LIBERTY ALLIANCE PROJECT

Liberty & User-centric Identity

Personal Digital Identity

- Typically no face-to-face contact when making identity claims
- Difficult to even roughly substantiate self-made claims (you say you're 21 but I can't even see you!)
- Third-party credentials seem ephemeral
- Improved technology brings privacy risks to people (e.g. correlation is easier)
- Improved technology can help resolve these (and other) personal ID management issues

What is user-centric identity?

- The user gets to make a choice about what identity information he reveals
- Choice may include “providing consent” to another, so that information may be released/asserted on one’s behalf
- Choosing means that the user may be granted, denied, or provided a different level of access to a service based on her choice

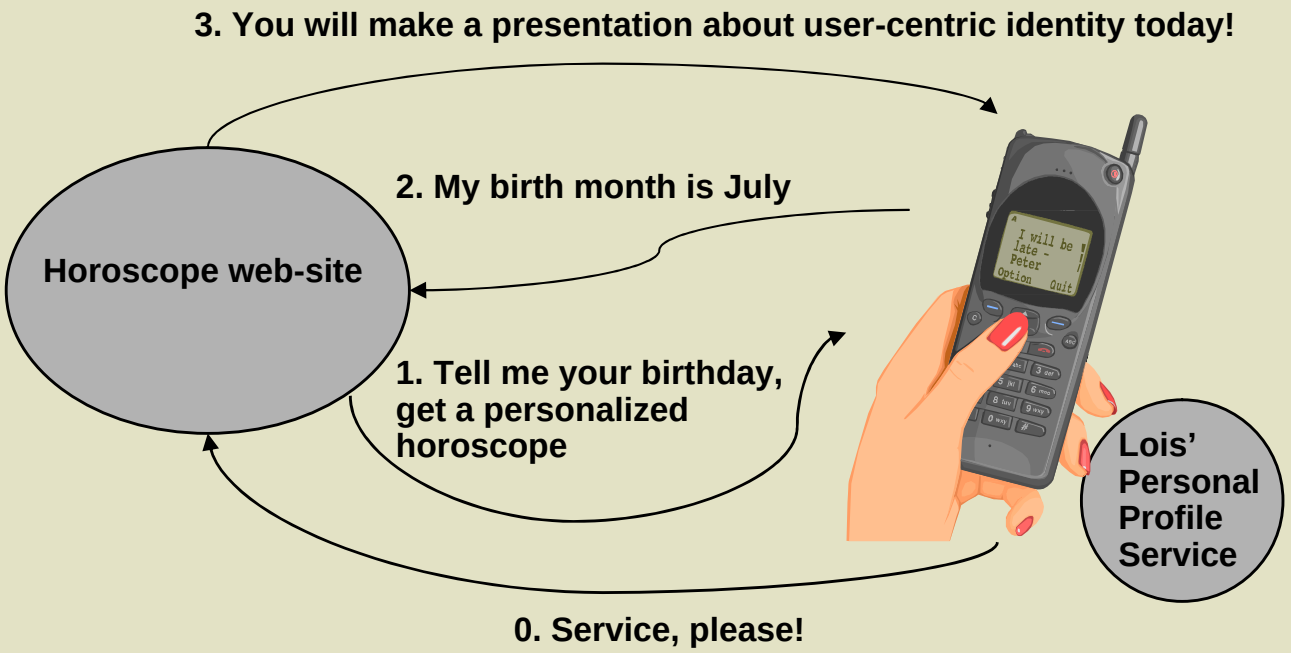
Liberty & User-centric Identity

- ID-WSF Identity Services (e.g. Personal Profile) can make (signed) identity claims on behalf of a user
- Liberty ID-FF is simply *web-browser* based SSO
- Identity Provider can make (signed) identity claims on behalf of a user (including a claim about authN status)
- Service provider redirects the user to their identity provider - through the web browser - with no user interaction!
- LECP profile of ID-FF 1.2 (now also part of SAML 2.0) allows user to explicitly select identity provider (and thus identity).
- LECP is a special case of an identity service - an “authN request/response forwarding service!”
- Any identity service can run on a user-operated device (such as a mobile phone or a PC)
- ID-WSF Personal Profile service provides similar information to that now given by a Microsoft “Infocard”

Personal Identity Services

- Liberty ID-WSF specifies a framework for providing identity services
- An identity service is one which makes claims about some identity (my age is 21…again!)
- Identity services might be provided by a user-operated device (not just a server) using PAOS
- PAOS allows a user agent (with no fixed IP address!) to advertise services it can provide via an HTTP header

Personal Identity in Action



Liberty-enabled Clients and Proxies

- User browses to service provider (SP), advertising support for LECP (via HTTP header)
- SP sends authentication request (AuthNReq) to LECP (i.e. to user agent)
- LECP forwards AuthNReq to identity provider (IdP)
- LECP can choose to authenticate both SP and IdP
- LECP can itself potentially act as an IdP
- LECP was submitted with ID-FF 1.2 specifications to SSTC and is now also part of SAML 2.0

LECP interactions

Summary

- Personal identity services can be user-centric, regardless of where they are located
- Personal identity services are possible today with Liberty ID-WSF and ID-FF LECP
- LECP is a user agent-based “identity selector” for web browser-based SSO
- All ID-WSF identity services can be run on devices and software closely associated with a user

Further reading

- http://www.projectliberty.org/about/whitepapers/Personal_Identity.pdf (Personal Identity whitepaper)
- http://www.projectliberty.org/specs/draft-liberty-idff-bindings-profiles-1.2-errata-v2.0.pdf (section 3.2.4 - LECP profile of ID-FF)
- http://www.projectliberty.org/specs/liberty-paos-v1.1.pdf (concerning the advertisement to HTTP servers of identity services running on a “client”)
- http://www.projectliberty.org/specs/liberty-idwsf-client-profiles-v1.1.pdf (processing rules and guidelines for creating identity services on “clients”)