Integrated Business, Legal and Technical Architecture

*Kerberos Conference*
*October 2012, MIT*

Dazza J Greenwood, JD
Lecturer, MIT Media Lab
President, CIVICS.com
BLT System Rules Approach

• CIVICS.com has a structure & method for agreeing business, legal & technical integrated system rules for Identity Federations, enabling participants to better define, avoid, reduce, mitigate, shift, absorb and manage risks.
National Contexts and Scenarios

• US NSTIC and IDESG development of an Identity Ecosystem Framework featuring accreditation with certification of base-line compliance by Trust Frameworks

• UK Identity Assurance development of Scheme Rules for large scale provision of identity services.
Business Contexts and Scenarios


Overview: **BLT Rules Architecture**

- Explicit BLT Use Cases and Context
- Same BLT Roles, Relationships & Definitions
- Including BLT key rules in one agreement reduces delays, cost and confusion about ID Federation.
- The rules are deliberately, traceably & obviously first defined & driven by business scenarios, requirements & constraints.
- The legal and technical rules, by appearing as sections of a single document can clearly support and reflect the business drivers.
Insurance & Financial Services Industry Example **BLT Rules Methodology**

- Requirements and Approvals Align to BLT Executives of Each Partner
  - Business: CEO/COO/CFO (Sales/Logistics/Ops)
  - Legal: General Counsel/Compliance
  - Technical: CIO/CTP/CSO
Insurance & Financial Services Industry Example BLT Rules Methodology

• Cross-Industry Legal Team, Business Team and Technical Team, Each Accountable for Defining Their Respective Sections of the System Rules.

• CIVICS.com Facilitation & Drafting Support for Teams & Among Team Chairs To Harmonize & Integrate BLT System Rules Architecture

• Key Stakeholder Executive Level Leadership on Steering Committee, Later Became Board of Directors. Board Approves and Publishes Rules.
Identity Use Cases 0.1
Business, Legal and Technical
Attribution and Content

• IIW Session by John Biccum and Dazza Greenwood, May 30, 2012
• Use Cases intended to identify basic use cases comprising the federated identity
• Intended for use by ABA Task Force and other Standards Groups developing ID Use Cases
• For the Long Story: http://civics.com/use-cases/
Dimension of Integrated Use Case

• “Business Context: Scope/Purpose, Roles/Relationships and Transactions”
• “Legal Context: Parties/Contracts, Rights/Responsibilities & Decisions”
• “Technical Context: Standards/Technology, Actors/Actions and Security”
Basic Identity Use Cases

- USE CASE #1: Workplace SSO, “Tightly Bounded Circle of Trust”
- Use Case #2: Public Sector Issued Identity Credentials and Token
- Use Case #3: Mass-Market Consumer “Lightly Bounded” Reusable Identity
Use Case #1 Business Dimension

"Circle of Trust" of All Participating Business Partners

Business Relationship Between Transacting Companies

Role in Marketplace

Buying Company

Purchasing Manager

Role in Marketplace

Selling Company

#1 Log Into Partner Company Application

#2 Conduct Business Transaction (Purchase Order)

Catalog of Goods and Ordering Process
Use Case #1 Legal Dimension

Existing Commercial Contracts Between Partners

System Rules of Trust Framework for Federated Identity

Participation Agreement

User Authority

Agent of Company

Participation Agreement

#1 Assertion of Employee Identity

#2 Conduct Transactions on Behalf of Employer

Relying Party

#2 Electronic Agent and Automated Transaction
Use Case #1 Technical Dimension

Federation Network and Central or Shared Services

Configured End-Points Between Two Domains in Federation

Expected Metadata and Server Address

User Authority

Approved Client or Device of User

#1 Assertion and Authentication of Asserted Identity.

#2 Authorization, Access Control & Session mgmt.

Expected Metadata and Server Address

Relying Party

#1 Identity Server

#2 Application Server
Possible Vision

- [http://youtu.be/8BnjeWO03Qs](http://youtu.be/8BnjeWO03Qs)
Update: MIT Work on Core ID
Basic Concept

Various Realms of Identity

Innocent Citizen

Identity as an Employee
Vis Employer, Co-Workers, Suppliers, Customers, etc.

John Public

Identity as a Citizen
Vis voting (local), driving (state), taxes (federal), etc.

Johnson Qwerty Publico

Identity as a Consumer/Customer
Vis supermarket, video store, attorney, doctor, amazon, etc.

Johny Public

Identity as a Parent/Parishioner
Vis spouse, children, neighbors, place of worship, friends, clubs, etc.

JoJo, aka Qwert aka Q-Ball
Core ID Starts With a Seed

Following Slides are from Draft MIT White Paper

- Seed Registry (Offline Secure)
- Deliver Immutably Obluscated ID
- Core Identifier Registry
  - Issue/Validation Service
  - Revocation/Archival Service
- Secure transfer of Core ID
- Persona Provider (PP)
  - Issue/Validation Service
  - Revocation/Archival Service

- Citizen Authorizes Creation of seed identifier
- Citizen Authorizes Identifier Creation & Transfer into New Persona

Seed Identifier → Core Identifier → Persona
Core ID Spawns Downstream ID
Relying Parties Access Persona

Citizen

Persona "Bob"

Attribute: Age > 18

Attribute: Reside in MA

Attribute: Credit Score > 700

Mass. DMV

MyFICO.com

Relying Party (RP)

amazon.com

Validate “Age” and “Residence” Attribute Claims

Validate “Credit Score” Attribute Claim
Persona Can Be Deleted or Ported
Archive is Essential

Citizen

Legal Identifier(s)

Citizen authorizes creation of seed identifier (based on legal identifiers) and storage at operator

Authoritative Seed Service Provider

contract

contract

contract

Seed Registry Operator

Seed Registry (Offline Secure)
More Information

• [www.CIVICS.com](http://www.CIVICS.com)

and

• [http://eCitizen.mit.edu](http://eCitizen.mit.edu)

Dazza Greenwood, 650.504.5474

dazza@civics.com or dazza@media.mit.edu