A handful of Identity Solutions

• SAML (OASIS)
  • exchanging authentication, authorization and related data, generally between secured domains

• OpenID (OpenID Foundation)
  • decentralized standard for authentication, primarily for access control

• OAuth (IETF)
  • distributed, secure API-style authorization for access to services and data over HTTP

• InfoCards (Information Card Foundation)
  • user-centric authentication, authorization and attribute exchanging, focus on privacy
Venn of Identity

**SAML**
- Framework for addressing a variety of security, privacy, and trust goals
- Extensive web SSO profile with attribute transfer
- Reusable security token format
- IdP discovery is typically handled out of band, varying by use case
- Integrates with web services; is XML-based

**OpenID**
- Simple scripting-friendly SSO protocol for Web-wide identity
- Supports attribute transfer via extension
- Its original design prioritized Web scalability over security
- IdP discovery is solved by dereferencing the ID of the user or IdP

**InfoCard**
- Client-centered WS-* profile and interface for attribute transfer and user authentication with consent; can be used with SSO
  - Addresses security and privacy goals such as phishing resistance and IdP-to-RP unlinkability
  - IdP discovery is built into card mechanism

Eve Maler – VennOfIdentity.org
Acknowledgments: Gary Ellison, Johannes Ernst, Paul Madsen, Jeff Hodges, Ashish Jain, many others
**Venn of Identity**

**SAML**
- Framework for addressing a variety of security, privacy, and trust goals
- Extensive web SSO profile with attribute transfer
- Reusable security token format
- IdP discovery is typically handled out of band, varying by use case
- Integrates with web services; is XML-based

**OpenID**
- Simple scripting-friendly SSO protocol for Web-wide identity
- Supports attribute transfer via extension
- Its original design prioritized Web scalability over security
- IdP discovery is solved by referencing the email of the user or IdP

**InfoCard**
- Client-centered WS-* profile and interface for attribute transfer and user authentication with consent; can be used with SSO
- Addresses security and privacy goals such as phishing resistance and IdP-to-RPunlinkability
- IdP discovery is built into card mechanism

**OAuth**
- Web-centric API for HTTP authN and distributed authZ
- Delegated access
- Message security
- Focuses on codifying current web practices
A handful of Standards Bodies

- IETF
- OpenID Foundation
- OASIS
- Information Card Foundation
A handful of Standards Bodies

• IETF
• OpenID Foundation
• OASIS
• Information Card Foundation OASIS
A handful of Standards Bodies

• IETF
• OpenID Foundation
• OASIS
• Information Card Foundation

• 3GPP
• APEC
• GSMA
• HITSP
• IDABC
• ISO
• ITU-T
• NHIN
• NIST
• OMA
• UN/CEFACT
• W3C
• WS-i
A handful of Standards Bodies

- IETF
- OpenID Foundation
- OASIS
- Information Card Foundation
- 3GPP
- APEC
- GSMA
- HITSP
- IDABC
- ISO
- ITU-T
- NHIN
- NIST
- OMA
- UN/CEFACT
- W3C
- WS-i
A handful of Standards Bodies

• IETF
• OpenID Foundation
• OASIS
• Information Card Foundation

• 3GPP
• APEC
• GSMA
• HITSP
• IDABC
• ISO
• ITU-T
• NHIN
• NIST
• OMA
• UN/CEFACT
• W3C
• WS-i
Identity Sherpas

• Will Norris
  • OpenID, XRD, Shibboleth
• Scott Cantor
  • SAML, Shibboleth
• Drummond Reed
  • XRI, XDI, Information Card
• Leif Johansson
  • OAuth