Digital Identity in Perspective

John Tolbert
May 2011
History

• Users
• Groups
• ACLs
• RBAC
• ABAC
• PBAC
• PABAC
• RAdAC
The machinery of identity

- LDAP directories
- Web access management systems
- Identity federation
- Public key infrastructure
- SmartCards
Different communities, different identities

- Education
- Enterprise
- Government & defense
- Health care
- Finance
- Retail
- Social media
Digital identity: not an end-in-itself
Issues

- Identity providers?
- Standards support & interoperability
  - SAML
  - OpenID
  - oAUTH
- Movement of emphasis from identity to access control, audit, and privacy
- Data protection
- Platform assurance
Data Protection

We must find innovative ways to protect data within all levels of electronic systems:

1. Inventory data
2. Categorize data
3. Tag/mark data with meaningful metadata
4. Cryptographically bind metadata to data objects
5. Allow administrators to grant permissions to individual data elements, based on user/device/application identities as well as resource metadata, actions, and environmental factors.
The Road Ahead
The Road Ahead

- The “role” of identity
  - Balanced with access control, privacy, etc.
  - Platform assurance
  - Encourage work of Trusted Computing Group

- Extend existing standards and profiles
  - SAML
  - XACML
  - OpenID, oAUTH

- Interoperability of identity concepts, products, and protocols, across multiple platforms and multiple sectors: Kantara Initiative