Identity Management Systems Research

Jim Dray, IDMS Program Manager
NIST

A Vision of Global eID

- I hold a smart card with a secure private key, public key certificate and biometric
- Anywhere in the world, a relying party can ask the card to prove my identity
- I unlock the card by submitting my biometric, and the card proves possession of the private key by signing a challenge
- I am granted access to a broad range of services

Desirable Properties

- My card works seamlessly everywhere
- I control my private information
- Relying parties can trust my proof of identity, and I can trust them

My Card Works Everywhere

- Federation: The ability to recognize identities from another domain
- Interoperability
  - Platform: Soft/hard token, interfaces, etc.
  - Credentials: Data formats, namespaces, etc.
- Federation models are not necessarily interoperable (even PKI-based ones…)

Control of Private Information

- User centricity
  - Different credential profiles (health care, transit, telecom, eGov services)
  - Minimize information trails
- Clear understanding of what information will be collected and how it will be used
- How to securely tell a soft/hard token which credential objects to release?

Trust

- The purpose of an identification system is to bind an identity and associated set of attributes to an individual
- Trust between relying party, identity provider and individual
  - Mutual authentication
- Audit of the enrollment process, secure protocols

Landscape

- **Many ongoing attempts to implement Identity Management**
- **International examples**
  - ICAO ePassports, ILO Seafarer's card, EC Manchester Ministerial Directive '05
- **U.S. examples**
  - HSPD-12(PIV), RealID, Transportation Worker's ID card

Research Topics

- Common models
- Ontology, namespaces
- Interoperability
- Why do we want globally interoperable eID?
- What is an identity, and what aspects of it do we need/want to manage?

Thanks for listening!

james.dray@nist.gov