2nd Nationwide Health Information Network Forum:
Health Information Network Security and Services
October 16-17, 2006

Panel Discussion

Provider Authentication and Authorization

Raja Kailar, Ph.D.
CTO, Business Networks International Inc.
Connecting for Health NHIN Team

EXPERIENCE. RESULTS.

HIN Service Provider Access Control Models

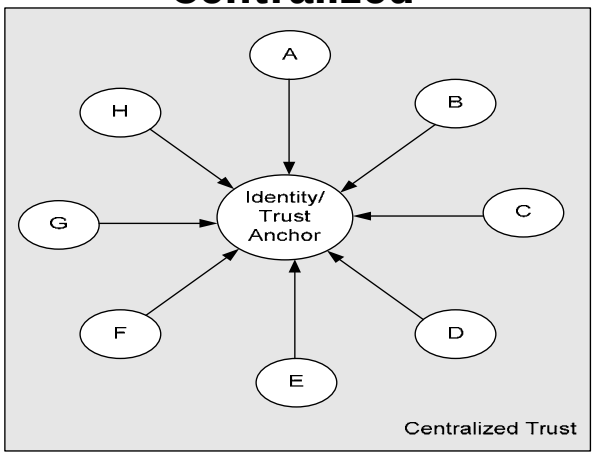
- **Model 1: HIN Service Provider Performs User Level Access Control**
  - Pros
    - Fine grained, direct control
    - Lesser dependency on other systems policies/processes
  - Cons
    - Harder to manage, scale
    - Identity synchronization/mapping

- **Model 2: HIN Service Provider Relies on Edge System (or Proxy) for User Level Access Control**
  - Pros
    - More scalable, manageable
    - No user directory synchronization/mapping
  - Cons
    - Coarse grained (organization level) access control
    - Requires higher level of trust on edge system or proxy

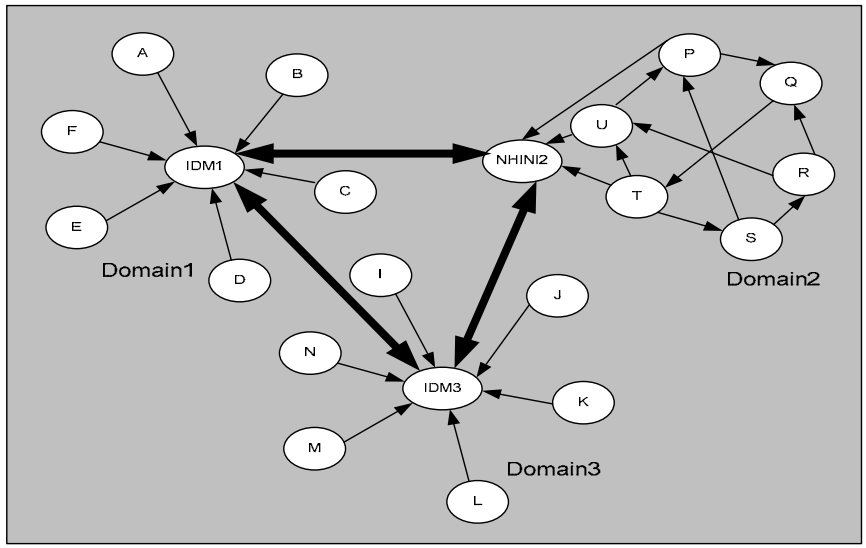
Provider Authentication and Authorization

Trust Models for Authentication/Authorization

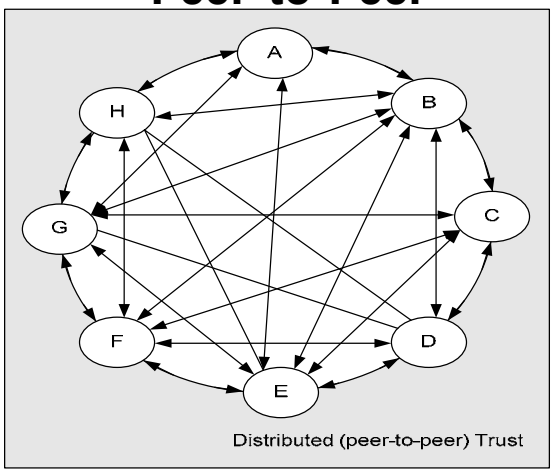
Centralized



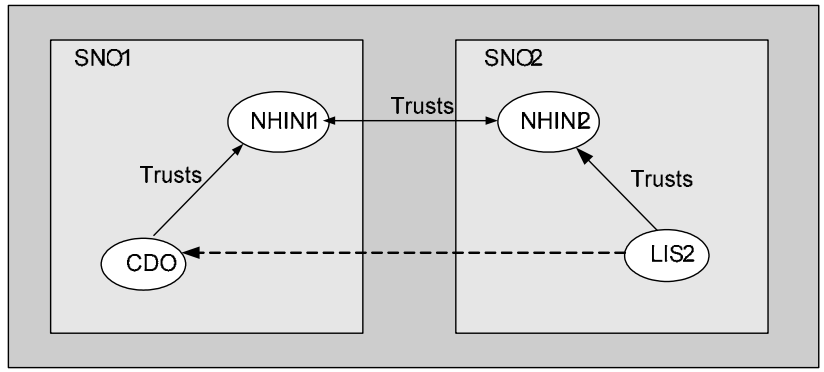
Mixed



Peer-to-Peer



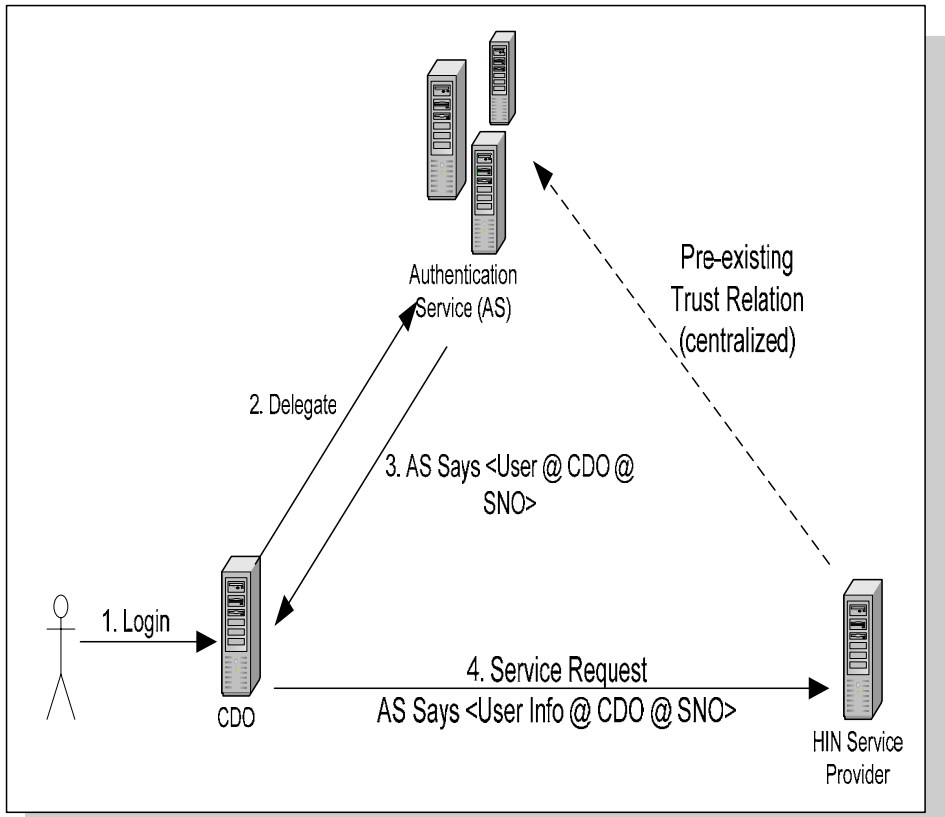
Transitive



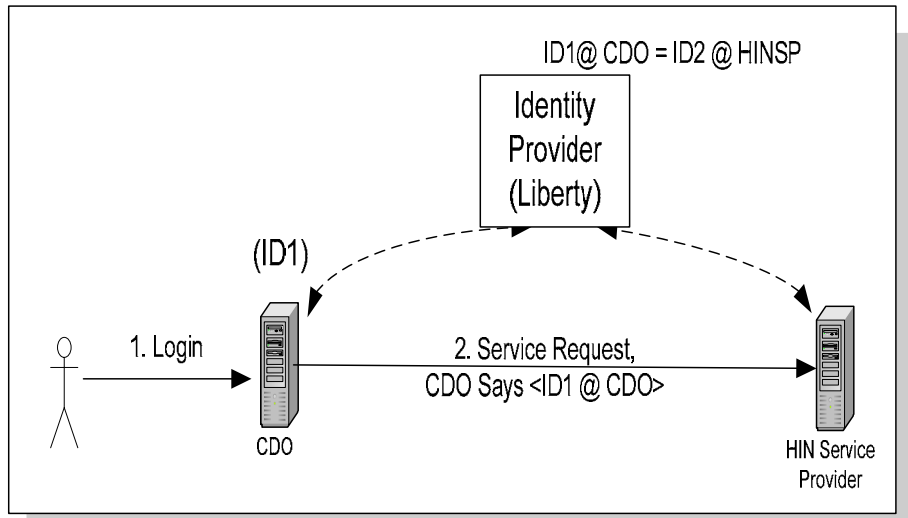
Provider Authentication and Authorization

User Level Authentication/Authorization Models

Centralized Identity/Authentication (Microsoft Passport Model)



Federated, With Identity Mapping (Liberty Alliance Model)



Comparison of User Level Authentication/Authorization Models

- **Centralized**
  - Pros
    - Single user repository, no synchronization
    - Ease of maintenance
    - Uniform implementation, fewer trust relationships
  - Cons
    - Single point of failure/vulnerability
    - Loss of local control
    - Scalability of central node
    - Tight coupling with central service

- **Federated**
  - Pros
    - Local control of user identities
    - Uses existing networks and trust relationships to build new ones.
    - Privacy (e.g., user aliases)
  - Cons
    - Directory synchronization/mapping
    - Complexity of different implementations across the network (interoperability)
    - Dependence on prior business agreements and remote systems security processes

Information Exchange for Access Control and Audit

Provider Attributes (Identity, Role, Location, Organization, SNO)

- Standards
  - NPI, SAML 1.1/2.0, WS-Security, WS-Federation, Liberty Alliance 1.0/1.2
- Issues
  - Identity federation standards are evolving
  - Which standards are applicable to NHIN?
  - Provider roles
    - » Standard vocabulary
    - » Policies for establishing roles
  - Lack of Liberty Alliance compliant identity providers and applications

Small Providers (With no real "Edge System")

- **Provider Portal Services**
  - Provider a subscriber, not an employee of Portal Service
    - Does Portal Service use same rigor when enrolling providers as a CDO enrolling provider as an employee/partner?
  - Need policies for "minimum level" of Identity proofing, Authentication (e.g., e-Authentication standards)
    - High Minimum:
      - » Pros: High security
      - » Cons: Complexity, High entry barrier
    - Low Minimum:
      - » Pros: Relatively lower complexity
      - » Cons: Relatively lower security
  - "Minimum level" needs to strike balance between security and ease of implementation/use.

Making Legacy Systems Interoperate

- Well established mechanisms in SNOs/Edge systems. Many are proprietary.
- Standards adherence for identity/authorization assertions communication and access control
  - Pros
    - » Higher degree of interoperability
    - » More data sharing
    - » Better experience for end users
  - Cons
    - » Complexity, cost
    - » Need new business and trust relationships (e.g., with identity providers)
- Initially, may require higher reliance on trust assumptions and “reactive” enforcement (e.g., audit) to lower entry barrier.

Provider Authentication and Authorization

CSC/CFH Approach to Provider Authentication and Authorization

- Network Trust model – mix of centralized and peer-to-peer
- Transitive trust (*CDO* ←→ *ISB1* ←→ *ISB2* ←→ *Lab*)
- Legally binding agreements enforce trust assumptions (CFH Policy Framework)
- HIN Service Providers currently (prototype) rely on provider identification and authentication at edge system (CDO / Lab)
- Extensible to do more fine grain access control at HIN Service Providers using "assertions" (local policy at HINSP)
  - Evaluating SAML 2.0 assertions for communicating user attributes
- Until NHIN policies/standards available, identity proofing, authentication are driven by local policies
- Auditing at each node and legal recourse for breaches of confidential information