The Security Assertion Markup Language (SAML) and Liberty Web Services

Eve Maler
eve.maler@sun.com
http://www.xmlgrrl.com/blog

GSA Identity Workshop, 27 February 2007

The big picture in federated identity

Opportunities with federated identity

- When you say *federated*, think *distributed*
- Services and applications can:
  - Offload authentication and identity lookup tasks
  - Unify treatment of all “things with identities”
  - Provide finer-grained access control and differentiation
- Organizations can:
  - More securely outsource business functions
- People can:
  - Unify management of their identity information
  - Avoid authenticating repeatedly
  - Have better-personalized online experiences

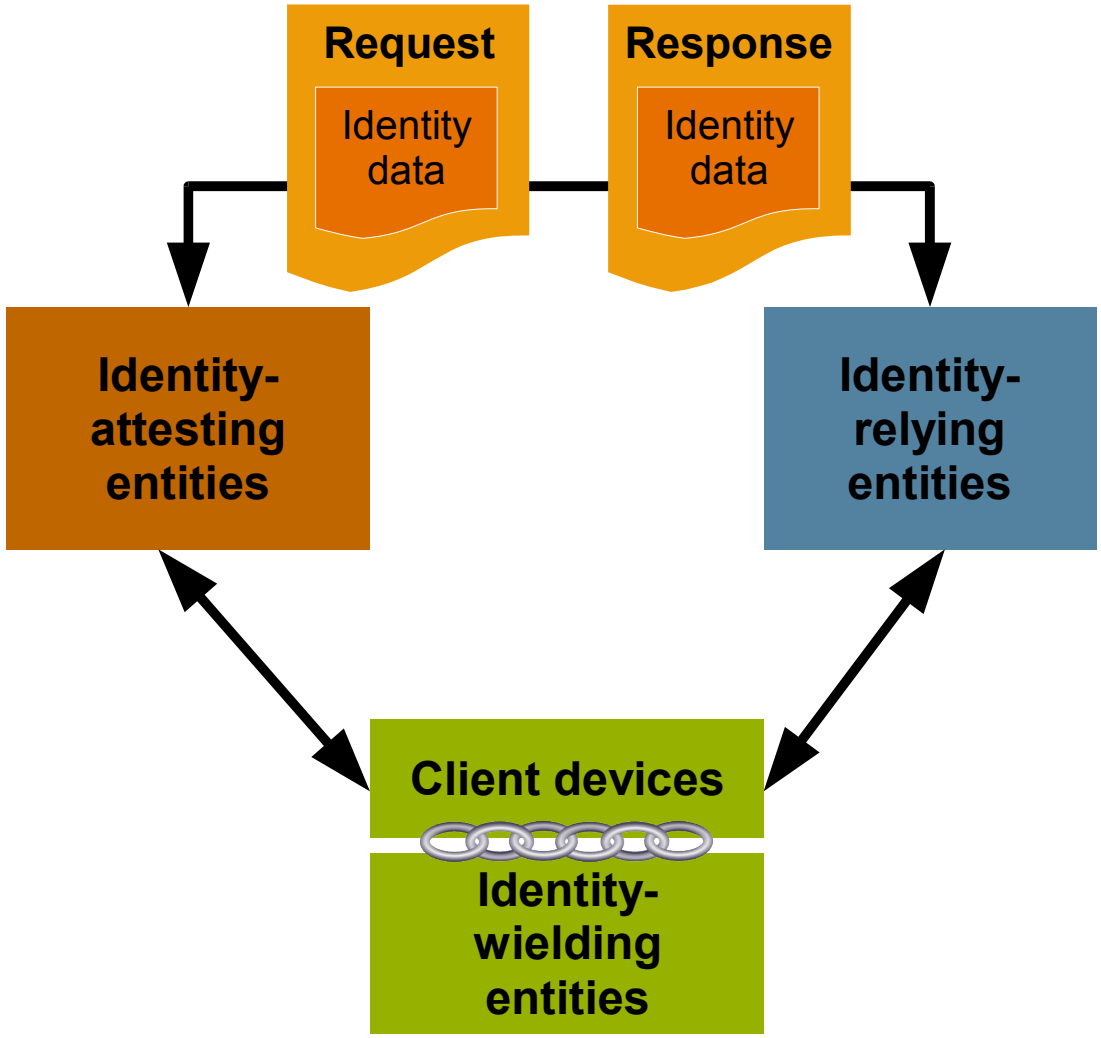
Risks and challenges

- Compromised privacy
- Regulatory compliance
- Unifying disparate identity and security models
- Integrating with legacy systems

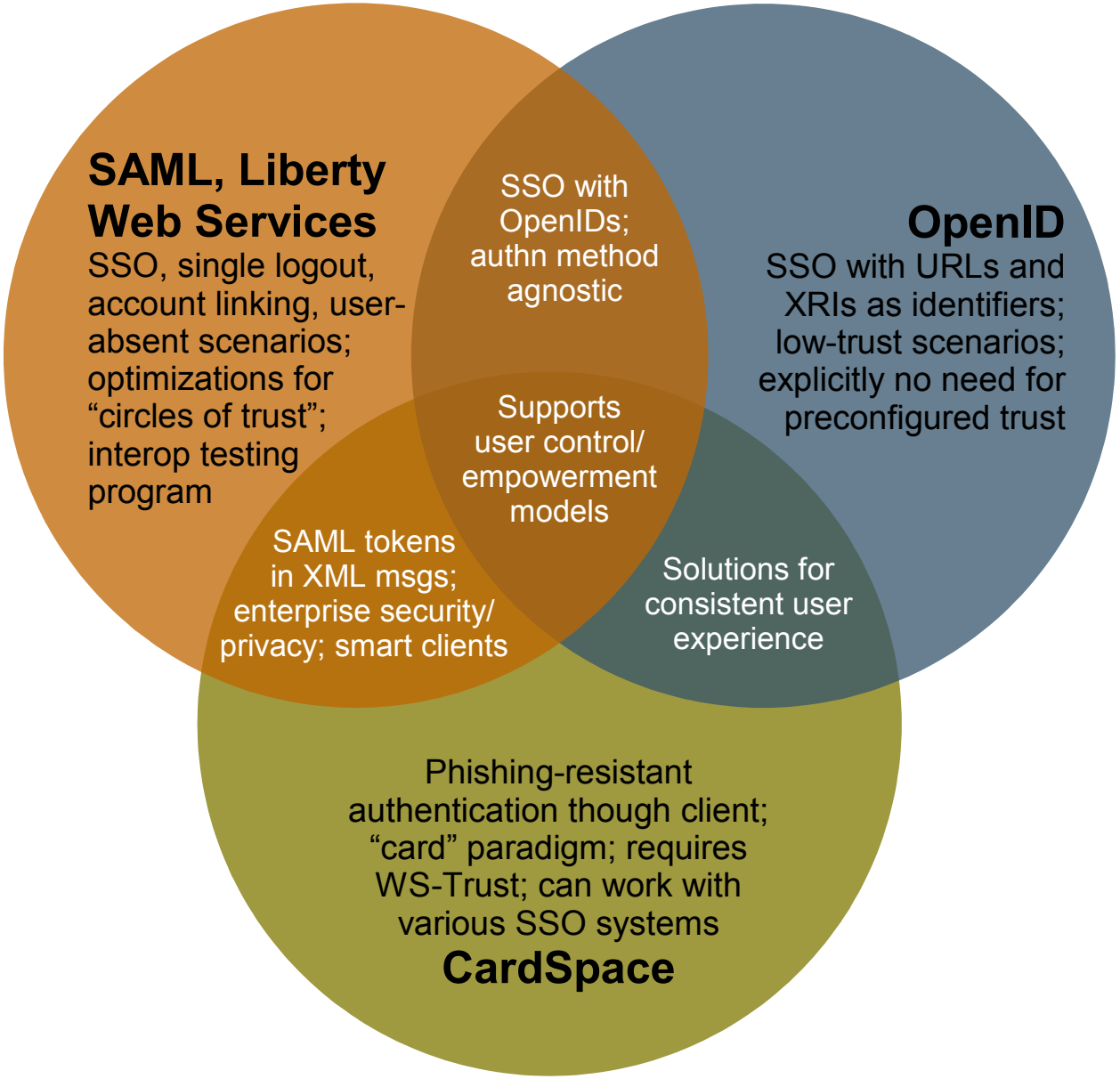
...all of which can be mitigated by:

- Open technology standards
- Deployment policy guidance
- Independent third-party certification

Common system entities and modes of communication across technologies



One view of the technology landscape



More about SAML

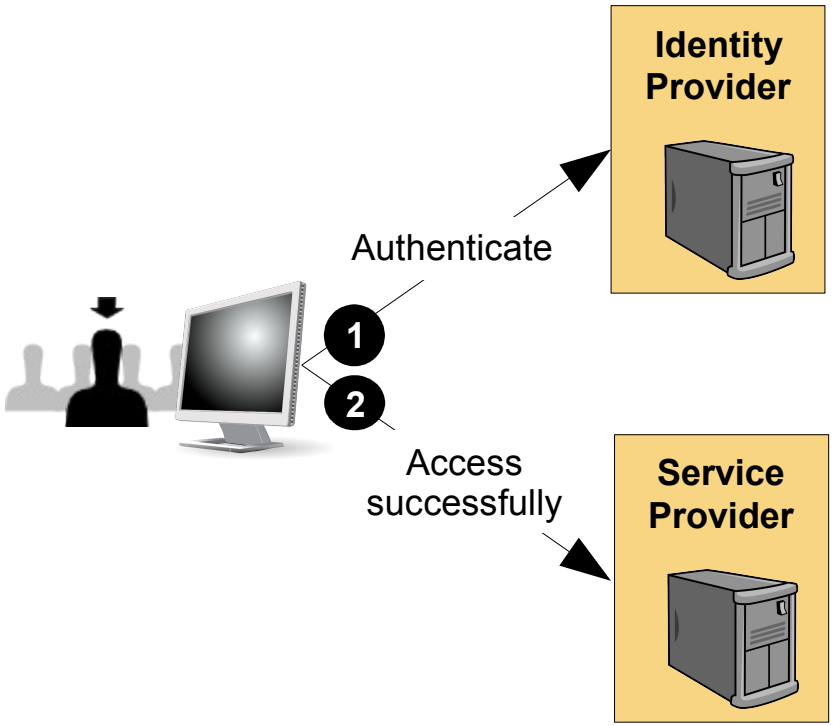
SAML in a nutshell

- **SAML is...**an XML-based framework for marshaling security and identity information and exchanging it across domain boundaries
- **SAML is...**widely supported in products and FOSS, with 3rd party interop certification performed by the Liberty Alliance
- **SAML is...**used and/or mandated in many reference architectures, including many e-government projects:
  - E.g., Denmark IT and Telecom Agency, Finnish Tax Board, Sunderland UK City Council, France Mon Service Public portal – and GSA E-Authentication initiative!
- **SAML V2.0 was...**standardized at OASIS in 2005, reflecting convergence of SAML V1.x, Liberty Federation, and Internet2 Shibboleth

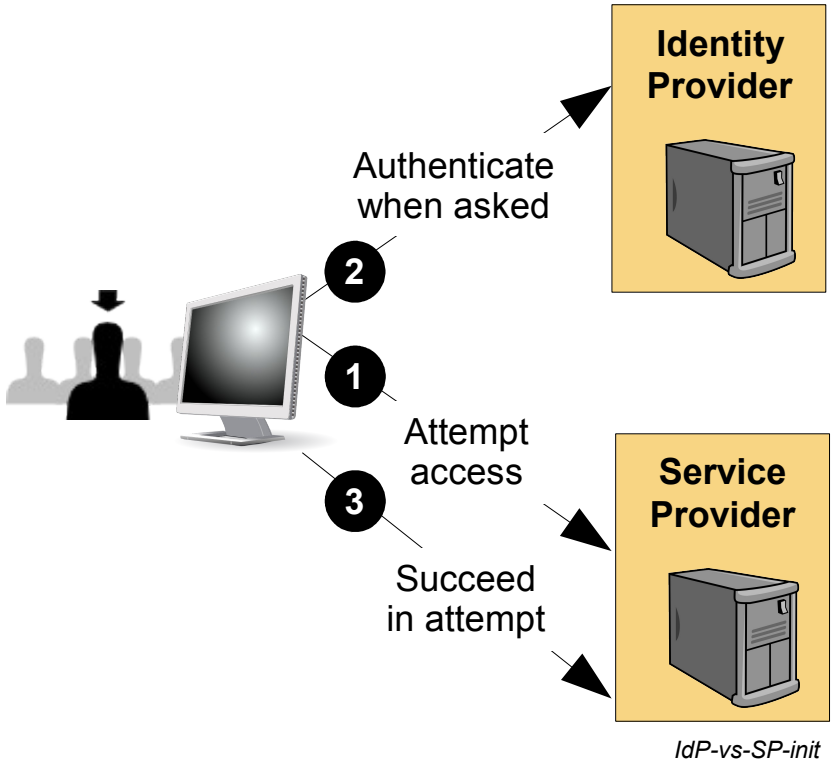
Major SAML use cases

- **Single sign-on** (SSO) of many varieties
- **Account linking** (associating two of a user's existing web accounts) without having to compromise privacy
- **Attribute exchange** for relying-party authz and personalization
- **Single logout** from several apps across a single distributed authentication session
- Anyone can satisfy other use cases with profiling/extension:
  - **Lightweight SSO** Profile for XMLSig-free SSO
  - **OpenID-SAML** and **iSSO** Profiles for SSO à la OpenID
  - **SAML Token Profile** for protecting SOAP traffic using WS-Security
  - **Liberty Web Services** for an end-to-end identity SOA layer

Classic single sign-on scenarios



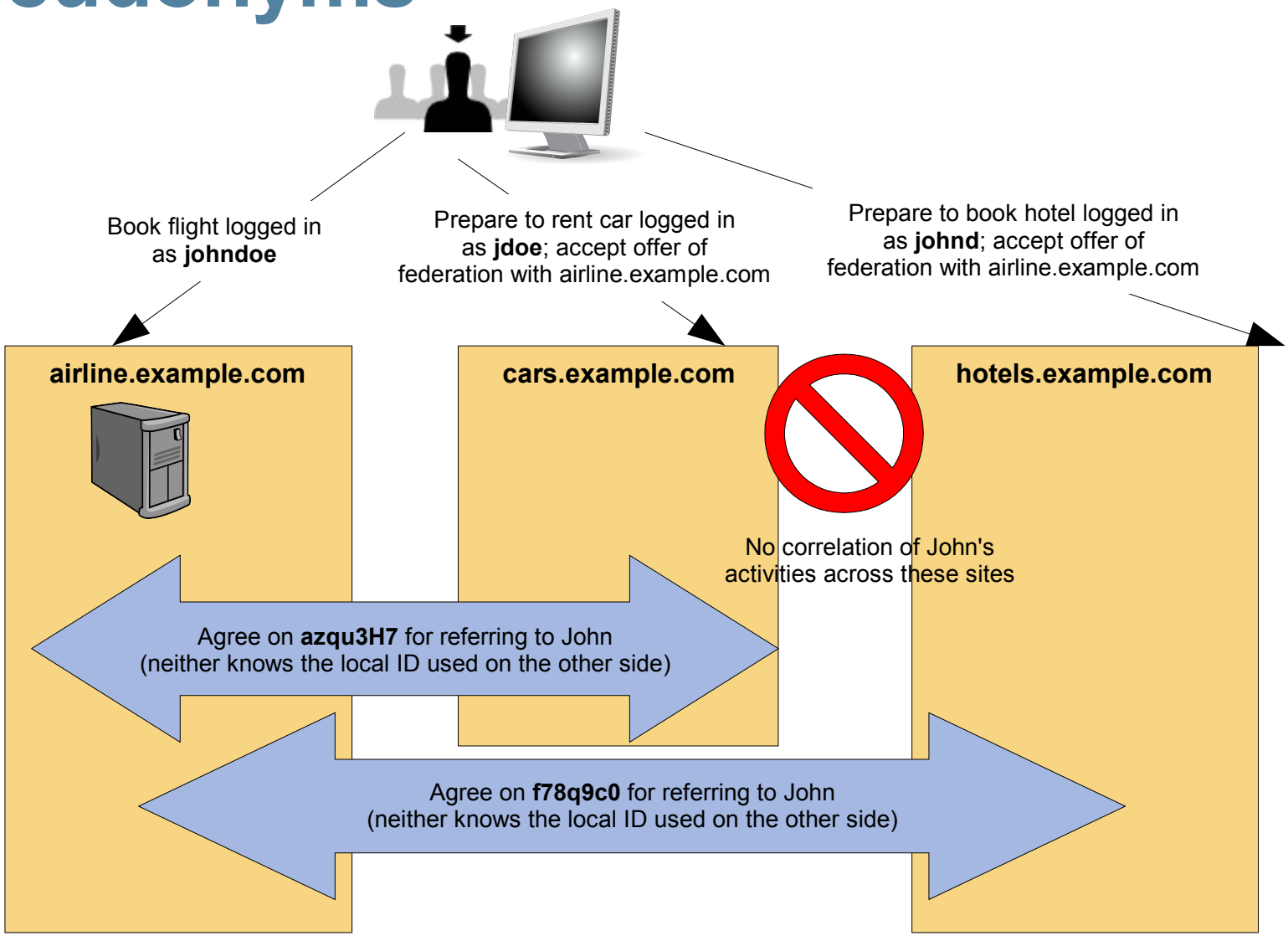
IdP-initiated



IdP-vs-SP-init

SP-initiated

Linking accounts with privacy using pseudonyms

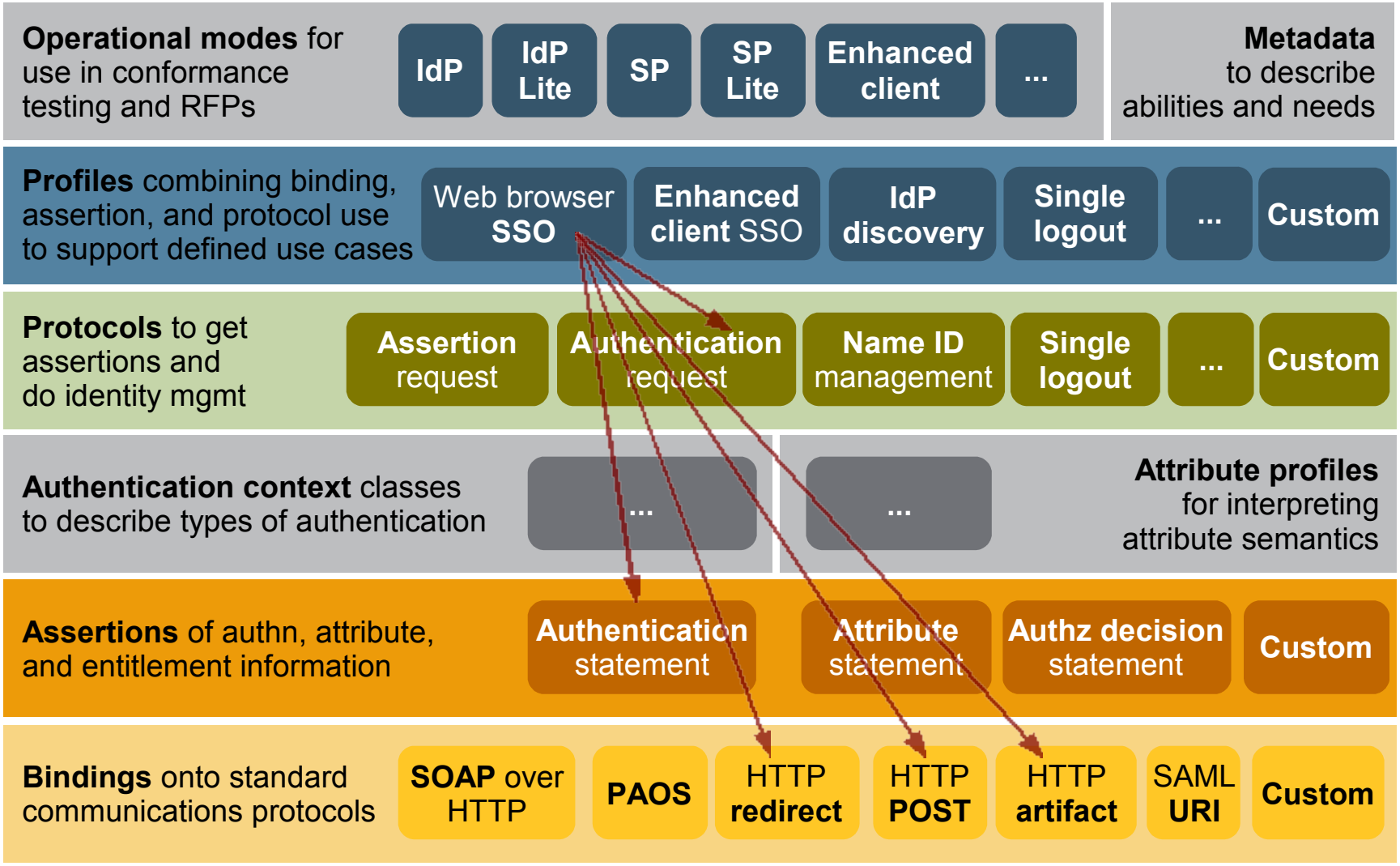


IDFed-usecase

SAML assertions are at the core

- An assertion is a claim made by someone – an **issuer** – usually about someone – a digital **subject**
- A SAML assertion contains one or more statements:
  - **Authentication** statement: “Sam authenticated with a smartcard PKI certificate at 9:07am today”
  - **Attribute** statement (which can contain multiple attributes): “Sam is a manager and has a $5000 spending limit”
  - **Authorization decision** statement (now deprecated in favor of the XACML SAML profile): “Yes, Sam can read that web page”
- You can make your own customized statements
  - XACML's SAML-based assertions allow an issuer to say “this is one of my policies” without referring to a subject

SAML framework



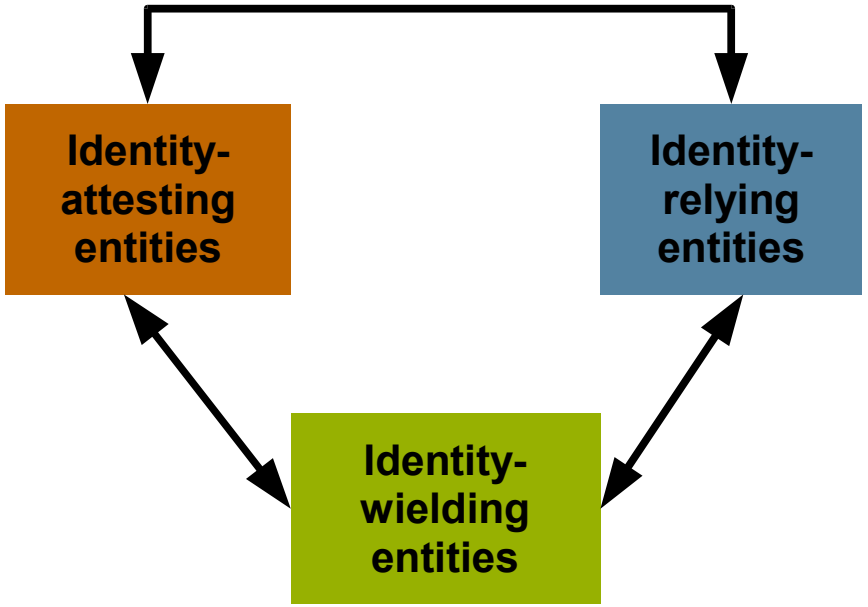
More about the Liberty Alliance and Liberty Web Services

The Liberty Alliance in a nutshell

- An open consortium of ~150 businesses, government agencies, and NGOs
- Since 2001, its mission has been to foster a *ubiquitous, interoperable privacy-respecting federated identity layer* for web applications and services
- It conducts a great deal of proactive cross-industry coordination and liaison activity
- Leadership of the Alliance:

Standards published by Liberty (so far)

ID-WSF: Identity Web Services Framework
- Focused on application-to-application interaction



ID-SIS: Service Interface Specs
- ID-SIS plus ID-WSF equals *"Liberty Web Services"*
- Defines particular useful services
- Personal profile, geolocation...

ID-SAFE: Strong Authentication
- For interoperable strong authn
- On the way...

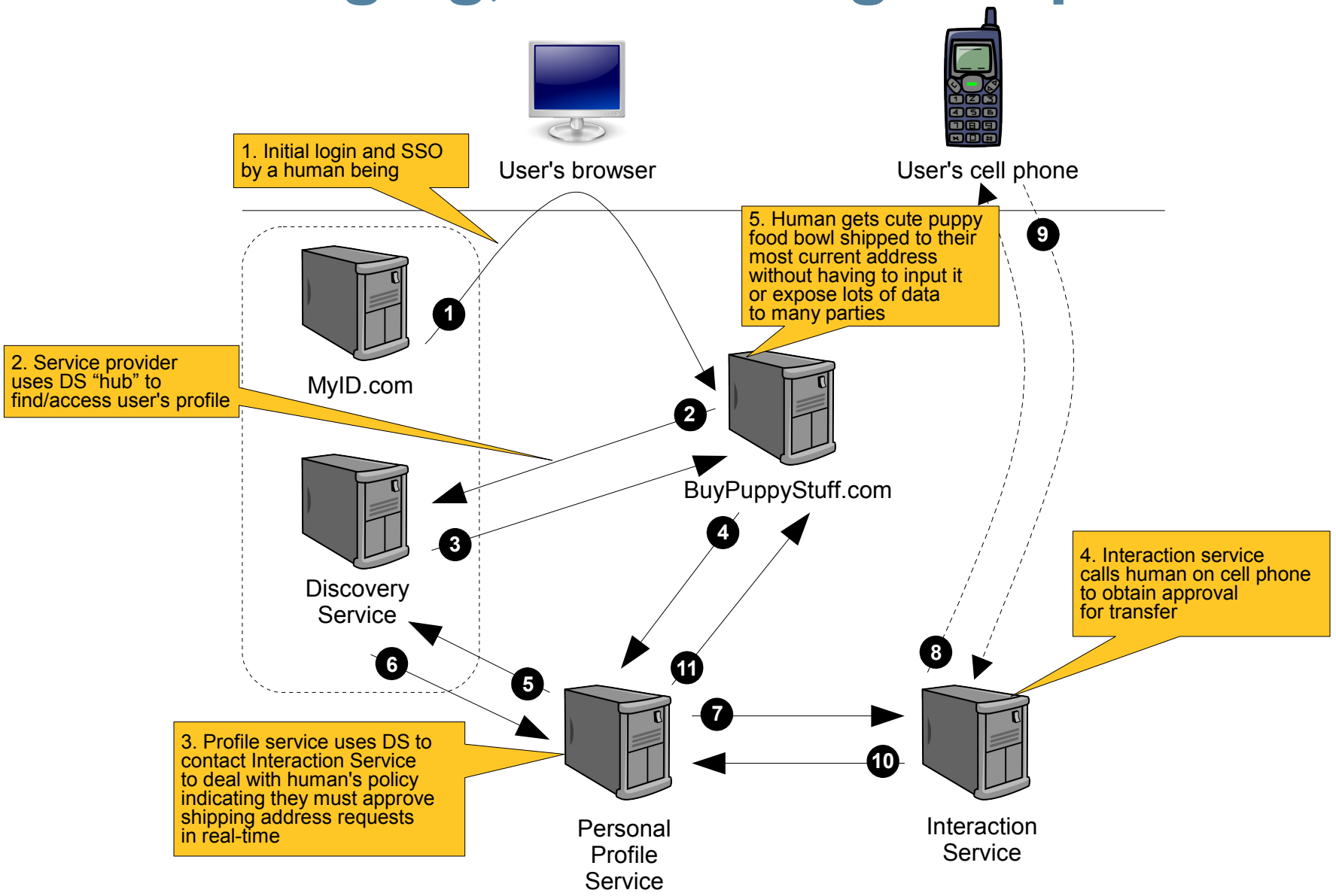
ID-FF: Identity Federation Framework
- *"Liberty Federation"*
- Focused on human-to-application interaction
- Now converged with SAML V2.0
- Liberty Interoperable™ testing certification

Why is application-to-application interaction needed?

- To get around browser payload limitations
- To allow identity-enabled actions to happen silently (mediated by policy) when you're not around
  - All the way from *pay my bills automatically*...
  - ...to *let the emergency-room doctor access my medical records from another country if I'm in a coma*
- To allow multiple services to cooperate securely
  - Providing both personalization and access control

- Liberty uses SOAP-based protocols to achieve these goals

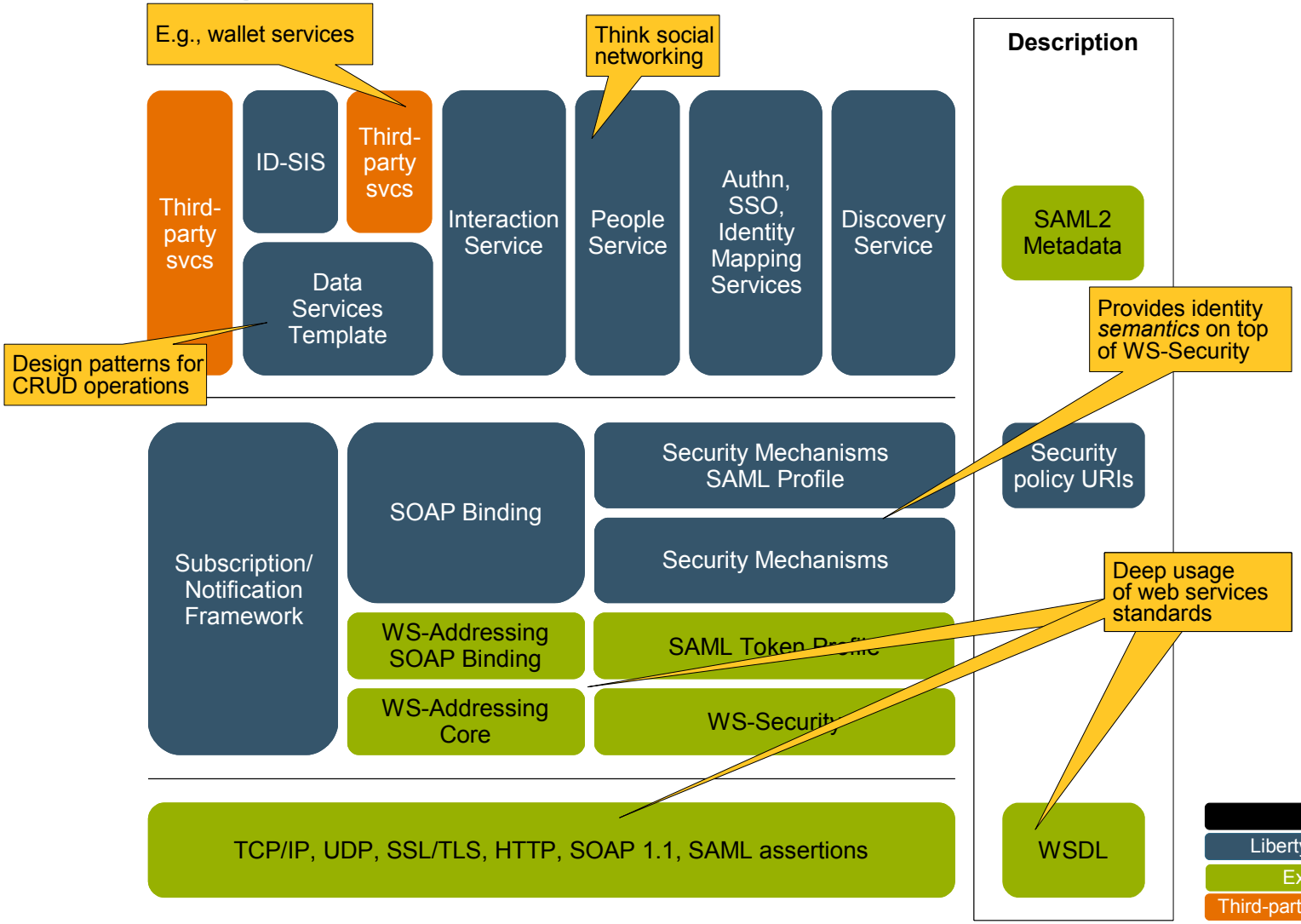
An all-singing, all-dancing sample flow



Design goals

- A standards-based architecture for identity web services
  - Ecosystems of services that expose interfaces on behalf of *individual* users' identities
- A flexible foundation layer for application development and deployment
  - Across security domains, computing platforms, and network devices
  - Across time, allowing for service location flexibility
- The option of maximum privacy and security
  - Identity information requests access-controlled
  - Minimal disclosure of identity information
  - Protection against disclosure of identifiers

Liberty Web Services framework



Resources

Major open-source implementations

- Sun's http://OpenSSO.dev.java.net
  - SAML, ID-FF, ID-WSF in Java; SAML in PHP (“Lightbulb”)
- Internet2's http://www.OpenSAML.org
  - SAML in Java and C++
- Internet2's http://sourceforge.net/projects/guanxi/
  - Shibboleth profile of SAML in Java
- Ping Identity's http://www.SourceID.org
  - SAML and ID-FF (and WS-Fed) variously in Java, .NET, Apache
- Entrouvert's http://LaSSO.Entrouvert.org
  - SAML, ID-FF, ID-WSF in C with SWIG bindings for Python, Perl, Java, PHP
- Symlabs' http://ZXID.org
  - SAML, ID-FF, ID-WSF (and WS-Fed) in C with Perl/PHP wrappers
- Conor's http://www.cahillfamily.com/OpenSource/
  - ID-WSF C client and Java server
- Keep an eye on http://www.openLiberty.org

Additional resources

- For more information on SAML:
  - The draft Technical Overview at the OASIS SAML home page is a cookbook of the most popular flows and contains assertion and message examples for vanilla SSO:
    http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
    http://www.oasis-open.org/committees/download.php/22553/sstc-saml-tech-overview-20-draft-13.pdf
- For more information on Liberty Web Services:
  - Visit the resource center for lots of presentations and white papers:
    http://www.projectliberty.org/index.php/liberty/resource_center
- For more information on interop certification and adoption patterns:
  - http://www.projectliberty.org/index.php/liberty/liberty_interoperable
    http://www.projectliberty.org/index.php/liberty/adoption
  - And don't miss the GSA E-Authentication site!
    http://www.cio.gov/eauthentication/

Thank you! Questions?

Eve Maler
eve.maler@sun.com
http://www.xmlgrrl.com/blog