Trust and Identity

• Why It Matters
  – An Identity Layer for the Internet
  – Benefits for the Rest of the Stack

• What It Is – Technologies and Policies
  – Campus and Organization
  – National and Global

• What are the current issues
  – Interfederation and federated incident handling
  – Attribute release and consent
  – Metadata evolution
  – Sustainable open source infrastructure and TIER
An identity layer for the Internet

- Provides interoperable identity and access control
  - Identities – Identifiers - Attributes
- Core to security and privacy
- Stretches from campus to national federation to international
- Reaches far beyond technologies to business processes and wetware
Federated Identity & Access Management

1. Single sign on
2. Services no longer manage user accounts & personal data stores
3. Reduced help-desk load
4. Standards-based technology
5. Home org and user controls privacy
6. Service controls access based on attributes
7. Operations cross institutional boundaries
   - So typical notions of control don't apply
   - Trust becomes a key condition of operation
Benefits for Networking and Security

- Networking
  - Eduroam
  - Enable and control access to VPN’s, SDN, etc.
  - Map mobile devices to identities
- Security
  - User authentication and authorization
  - Scalable access control
Benefits to Research and Cloud Services

• Research
  – Enable DMZ capabilities
  – Single secure login to multiple CI resources
  – Collaboration platforms

• Cloud Services
  – Provisioning of campus identity, authentication and groups into the cloud services
  – Putting a campus IdP into the cloud
From campus to international

• Campus
  – Operate (either on premise or in the cloud) a basic set of identity management systems for their users and their extended community
  – Establish campus policies and procedures on the key identity issues, including authentication, authorization, attribute release and consent, etc.

• National Federation
  – Bind signing keys for organizations to those organizations and distribute those keys securely
  – Assign end-entity tags on organizations for discovery, attribute release, etc; establish reference attribute schema; distribute attribute release profiles to participants; other duties as assigned

• International
  – Exchange metadata internationally among national federations
  – Try to make semantic sense out of wild diversity
Key Technologies

- Protocols
  - SAML and Shibboleth, OpenID Connect, OAuth, PKI
  - Metadata management
    - Signing keys, end-entity tags, static and dynamic metadata management
- Payloads
  - Eduperson
    - A collection of normative “on-the-wire” attributes and controlled vocabulary for identity and relationships
  - Group memberships, accessibility schema, personalization attributes, etc.
- Policies – Levels of Assurance (LOA), end-entity tags, etc.
Basic functional model

- Identity providers (IdP’s)
- Service providers (SP’s/RP’s)
- Identity Gateways
  - converts Social2SAML
- Portals
  - Typically science gateways to domain resources
  - commercial
- Attribute authorities
- Federation operators
Current issues

• Interfederation and federated incident handling
• Attribute release and consent
• Metadata evolution
• Sustainable open source infrastructure and TIER
• Some items are no longer unsolved issues
  – MFA is happening
  – Transport protocols are heading for interop – e.g. OpenId and SAML
  – Command lines mechanisms emerging (ECP)
Edugain membership
InCommon and interfederation

- InCommon has joined eduGAIN
  - Has a metadata service ingestion mechanism being tested
    - Starting dynamic metadata testing within InCommon
  - Exporting InCommon metadata into eduGAIN also in the plans
    - First IdP’s, then SP’s
    - Opt in/out sets of issues
- Exposes the next set of critical issues, some of which are very hard
  - Attribute release internationally
  - Inconsistent international semantics of common attributes
- Other forms of interfederation also probable – K-12, other verticals
Federated incident handling

• Concerns of major science service providers that if they go the federated route, they need to be notified by IdP’s of compromised accounts relevant to the service provider.
• Crosses identity – security perimeters on campus
• To automate will require new campus infrastructure (e.g. identity event log harvesters) and inter-campus mechanisms (incident routing)
• “Sir-T-FI” initiative helping to define and solve the problem
• Aligns well, surprisingly, with some innovative commercial sector thoughts
• Stay tuned
Attribute Release and Consent

- Attribute release is proving very problematic
  - Attribute retentive institutions
  - Selective release of values from a multi-valued attributes is not yet solved
  - Social IdP’s have set a promiscuous release bar
- Several tools being used
  - Research and Scholarship (R&S)
  - Consent
- Multiple protocols, regulation
- Efforts underway to create usable and scalable consent
Metadata Evolution

- Metadata is increasing in size and complexity
  - Growth in new participants, interfederation, end-entity tags, etc.
  - Size is affecting distribution and usage
- Moving to dynamic metadata
  - Similar to the shift from /etc/hosts to DNS
  - Metadata protocols in development and standardization
  - Need additional mechanisms to work through registration of participants and trust paths.
- Urgent and important and hard
- See reep.org, samlbits.org
Sustainable open source

• Grant-funded successes need to become sustainable open-source infrastructure
• Efforts in Europe and the US
• TIER – Trust and Identity in Education and Research
  – an Internet2 effort to solidify, integrate, and fill in the gaps in open-source IdM software
  – Shib, Grouper, person registries, provisioning, directories, consent, local federation managers, collaboration platforms, etc.
  – API’s, code and cloud service offerings part of the plan
• Other parts of the software cyberinfrastructure need sustainability too.