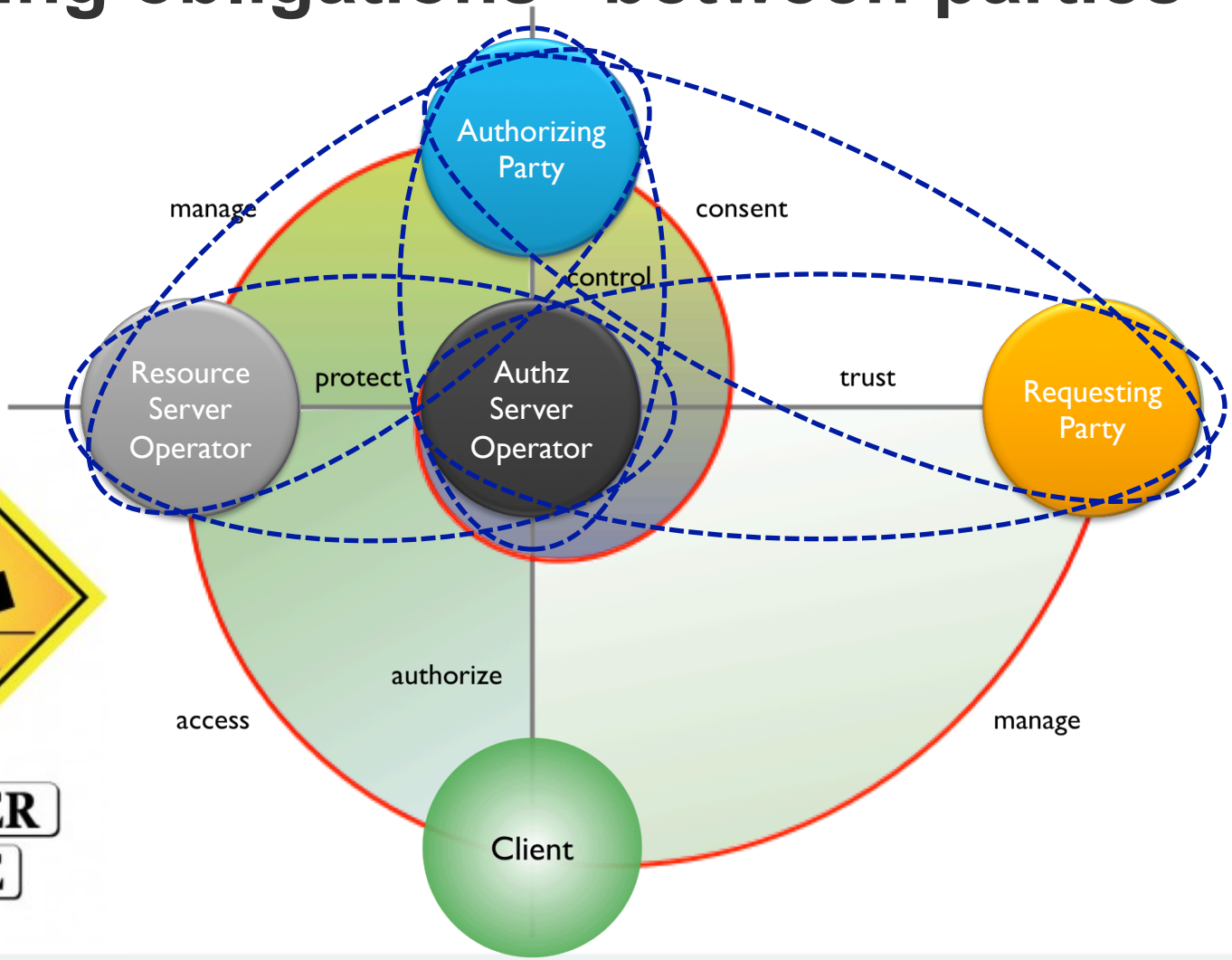
Scope IDs point to descriptions




```
{
  "name": "View",
  "icon_uri": "http://www.example.com/icons/reading-glasses"
}
```

Dazza's innovation: include formal terms of authz in them

A business innovation: enabling "binding obligations" between parties



Obligations are tied to auditable changes of protocol state

- Phase 1: protect resources
  - Obligations revolve around the introduction of the AS and RS
  - The state change: issuance of a “protection API token” for OAuth-mediated access to that API
- UMA phases 2 and 3: get authorization and access resource
  - Obligations run the gamut of types and state changes
  - The two key ones:
    - Requesting Party-Authorizing Party: Adhere-to-Terms
    - Authorizing Party-Requesting Party: Adhere-to-Terms
    - Scope terms of authz can be surfaced up into this agreement if the AS requests a **claim** that confirms consent

Next steps for this approach

- *Vetting of contractual framework clauses*
- *Vetting of spec security and auditing provisions*
- *Vetting of the spec/contractual connection: third-party certification?*

- *Nearly any protocol specification can adopt the state-change approach…*

Thank you

Eve Maler

+1 617.613.8820 ***(but based in Seattle!)***

emaler@forrester.com

@xmlgrrl

www.forrester.com