The Liberty Alliance

and its role in providing solutions for identity, authentication, privacy, and usability

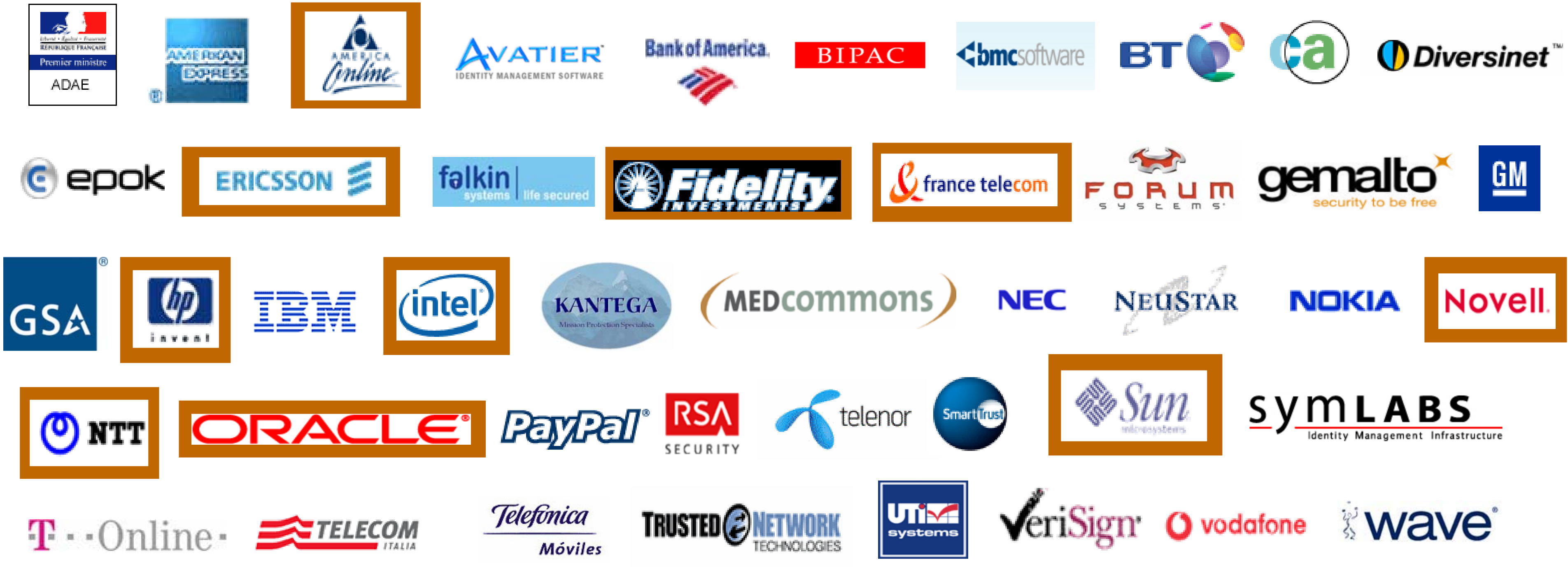
FTC Proof Positive Workshop, 24 April 2007
Gerald Beuchelt, Sun Microsystems
gerald.beuchelt@sun.com

Introducing the Liberty Alliance

- An open consortium of ~150 businesses, government agencies, and NGOs, founded in 2001
- Its mission is to foster a *ubiquitous, interoperable, privacy-respecting federated identity layer* for web applications and services
- It delivers:
  - **Technical specifications** addressing interoperability of identity, security, and privacy features in disparate systems
  - **Business guidelines** addressing the impact of policy, regulations, and legal agreements in deployment
  - A forum for coordinating various identity initiatives and testing **product interoperability**

Liberty's global membership

- **Management board** and sponsor members are shown below

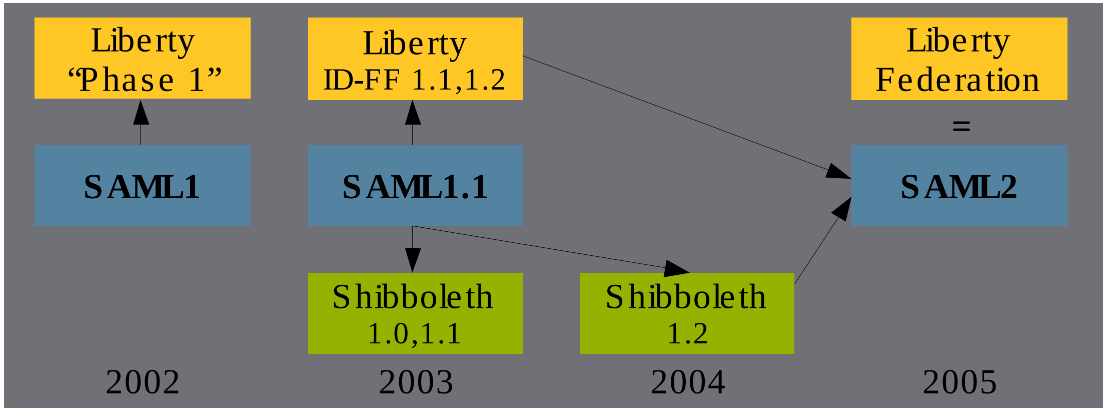


Single sign-on and identity federation

- **Single sign-on** allows a user to reuse the “same login” (user name and act of authentication) to get access to multiple sites
- **Identity federation** allows a user to link two “logins” (user names) from different sites together, and then single sign-on to both in the future
- Privacy sensitivity requires the ability to:
  - Distribute information about the act of authentication without identifying the user uniquely (using pseudonyms)
  - Minimize the sharing of other personally identifiable information
  - Accede to the user's wishes through their expression of policy or their real-time consent

Liberty Federation

- Liberty pioneered full-fledged identity federation, building on SAML and delivering the Identity Federation Framework (ID-FF) standard
- Convergence efforts led to SAML V2.0
- SAML2 + business guidelines + interoperability certification = today's **Liberty Federation** standard



Liberty bases new federation standard on emerging SAML standard

Liberty tracks SAML evolution; Internet2 Shibboleth bases its solutions on SAML also

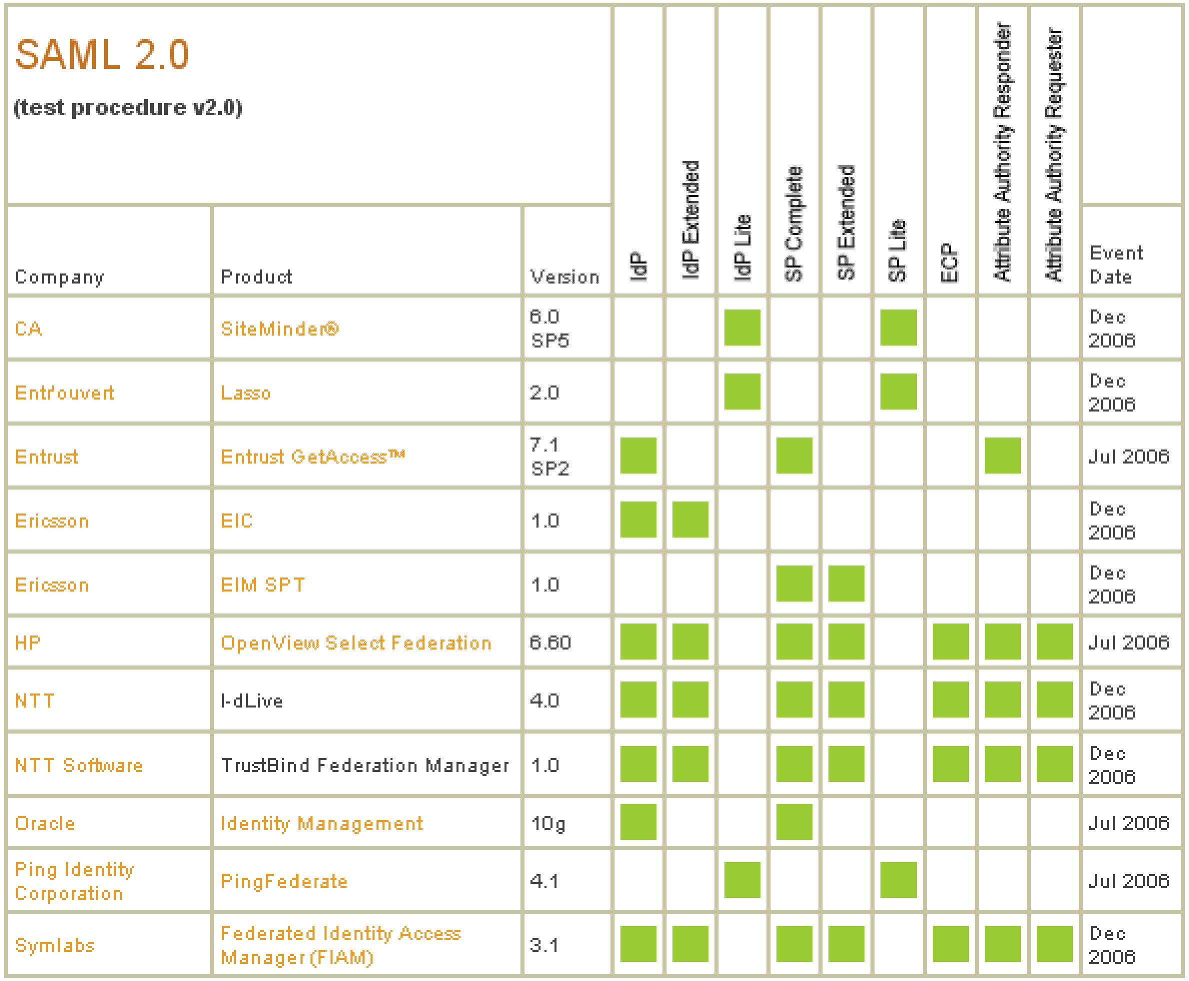
Liberty contributes ID-FF to OASIS for SAML2 convergence; Shibboleth also takes part

Liberty endorses SAML2 as its identity federation solution and provides interop and conformance testing; Shibboleth is working on new SAML2-based APIs

A sampling of vendor adoption

ALCATEL
ELIOS Informatique
Entrust
Entr'Ouvert
epok
ERICSSON
ETRI
gemalto
security to be free
hp
invent
NEC

Novell.
NOKIA
Connecting People
NTT
PingIdentity™
Reactivity
RSA
Sun
microsystems
symLABS
Home of DirectoryScript™



SAML 2.0

(test procedure v2.0)

Company	Product	Version	IdP	IdP Extended	IdP Lite	SP Complete	SP Extended	SP Lite	ECP	Attribute Authority Responder	Attribute Authority Requester	Event Date
CA	SiteMinder®	6.0 SP5			🟩			🟩				Dec 2006
Entr'ouvert	Lasso	2.0			🟩			🟩				Dec 2006
Entrust	Entrust GetAccess™	7.1 SP2	🟩			🟩				🟩		Jul 2006
Ericsson	EIC	1.0	🟩	🟩								Dec 2006
Ericsson	EIM SPT	1.0				🟩	🟩					Dec 2006
HP	OpenView Select Federation	6.60	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Jul 2006
NTT	I-dLive	4.0	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Dec 2006
NTT Software	TrustBind Federation Manager	1.0	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Dec 2006
Oracle	Identity Management	10g	🟩			🟩						Jul 2006
Ping Identity Corporation	PingFederate	4.1			🟩			🟩				Jul 2006
Symlabs	Federated Identity Access Manager (FIAM)	3.1	🟩	🟩		🟩	🟩		🟩	🟩	🟩	Dec 2006

Going beyond user-mediated interaction

- The **Liberty Web Services** standards (ID-WSF and ID-SIS) define how identity information can flow securely as part of a web services transaction
  - Allowing users to set policy that mediates interactions silently instead
  - But providing for ways to contact users to gather informed consent, additional attributes, additional policy...
- Any one such transaction may need to identify the human sender, the invoking service, the receiving service, and the target identity
  - In looking up your colleague's calendar, *your colleague* is the target identity
  - Any of these may need to be privacy-protected

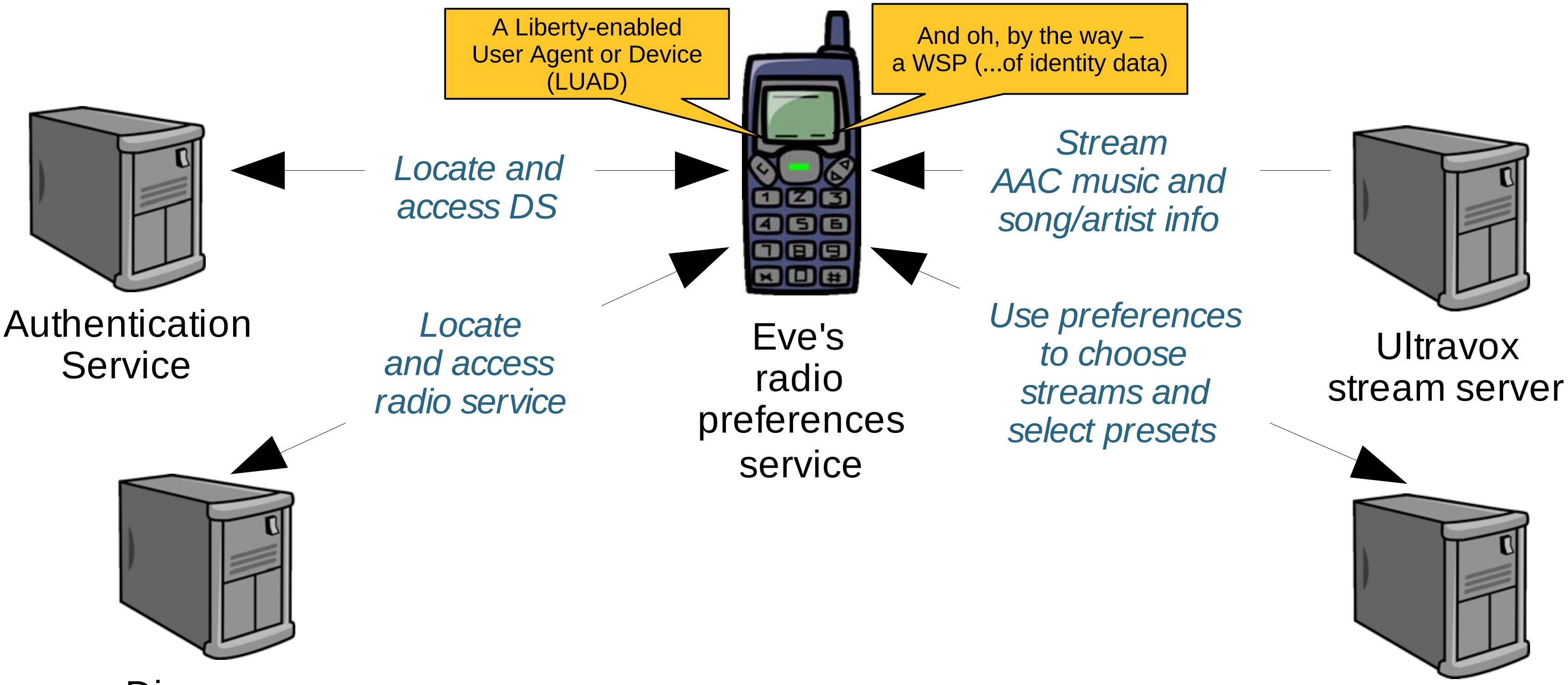
Real-life example 1: Sun-BIPAC

- BIPAC offers customized political services to Sun employees online
  - Sharing unrestricted content: easy
    - Just look for **sun.com** referrer/IP address
  - Sharing legally restricted content: not so easy!
    - **The service needs** stronger authentication, along with the user's citizenship, shareholder, and employment status
    - ...*and* **Sun and its employees need** to keep from exposing their actual identities to BIPAC, to comply with regulations and give users confidence about their “political privacy”
- Ultimately achieved with Liberty identity services – which BIPAC is now rolling out to more customers

Real-life example 2: Radio@AOL

(credits: Conor Cahill and John Kemp)

- The ultimate in user control: your personal device serves up your preferences



A Liberty-enabled User Agent or Device (LUAD)

And oh, by the way – a WSP (...of identity data)

Authentication Service
Locate and access DS
Eve's radio preferences service
Stream AAC music and song/artist info
Ultravox stream server
Locate and access radio service
Use preferences to choose streams and select presets
Discovery Service
Radio@AOL

Person-to-person federation

- The **People Service** (**PS**) lets you create reusable groups and roles involving other people's identities
  - And use them to control access to your resources
  - Even if multiple IdPs are involved
- Whereas today in (say) Flickr, you can create lists only for “friends” and “family” with Flickr IDs
  - And you can't reuse these lists with other services
    - Though you can issue “foreign” guest invitations by email
- The PS is useful for business scenarios too
  - Managing team access to resources in joint-venture projects
  - Identity proofing when a colleague loses their token

New technical work at Liberty

- The **Strong Authentication Expert Group** is currently defining requirements for interoperability among strong auth methods (ID-SAFE)
- The **Technology Expert Group** is expanding its work on advanced identity awareness in client devices
  - PCs, phones, PDAs, set-top boxes, TVs, stereo components...
  - Going way beyond commercial browsers for strong local authentication, privacy, mobility...

New Liberty communities

- The **eGovernment Special Interest Group** held a workshop in Brussels yesterday!
  - Representatives from the UK, France, Ireland, Norway, Finland, Spain, Netherland, Austria, New Zealand, Germany, and Belgium attended
- The **Concordia** program is collecting requirements around using multiple technologies and protocols together, to foster harmony

More Examples

- Country of Norway: eNorway 2009
  - “MiniSide”: Coordinated digital portal for the population, across sectors and levels of administration with significant cost savings
  - Access to healthcare, tax, motor vehicle registration, social security, student loans and other government services
- eAuthentication
  - U.S. government-wide federated authentication component for the federal enterprise architecture
  - Currently 31 Relying parties, including DoA, DoC, DoE, DoJ, NASA, Treasury, DoT, SSA

Final food for thought: Liberty and Web 2.0

- SAML, Liberty, XRI, and OpenID protocol designers have been discussing the proposition:
  - Can we move from ***incompatibility*** to ***equivalence*** to ***compatibility*** to ***convergence***?
- “Lightbulb” integration of OpenID discovery and metadata with SAML has shown one possibility
  - Existing specs for XRI SSO and Lightweight SSO may give way to an “OpenID-SAML profile”
- Additional ideas:
  - Leveraging existing attribute exchange technology in new “identity schemas” work
  - OpenID-enabled People Service

Thank you!
Questions?

Gerald Beuchelt
gerald.beuchelt@sun.com

Additional Material

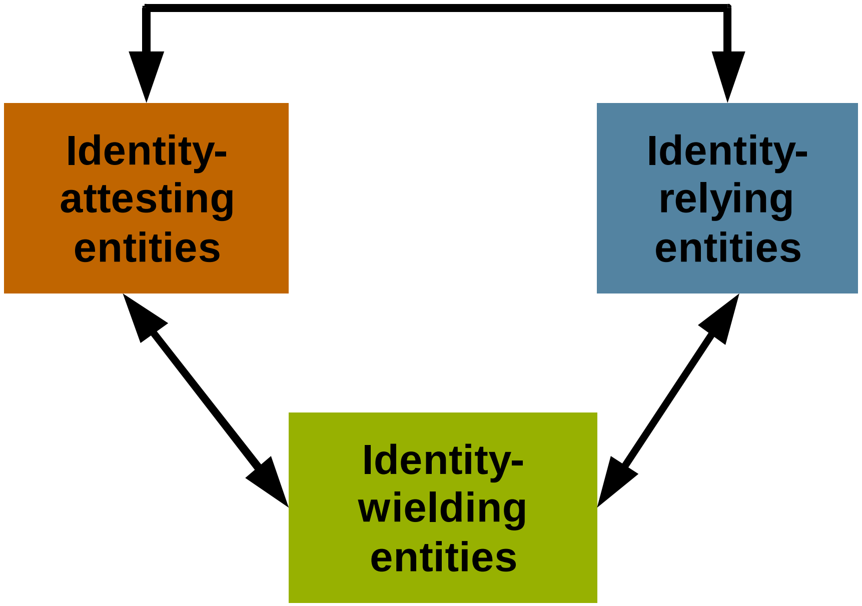
Specifications, Protocols, Links

Liberty published standards in context

- **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...


Identity-attesting entities
Identity-relying entities
Identity-wielding entities

ID-FF: Identity Federation Framework

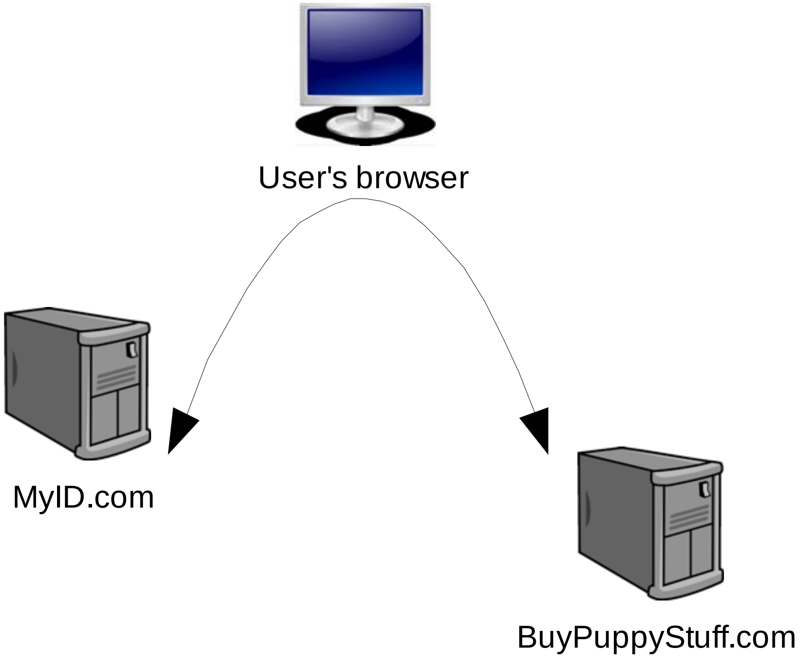
- *“Liberty Federation”*
- Focused on human-to-application interaction
- Now converged with SAML V2.0

Major benefits of ID-WSF's design

- Authentication, authorization, and application of usage policy against consumers of identity data
- User privacy through use of pseudonyms
- Dynamic service discovery and addressing
- Common web services transport mechanisms to apply identity-aware message security
- Abstractions and optimizations to allow anything – including client devices – to host identity services
- Unified data access/management model for developers
- Flexibility to develop arbitrary new services
- Support for social identity applications

The human-to-app story

- Single sign-on, single logout, etc. take place among:
  - The user (with actions mediated by a **client** of some kind)
  - An **identity provider** (**IdP**)
  - A **service provider** (**SP**) that serves as a **relying party** (**RP**)
- These actions are communicated primarily with XML over HTTP(S)

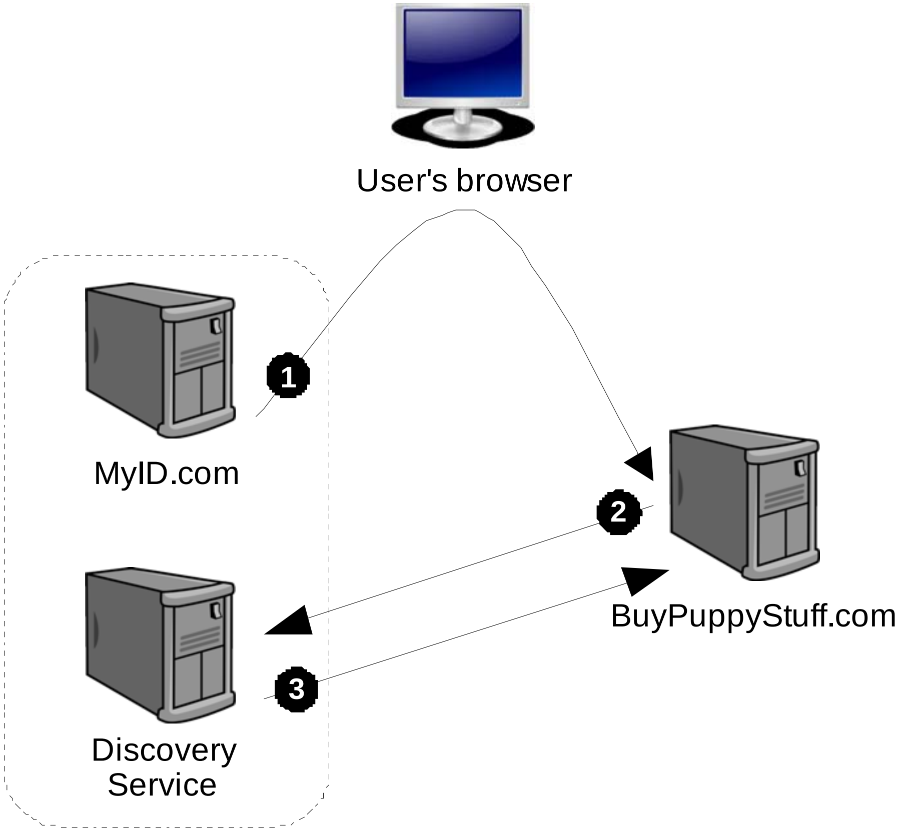


Why app-to-app interaction?

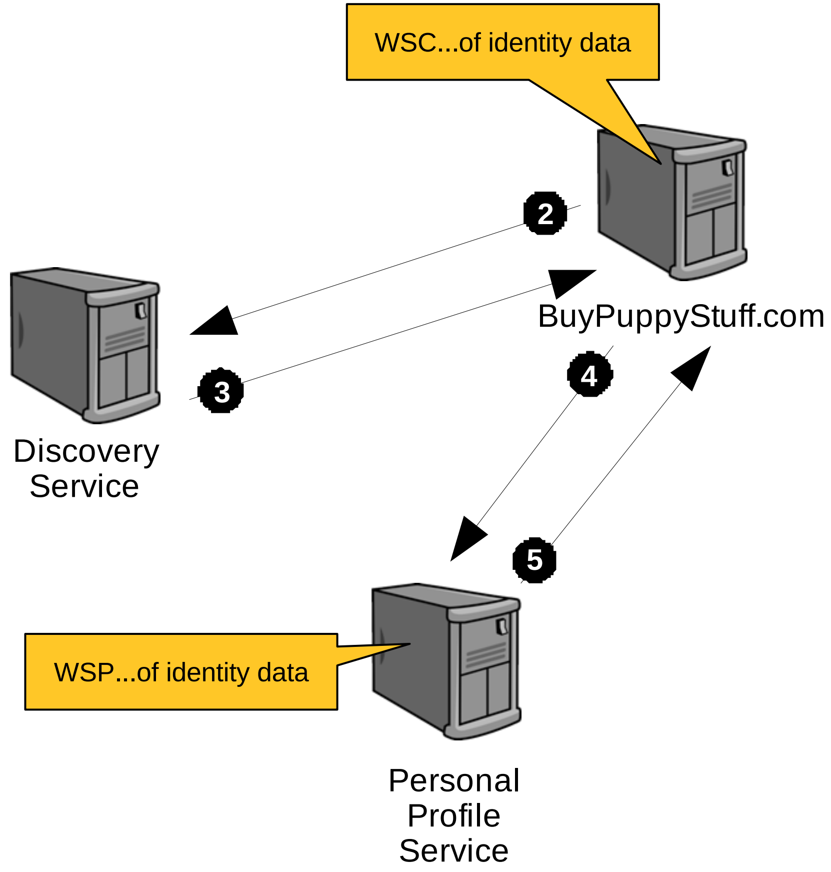
- Get around browser payload limitations
- Allow identity-enabled actions to happen silently (mediated by policy) when you're not around
  - All the way from *pay my bills automatically*...
  - ...to *let the emergency-room doctor access my medical records from another country if I'm in a coma*
- Allow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

Kicking off an app-to-app interaction

- It usually starts with a user (possibly not you!) logging in and asking for some service behavior involving your identity
- During SSO, the IdP informs the SP where to find *your* **Discovery Service** (**DS**)
  - A hub for locating, and possibly getting coarse-grained authorization to use, various identity services of yours
- In a typical deployment, the IdP and DS form one tightly coupled software component



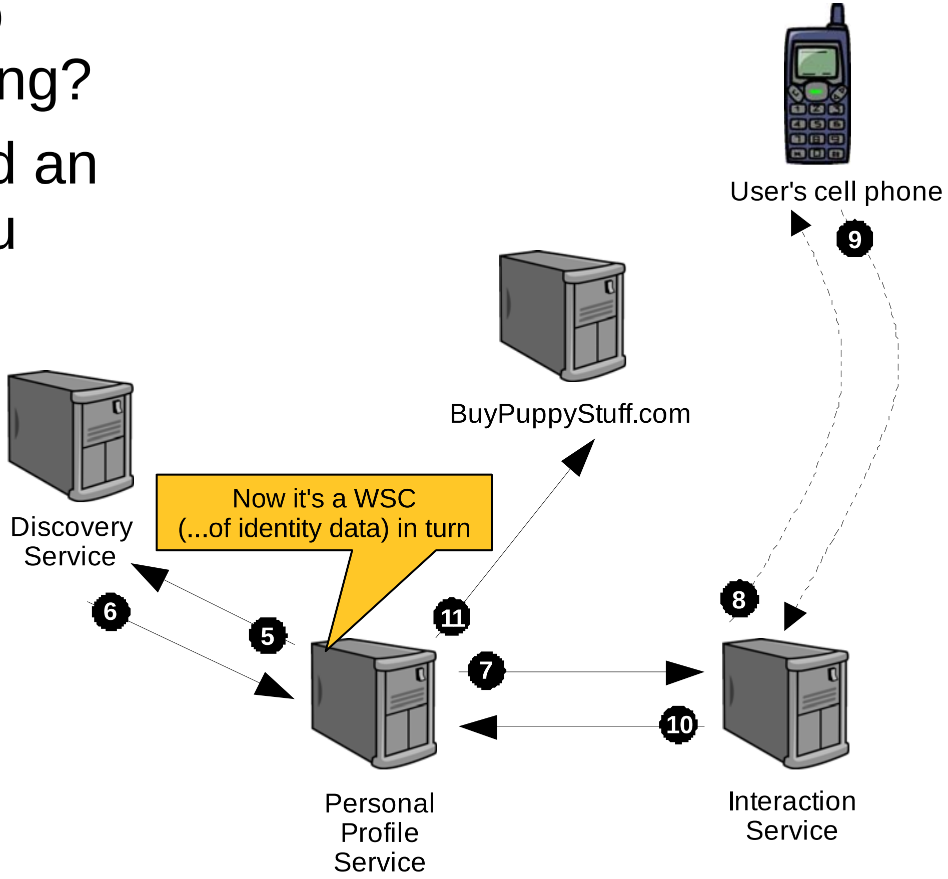
The locate-and-access dance



- The SP dons the role of a **web service consumer** (**WSC**)
  - A WSC is the requestor endpoint, and a **web service provider** (**WSP**) is the responder endpoint
  - **Tip:** Mentally add “of identity data” to remember which is which
- The WSC asks the DS where a particular WSP is, and asks for access
  - WSPs will typically do fine-grained WSC authorization themselves
- One example of a WSP is the ID-SIS **Personal Profile** (**PP**) service for name, address, etc.

Getting information-sharing approval

- What if the PP service needs to check with you before responding?
- It can ask your DS where to find an **Interaction Service** (**IS**) for you so it can bother you real-time
  - According to your own policy preferences for what's important enough to bother you with
- The PP is acting as a WSC
  - Doing the locate-and-access dance itself, just like BuyPuppyStuff did
- The IS uses non-Liberty means to (e.g.) SMS you for approval



Observations

- These logical components were included for maximum privacy and flexibility, but not every deployment needs them all!
  - And the worst case is still optimized so that devices sensitive to “protocol chattiness” can handle it
- Any identity service can “recursively” use the discovery and access system provided by the DS to call another one
- At any point a service can (attempt to) contact the user for informed consent, policies, more attributes...
- Throughout, the user might be known only by a pseudonym

Major open-source implementations

- Sun's http://OpenSSO.dev.java.net
  - SAML, ID-FF, ID-WSF in Java; SAML in PHP ("Lightbulb")
- 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!