



R&Ethinking Trust

Ken Klingenstein, Internet2

with discussant Rich Guida, Johnson and Johnson

- *Requirements: The Trust Continuum*
- *Theory of Federated Trust*
 - Definition
 - Transports
 - Models/Architectures
 - Trust quarks
- *Practice of Federated Trust*
 - Internal, Closed, and Open Federations
 - Liberty pilots
 - Shibboleth pilots
 - Others
- *Emergent issues*
 - Multiple federations – connections, overlaps
 - User interfaces
 - Role of PKI – where to put pieces of trust

The Continuum of Trust

- *Collaborative trust at one end...*

- can I videoconference with you?
- you can look at my calendar
- You can join this computer science workgroup and edit this computing code
- Students in course Physics 201 @ Brown can access this on-line sensor
- Members of the UWash community can access this licensed resource

- *Legal trust at the other end...*

- Sign this document, and guarantee that what was signed was what I saw
- Encrypt this file and save it
- Identify yourself to this high security area

Dimensions of the Trust Continuum

• Collaborative trust

- *handshake*
- *consequences of breaking trust more political (ostracism, shame, etc.)*
- *fluid (additions and deletions frequent)*
- *shorter term*
- *structures tend to clubs and federations*
- *privacy issues more user-based*

• Legal trust

- *contractual*
- *consequences of breaking trust more financial (liabilities, fines and penalties, indemnification, etc.)*
- *more static (legal process time frames)*
- *longer term (justify the overhead)*
- *tends to hierarchies and bridges*
- *privacy issues more laws and rules*



The Trust Continuum, Applications and their Users

- *Applications and their user community must decide where their requirements fit on the trust continuum*
- *Some apps can only be done at one end of the continuum, and that might suggest a particular technical approach.*
- *Many applications fit somewhere in the middle and the user communities (those that trust each other) need to select a approach that works for them.*



Federated Trust Definition

- *An interrealm approach – enterprises are realms, and they mutually join into federations to conduct business*
- *For the consumer marketplace, users subscribe to commercial service offerings to interact with business federations; enterprises that might offer consumer services include desktop OS's (Microsoft), ISP's (AOL), Telecoms (Nokia, telco's), consumer product vendors (Ford, United Airlines) and banks (Chase)*
- *Such Identity Service Providers (ECP) need to exchange trust amongst themselves and with others*
- *User brokers with local domain on the release of information within the federation*
- *User trusts local domain, local domain trusts federated member, federated member trusts local domain, all trust federation management*
- *Trust is used to accept or reject assertions or requests for attributes*

- *At one level (run-time)*
 - X.509 identity certs and their mutants
 - X.509 attribute certs
 - SAML
 - S-expressions, etc....
- *At another level (static storage and management)*
 - Roles
 - Attributes
 - Personal factors
 - Information sources...

- *Hierarchies*

- may assert stronger or more formal trust
- requires bridges and policy mappings to connect hierarchies
- appear larger scale

- *Federated administration*

- internal – within the subsidiaries of large corporations
- private – between several corporations for specific business needs
- Public – open to qualified enterprises for general uses

- *Virtual organizations*

- Shared resources among a sparse, distributed set of users
- Grids, virtual communities, some P2P applications
- Want to leverage other trust structures above

- *Where one makes the decision to trust (believe, reject, believe with constraints)*
- *The interrealm acquisition of trust info*
 - a priori
 - Coming with the assertions
- *Trust enforcement points*
- *Closely related to Authzanity*

- *The human aspect of trust*
- *A pool of atomic trust units*
- *Not fixed, can increase or decrease from feedbacks*
- *Come in flavors*
 - Personal
 - Legal
 - Financial
 - Risk factors also apply
- *Cause every theory needs them...*

• *A group of organizations (universities, corporations, content providers, etc.) who agree to exchange attributes using common transport protocols. In doing so they also agree to abide by common sets of rules.*

• *The required rules and functions could include:*

- A registry to process applications and administer operations
- A set of best practices on associated technical issues, typically involving security and attribute management
- A set of agreements or best practices on policies and business rules governing the exchange and use of attributes.
- The set of attributes that are regularly exchanged (syntax and semantics), including namespaces.
- A mechanism (WAYF) to identify a user's security domains
- Ways to federate and unfederate identities

- *At one level, federations are enterprise-oriented PKI*
 - Pure server-server PKI
 - XML DSig and SSL are perhaps the most widely used PKI today...
 - Local authentication may well be end-entity certs
 - Name-space control is a critical issue
- *At another level, federations have differences with classic PKI*
 - End user authentication a local decision
 - Flat set of relationships; little hierarchy
 - Focus as much on privacy as security
 - Web Services only right now: no other apps, no encryption

Functions for a Federation

- *Metadata management (signing keys, WAYF names, admin contacts, etc.)*
 - Collection
 - Distribution
 - Integrity- I/A, revocations of enterprise certs
- *Trust components*
 - Enterprise
 - Signing operations
 - Privacy protection
 - Attribute integrity
 - Client
 - End user authentication
 - May be centralized or decentralized in implementations
- *What else...(Federated identity operations?)*



Types of federations

- *Internal – within large corporations, among their subsidiaries*
- *Private (bilateral and small multilateral) – between trading partners, supply chains, etc.*
- *Public – InCommon, e-Authentication*



Public and Private Federations

Public federations need to think more about:

- *rules of engagement to participate in the federation and how it operates*
- *persistence of trust*
- *migration of installed base*
- *process for standardizing attributes that are exchanged*
- *privacy*
- *international issues*



Our Goals

A single infrastructure to support collaborative and legal trust

- *perhaps multiple transports for trust*
- *multiple levels of security*
- *nurture rather than mandate*
- *Integrate PKI and SAML*
- *Strengthen the role of the enterprise*
- *Build a public sector marketplace for identity and attributes*



Points of Control for the Relying Party in a Federation

- *Note: both origins and targets are relying parties...*
- *In Shibboleth terms...*
 - A target can choose whether to include a given origin in its WAYF presentation and use
 - Per individual resource, a target can determine whether to trust the assertions of a given origin
 - Per target, an origin can decide what requests for attributes it will respond to
 - Per target, an individual can decide what attributes they want their origin to release

Handling risk in federations

- *User and Origin*

- risk is privacy spill or blocked access;
- origin does its best to release attributes correctly and as user wishes and user relieves origin of risk

- *Origin and Target*

- Risk is inappropriate access to content
- origin does its best to release attributes that are correct and target relieves origin of risk

- *Target and Origin*

- Risk is privacy intrusion
- Target disposes of attributes as quickly as possible and origin and/or user relieves target of risk

- *WAYF – that it is run properly*

- Risk is improper certification of institutional signing key
- WAYF can disclaim responsibility



Federations in the last year

- *Communicator Hub ID is one of the pioneering Liberty Alliance-based services on the market, supporting vertical-industry B2B offerings such as SecuritiesHub. SecuritiesHub, which is sponsored by eight leading Wall Street investment firms, including Credit Suisse First Boston, Goldman Sachs, JPMorgan, Lehman Brothers, Merrill Lynch, Morgan Stanley, Salomon Smith Barney and UBS Warburg.*
- *Liberty Alliance (<http://www.projectliberty.org/>)*
- *Federal e-Authentication Initiative (<http://www.cio.gov/eauthentication/>)*
- *Not much use of federated .NET*
- *Shibboleth and InCommon (<http://middleware.internet2.edu/shibboleth>)*



The Practice of Federations

- *SecuritiesHub*
 - Using Liberty-compliant software
- *Microsoft delegating control of names spaces for Passport*
- *InCommon*
- *NSDL*
- *Local federations*
 - The UT-Houston Medical Complex
 - Pennsylvania Higher Ed Assistance Group

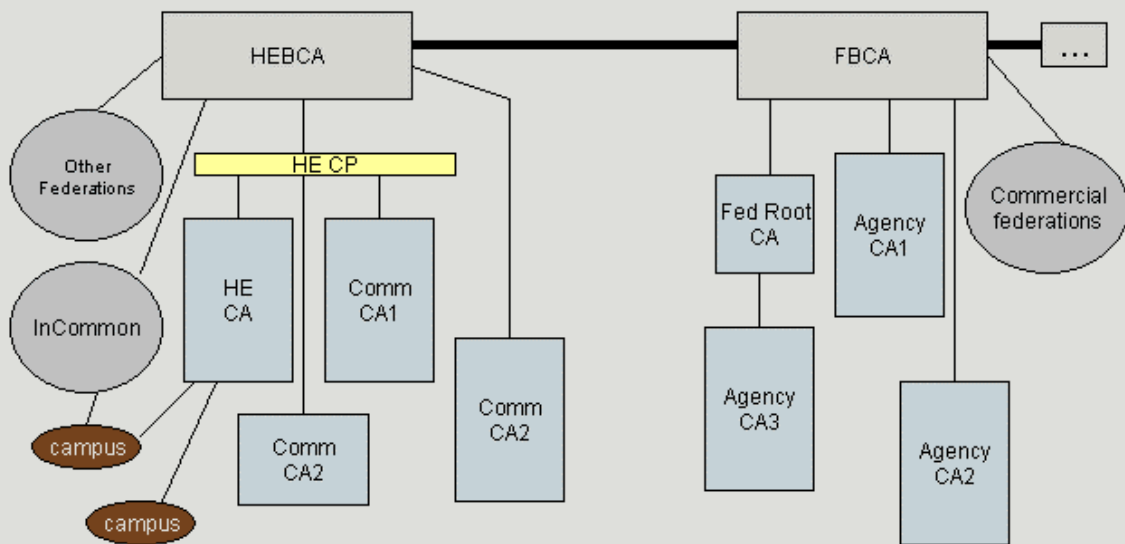


Federating organizations organization (FOO)

- *To explore the issues in federations, and multiple federations, and subclubs, and...*
- *Includes GM, Securities Industry, Johnson and Johnson, Microsoft, Fed e-AuthN, etc.*
- *Monthly discussions with minutes...*
- *Friends of foo as an email list to stay informed of the discussions*

Overall Trust Fabric

Trust diagram





InCommon Description

InCommon provides a framework for sharing network-accessible resources and information among a growing number of federated universities and companies. InCommon participants develop, deploy and promote technology, agreements and common practices that support the trusted delivery of goods and services



InCommon Activities

- *Current*
 - Process applications for admission into origin list or for being a target
 - Manage central WAYF and distribution of InCommon feed (members and their keys)
 - Member services – information, key revocation; no tech support
- *As needed in a while*
 - Development and posting of policies: authentication, privacy, etc.
 - Target contracts
- *As needed long-term*
 - Extra-federation relationships
 - Certification of origins
 - Consensus standards for LOA's, audits, etc...



Current InCommon Policy Issues

- *Origin and Target Distinctions*
 - Origins are participants; targets apply to use the way
- *Scope of participants*
 - Would like to limit it at first to I2 members, but there are important non-members in the pilots
- *Process to set direction*
 - All of NPPAC, subgroup, other
- *NSDL deployment*
 - Overlapping federations
- *Legal Issues*
 - Handling Risk
 - Establishing Trust

Major issues

- *Multiple federations*
 - Different release policies (cash rebates for identity)
 - User confusion
 - Interfederation
- *Relying party controls – credit cards vs PKI*
- *Weak SSL cert issuing processes*
 - Define assurance levels and processes for enterprises
- *Conservation of trust*
 - How much of the trust requirements of a federation should be addressed by the enterprise PKI aspect (e.g. the CA, the CP format, etc.)
- *Management of privacy*
 - How much does a user want?
 - How much can a user manage?



Open Questions

- *What are the similarities and differences between bridged PKI and federations?*
- *What does the concept of federated PKI really mean?*
 - Can XKMS be realized?
 - Is a federated PKI with global uniqueness = ($>$, $<$) than classic PKI



CREN CAat Current Status

- *17 Certs issued*
- *No one asking yet for more*
- *MIT ready to resume operations*



CREN CA@ Proposed Next Steps

- *Operational plan*
 - Set up storefront at Internet2
 - Establish a CP
 - Use MIT for continued operation
- *Types of certificates issued*
 - Only enterprise
 - Would work with outsourcers like NSC
- *Expected purposes that campuses would use them for*
 - As institutional keys for InCommon
 - Signing server certs
 - Issuing student webauthn certs
 - Signing campus S/MIME certs
 - Experimentation
- *July 1 target date*



One possible trajectory

- *HE defines several CP's*
 - One for enterprises to issue end-entity
 - One for shib-strong-ssl server certs
 - Others?
- *The CREN CA agrees to issue certs as above*
- *We do an RFP for vendors to respond*