Information Security
And
Privacy Advisory Board Meeting

Government Identity Projects
&
REAL ID

“Getting to Know You;

Getting to Know **All** About You”

Dan Combs

- President, Global Identity Solutions, LLC
  - Identity Policy, System and Service Consulting
- At-Large Board Member EC3
- Program Director, MIT Real ID Forum
- Member, Harvard Policy Group
- Dan.combs@globalidentitysolutions.com

REAL ID is Real

2 Steps Forward?

REAL ID

- Alive and Well-real fight is about money
- Replacement bill(s) likely
- Replacement bill passage-good odds
- Current Notice of Public Rule Making until early May
- Opportunity to use existing and developing identity infrastructure, EAF, EAP, PIV, Real ID to provide comprehensive ID functions for citizens

REAL ID

- EC3 REAL ID is Real Workgroup
- MIT Real ID Forum: MIT Online Forum: The Real ID Act of 2005
- MIT NPRM Online Forum:
- MIT NPRM Comment Session—April 11 1:00

Privacy Today

WHY?

- No One builds (or should build) an Identity system for the sake of building an identity system, but a lot of us act as if we are doing just that
- Let people in, keep people out, interact with the right people, machines, organizations, software
- Identify stuff--enrollment, verification: generally consists of something you know and/or something you can get your hands on

- Credentialing - provisioning
- Authenticating – using the credentials
- Federating
- Policy, Process, Technology, Audit
- Others have spent hundreds of millions so you don’t have to

How Do We Know Thee?
Let Me Count the Ways.

- FBCA (Federal Bridge Certification Authority--PKI)
- TWIC (Transportation Worker Identification Credential)
- TTP/RT (Trusted Traveler Program/Registered Traveler)
- HSPD 12 (Homeland Security Presidential Directive 12)
  - FIPS 201 (Federal Information Processing Standard 201
  - PIV (Personal Identity Verification of Federal Employees and Contractors)
- FIXS/DCCIS (Federation for Identity Cross-Credentialing Systems/Defense Cross-Credentialing Identification System)
- EAI (E-Authentication Initiative)
- EAP (E-Authentication Partnership)
- InCommon/InQueue Shibboleth-based systems
- State of Iowa Identity Security
- PhRMA-SAFE (Secure Access For Everyone/Signatures and Authentication for Everyone)
- REAL ID
- Multiple state and local projects
- Many others

Important Considerations/Components

- Governance
  - Sponsorship at high enough level
  - Proper set of Stakeholders involved in decision-making
  - Fast and Flexible: IT changes quickly, government does not
- Business Model
  - Who Pays Whom and How
- Liability
- Rules and Policies
  - Robust enough to guide, light enough to adapt
- Processes
  - Trustworthy
- Proof
  - Audit
- Technology
  - Communicate, compatible, interoperable

Identity Security Done Right

- Tried to Involve stakeholders inside and outside of government
- Identified broad range of users
- Involved users in development
- Focused on rapidly adaptable, flexible user-centric model
- Built a Sustainable Business Model

The Real ID Act of 2005

- End of life as we know it.

From NTIS website http://www.ntis.gov/hottopics/wildlandfires.asp

- Sliced bread

Not Your Daddy’s Drivers License

- Real ID (notice the big ID)
- Identity takes prominent (preeminent?) role
- Country-wide Federated Identity System (Not national id)
- Basis for developing identity system
  - Create/Improve privacy
  - Improve security
  - Help protect citizens and provides tools for self-protection
  - Improve identity functions
  - Integrate identity functions into wide range of commerce, interactions and transactions for government and non-government participants

RIDA--What It Is

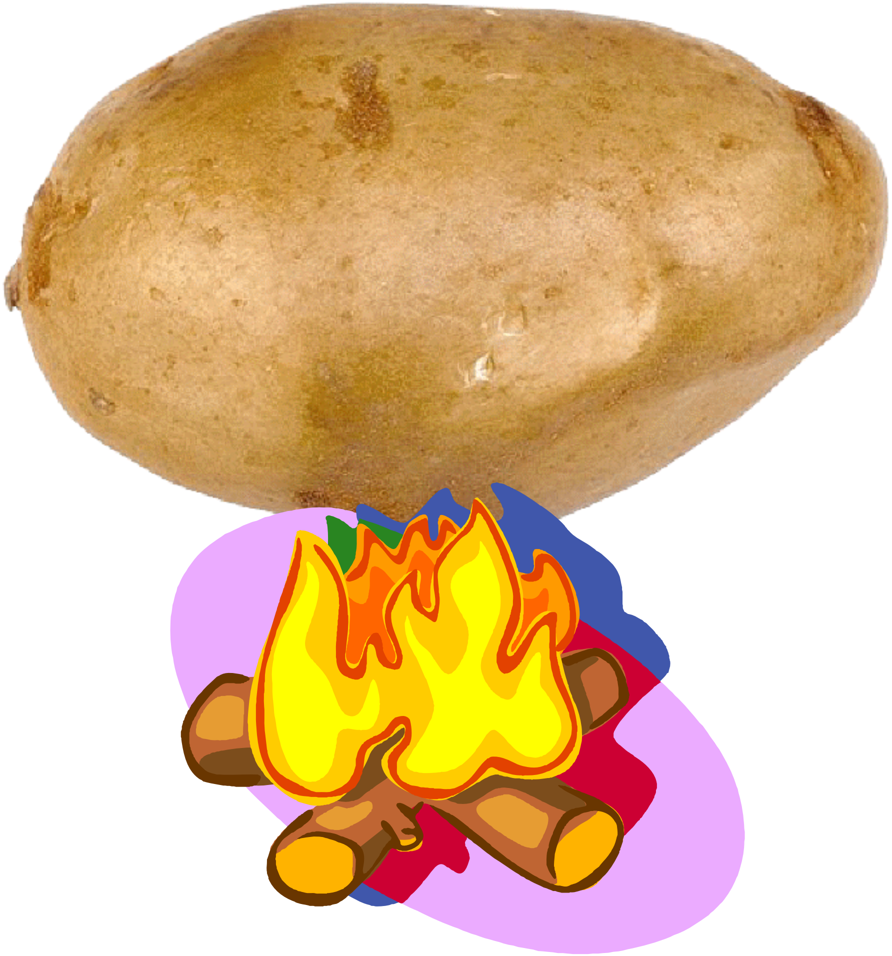
- The Real ID Act mandates minimum document requirements, specifying “information and features” on Real ID’s as follows:
- The person's full legal name.
- The person's date of birth.
- The person's gender.
- The person's driver's license or identification card number.
- A digital photograph of the person.
- The person's address of principle residence.
- The person's signature.

RIDA--What It Is

- Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.
- A common machine-readable technology, with defined minimum data elements.
- The Act specifies the presentation, scanning, retention and verification of identifying documents, the verification of legal status of an applicant, confirmation that any prior issued driver’s license or ID is cancelled. RIDA mandates participation by states to meet these requirements.
- DHS responsible administrative agency with to develop rules

Congress Was Not Handing Out Favors

- “Go build a country wide identity credentialing system without calling it a national ID”
- Minimal funding
- January 2007--Rules not out yet
- May 2008 “deadline”



Right Answer-Wrong Question

- The 9-11 terrorists obtained both legal and fraudulent drivers’ licenses
- Some in Congress believed this should be prevented
- The drivers’ licensing system will not likely be an effective barrier to dedicated terrorists obtaining government credentials
- Sledge hammers and mosquitoes
- A well-designed and well-built identity system can have lots of other really good outcomes

Secure Registration-ID Verification

- Clean
  - Yours, mine and ours, all ID data is dirty
  - Scour the data you have
  - Verify new information
  - Learn to provisionally trust all of it: it will be wrong so plan accordingly
- Collect
  - Capture user-asserted information
  - Verify where possible
- Connect
  - Build connections between important ID documents and systems

Credentialing

Physical Credential ⟷ Digital Credential

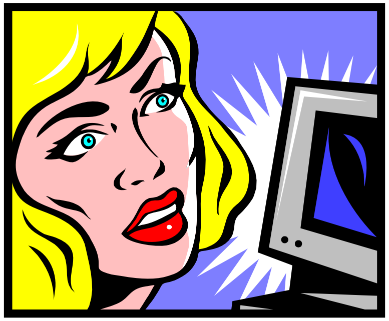
Issue

Manage

Revoke

Biometrics

In-person/Online



Assume we have an Identity

Most Identity work begins here

- Driver's License
- Birth Certificate
- Social Security Number

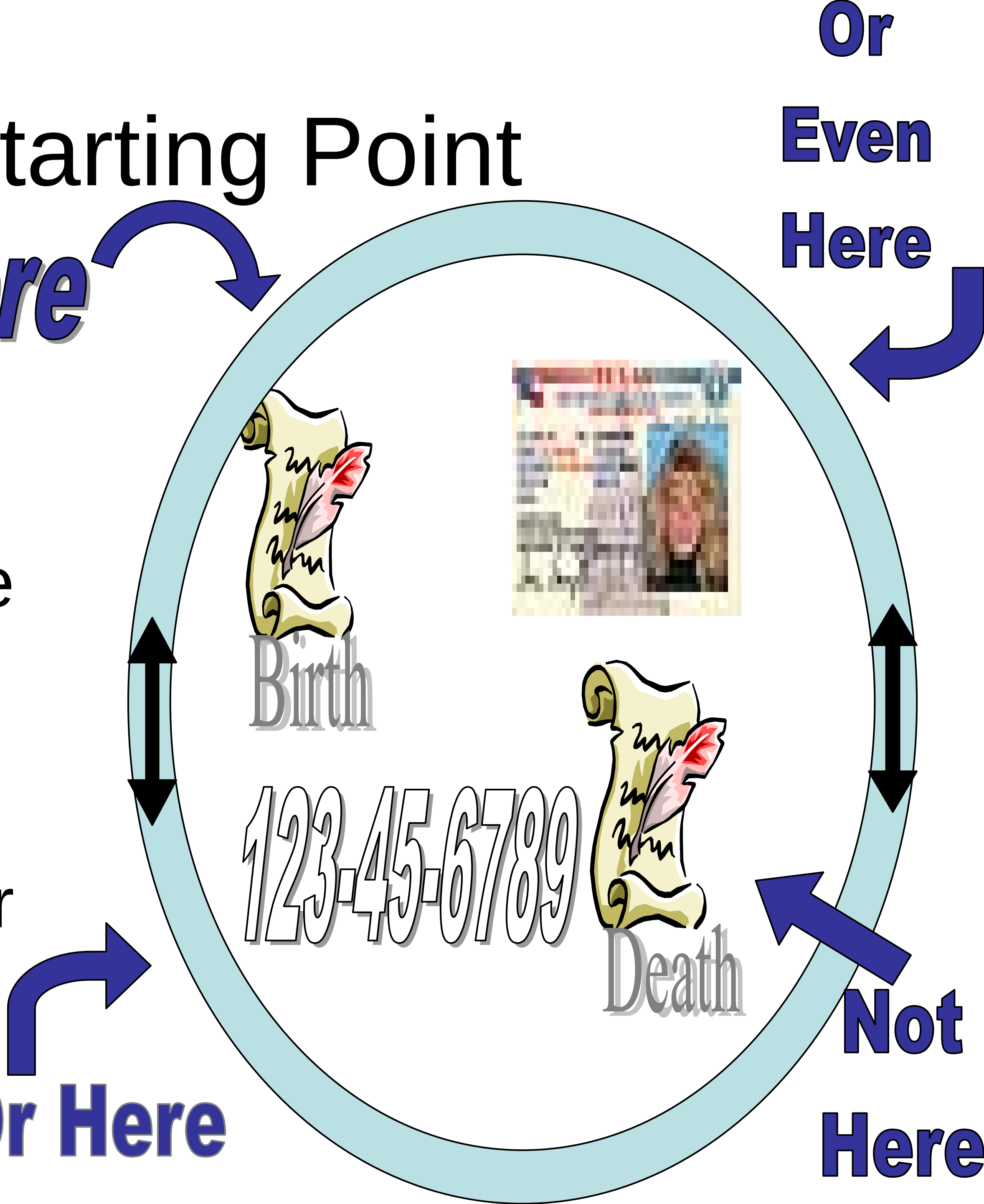
123-45-6789

This information is not very clean or accurate. Secure registration is vital.
Collect it; Clean it; Connect it.

A Starting Point

Start Here

- We need a beginning
- Identity is a core function of gov't (for now) and should not be performed as add-ons to other programs
- Secure Registration



Or Even Here

Birth

123-45-6789

Death

Or Here

Not Here

Identity Security

123-45-6789

Birth

Death

WHY?

Good Outcomes

- Identity functions are necessary. No good way to perform them
- Improve privacy
- Improve security
- Has anyone experienced or do you first-hand know someone who has experienced Identity theft or fraud?
- Decrease effects of Identity crimes
  - Reduce government losses
  - Reduce commercial and individual losses
- Decrease costs
- Improve Government service
- Facilitate business
- Loosen coupling of Government functions to Government; allow private sector opportunities
- Catalyze integration and transformation
- Reduce electronic functional friction

Real ID Issues

Ignore lessons of the Past, Rinse, Repeat

- Ignored lessons learned from Negotiated Rules process under Patriot Act
- No significant budget
- No ongoing operational system or program
- No ongoing governance
- No supporting business model or notice that one might be needed
- DHS alone; Ignored existing relationships between Department of Transportation and likely implementers—DMV's and DOT's
- Omitted other Federal agencies and other levels of government from law and rule-making
- Ignored many other stakeholders

Real ID Issues

- Too much attention to detail
  - Technological solutions written into law
  - Document requirements written into law; some contradict decisions made elsewhere for public and individual safety and policy goals
- Too little attention to big operational issues and outcomes
- Introduces concepts not defined or ill-defined in law (full legal name)
- Creates system of (potentially multiple) duplicate records of Birth Certificates and other supporting documents
- Synchronization issues; possibly multiple “official” versions of documents
- Creates different retention schedules for paper and electronic versions of supporting documents and in some cases shorter than life of REAL ID

Real ID Issues

- Calls for or assumes systems not in place or even planned
- Assumes information capability not available anytime soon
- Stops short of appropriately connecting the supporting documents or records
- Dramatically expands mission of drivers' license issuing agencies; some will consider new operating units and authorities internal or external to existing organizations

Real ID Issues

- Resistance among States
- New Congress
- Some calls for repeal
- Replacement bills drafted including Sununu/Akaka bill

REAL ID Federation

- Political, Practical and Legal considerations lead to Federation Model
- DHS personnel decided to initiate federation of state participants to mitigate/resolve some RIDA issues and assist in rules development and vetting
- Significant existing body of work on Federation development
- Several Identity Federations developed in recent years
- Growing body of support material, documentation and expertise
- A number of us noisy, pushy people who want to see Real ID become what it should be

ID Federations
Knock. Knock.

- Response to a need
  - Verification
  - Authentication
  - Access
  - Interaction
  - Transaction
  - Integration
  - Transformation
  - Shared costs
  - Common infrastructure/standardization

Challenges
Governance

- Allowing for and gaining participation of stakeholders
- Serious conflicts of interest among stakeholders
- Rapid response requirements for rapidly changing environment
- Potentially huge winners and losers

Challenges
Policy & Business Rules

Policy and Business Rule development maintenance and operation is at best herding cats. Sometimes the cats are small, cute and play nicely together.

Challenges
Policy & Business Rules

Other times not.

RIDA Business Models

- Money! It’s a gas.
  - Where does it come from?
  - Where does it go?
- Taxes
- Drivers pay through drivers’ license fees
- User transaction fees
- Data Sales
- Relying party fees
- Private sector investment and commercial models

Long Range
Reengineer Government

- Verified and Valid Identity of Individuals makes a lot of Government services easier
  - Issue licenses
  - Grant permission
  - Distribute benefits
- Loosely coupled Government functions leads to opportunities for non-government providers (think TurboTax and Kelly Solutions)
- Improve Privacy
- Fight Identity crimes
- Integration and transformation
- Cut cost of government, cut size of government, reshape government to better serve citizenry

Reengineer Everything Else

- Extend identity services beyond government
  - – further shares costs
  - – opens opportunities for non-government sector changes
  - – Can provide better individual access and control of personal information
  - – Improve user/customer service
  - – Simplify user experience
  - – Ease international travel, commerce and other interaction and transaction

Conclusion
The Real ID Act of 2005

- End of life as we know it.

From NTIS website http://www.ntis.gov/hottopics/wildlandfires.asp

- Sliced bread

Appendix

- These slides include additional detail on topics in this presentation including links to reference documents and resources.

Government and Related Identity Federations and Projects

- These pages include links and addresses to documentation and resource information.

FBCA

Federal Bridge Certification Authority

- http://www.cio.gov/fbca/
- http://www.cio.gov/fpkipa/drilldown_fpkipa.cfm?action=pa_welcome_page
- The Federal PKI Policy Authority (FPKIPA) sets policy governing operation of the U.S. Federal PKI Infrastructure, composed of: the Federal Bridge Certification Authority (FBCA); the Federal Common Policy Framework Certification Authority (CPFCA); the Citizen and commerce Class Common Certification Authority (C4CA) and the E-Governance Certification Authority. The FPKIPA approves applicants for cross certification with the FBCA.
- The FBCA (fpkipa.gsa.gov) is an information system that facilitates an entity accepting certificates issued by another entity for a transaction. The FBCA functions as a non-hierarchical hub allowing the "relying party" entity to create a certificate trust path from its domain back to the domain of the entity that issued the certificate, and then to test that path using the requirements set forth in X.509 to determine whether the offered certificate contains the requisite level of trust to allow the transaction to consummate.
- Policy, Process, Audit
- Technical Interoperability

Transportation Worker Identification Credential

- http://www.tsa.gov/what_we_do/layers/twic/index.shtm
- TWIC is an acronym for Transportation Worker Identification Credential. TSA has tested a system-wide common credential that can be used across all transportation modes. TWIC can be used for all personnel requiring unescorted physical and/or computer access to secure areas of the national transportation system. TWIC was developed in response to threats and vulnerabilities identified in the transportation system. TWIC was developed in accordance with the legislative provisions of the Aviation and Transportation Security Act (ATSA) and the Maritime Transportation Security Act (MTSA).
- The TWIC will positively tie the person to their credential and to their threat assessment. The credential can then be used with the local facility access control system to allow unescorted access to those in possession of a valid TWIC card.

Transportation Security Administration

Registered Traveler

- http://www.tsa.gov/what_we_do/layers/rt/index.shtm
- The Transportation Security Administration and private industry are developing the Registered Traveler program to provide expedited security screening for passengers who volunteer biometric and biographic information to a TSA-approved RT vendor and successfully complete a security threat assessment. The program is market-driven and offered by the private sector with TSA largely playing a facilitating role.
- Sponsoring entities (airports/airlines) and service providers (vendors) provide the necessary systems and processes to support RT, with TSA performing a limited, inherently governmental role such as providing the security threat assessment for adjudication and program oversight, as well as conducting physical screening at TSA checkpoints
- The Registered Traveler (RT) concept, as indicated in the Registered Traveler (RT) Model, has been authorized under the Aviation and Transportation Security Act (ATSA) as a means to **"establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs."** In order to establish an interoperable, vendor-neutral RT program for airline travel, the Transportation Security Administration (TSA) will partner with the private sector using a public-private partnership model.
- Standards http://www.tsa.gov/assets/pdf/RT%20Standards.zip

Homeland Security Presidential Directive/Hspd-12

- http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html
- Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

FIPS 201

- In response to HSPD 12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems.
- Incorporates three technical publications:
  - 800-73 “Interfaces for Personal Identity Verification” specifies the interface and data elements of the PIV card
  - 800-76, Biometric Data Specification for Personal Identity Verification” specifies the technical acquisition and formatting requirements for biometric data of the PIV system
  - 800-78, “Cryptographic Algorithms and Key Sizes for Personal Identity Verification” specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system

Personal Identity Verification (PIV)
of Federal Employees / Contractors

Computer Security Resource Center - CSD

- http://csrc.nist.gov/piv-program/index.html
- 800-96 PIV Card to Reader Interoperability Guidelines (http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf)
- Draft Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification (http://csrc.nist.gov/publications/drafts/800-76-1/SP800-76-1_draft.pdf)

FiXs

The Federation for Identity and
Cross-Credentialing Systems

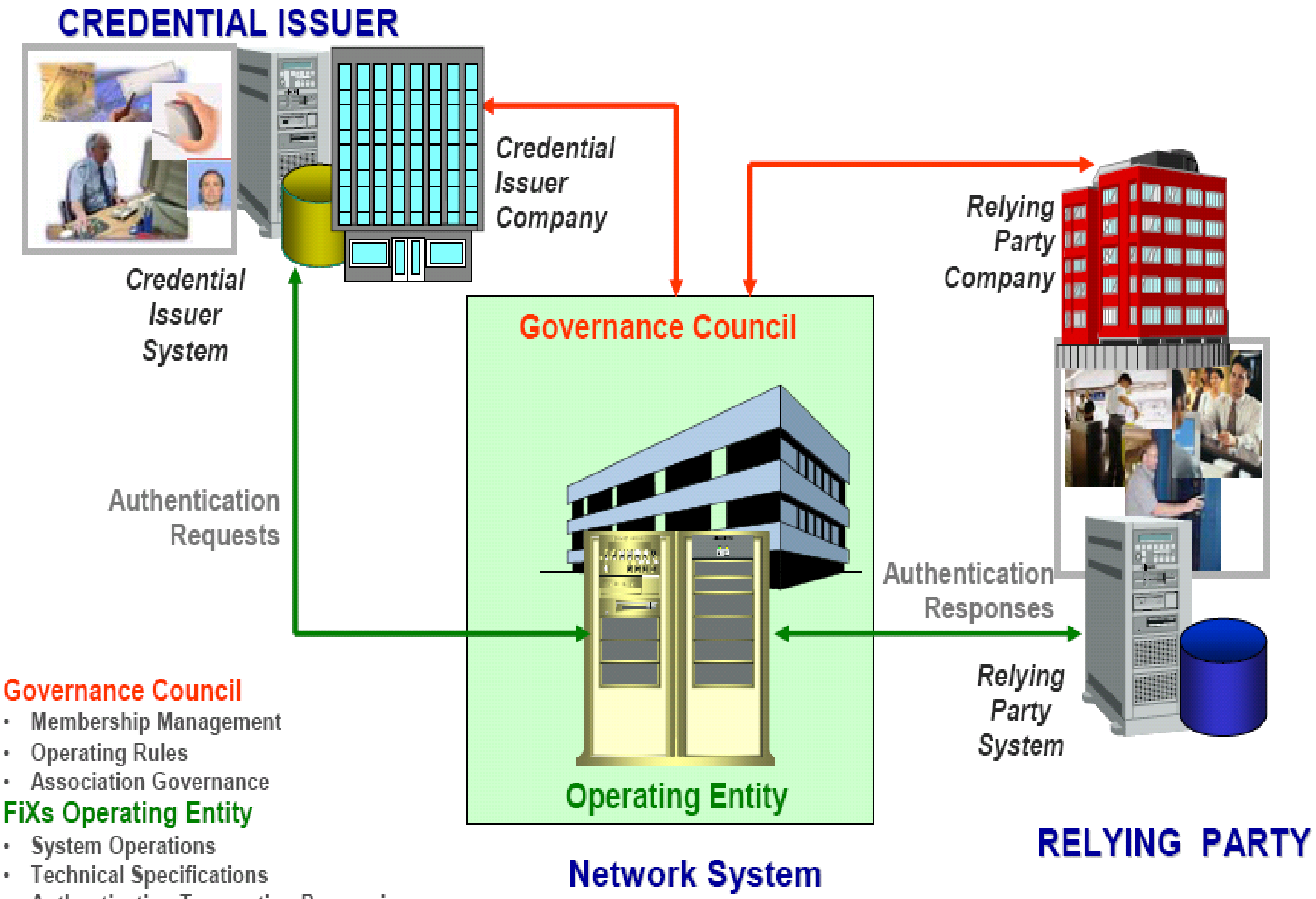
DCCIS

Defense Cross-Credentialing Identification System

- http://www.fixs.org/fixs.jsp
- FiXs is a coalition of government contractors, companies and not-for-profit organizations supporting development and implementation of an interoperable identity cross-credentialing network. FiXs has developed uniform, secure, reliable and easy-to-use electronic means of validating and assessing individual identity that can be used across organizations. FiXs is the 2005 Government Solution Center's first annual Successful Public/Private Sector Partnership Award winner. This new annual award recognizes a program managed by a government agency and its industry or association partner(s) that have improved government operations.
- By-Laws (http://www.fixs.org/docs/FiXs%20Bylaws%20v1%208_042706_final.pdf)
- Policy (http://www.fixs.org/docs/FiXs%20Policy%20092205_final.pdf)
- Operating Rules (http://www.fixs.org/docs/Op%20Rules%20version%201.0_092205.pdf)
- Trust Model (http://www.fixs.org/docs/FiXs%20Trust%20Model%20090705%20v1%200_final.pdf)

- http://www.fixs.org/docs/FiXs%20Network%20Utility%200106.pdf

FiXs Business & Operational Model Structure



CREDENTIAL ISSUER

Credential Issuer Company

Credential Issuer System

Authentication Requests

Governance Council

Operating Entity

Network System

Relying Party Company

Authentication Responses

Relying Party System

RELYING PARTY

Governance Council

- Membership Management
- Operating Rules
- Association Governance

FiXs Operating Entity

- System Operations
- Technical Specifications
- Authentication Transaction Processing

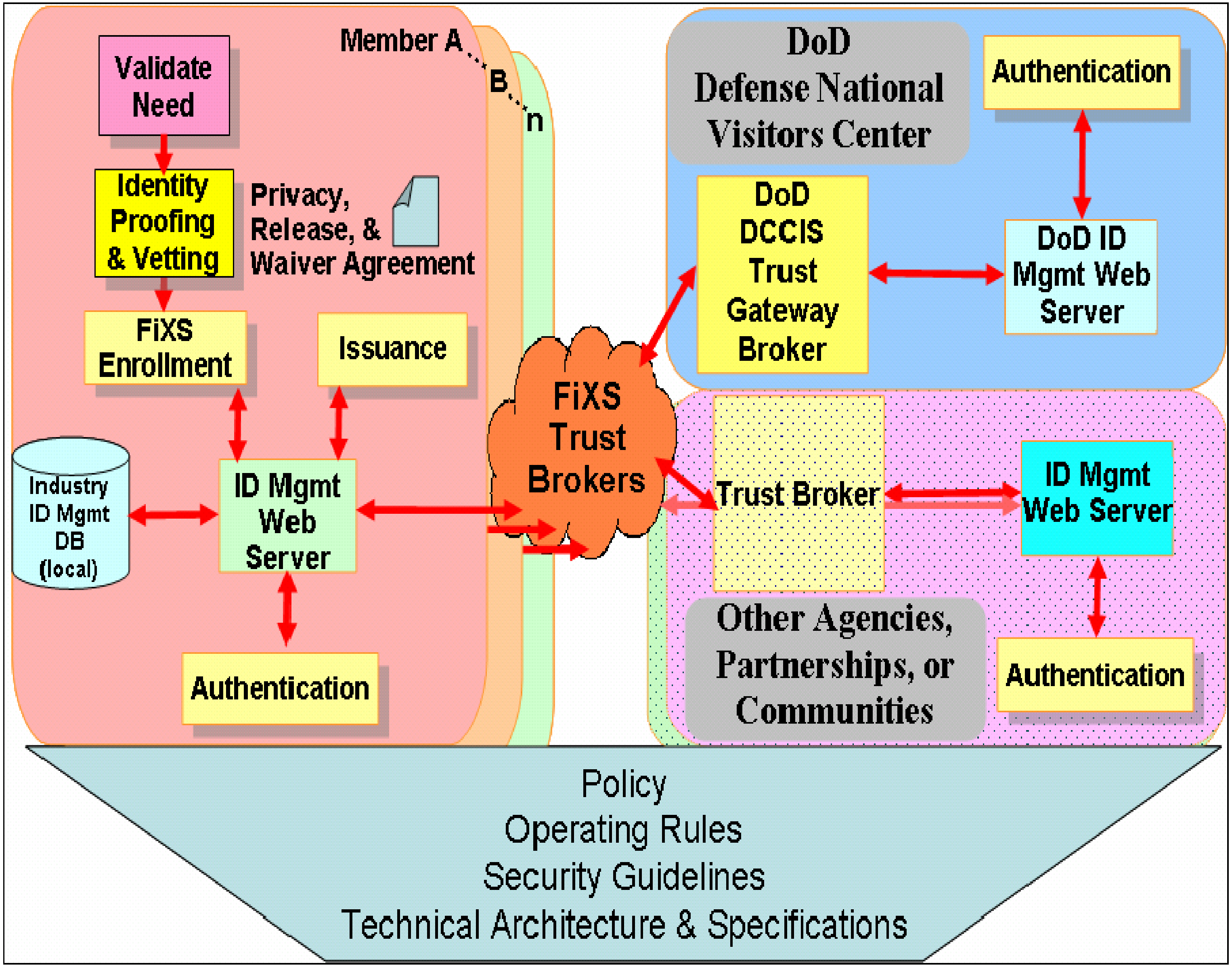

Member A
B
n
Validate Need
Identity Proofing & Vetting
Privacy, Release, & Waiver Agreement
FiXS Enrollment
Issuance
Industry ID Mgmt DB (local)
ID Mgmt Web Server
Authentication
FiXS Trust Brokers
DoD Defense National Visitors Center
Authentication
DoD DCCIS Trust Gateway Broker
DoD ID Mgmt Web Server
Trust Broker
ID Mgmt Web Server
Other Agencies, Partnerships, or Communities
Authentication
Policy
Operating Rules
Security Guidelines
Technical Architecture & Specifications

Figure 1 – FiXs Trust Model, showing multi-party trust with DoD and other organizations

FiXs

The Federation for Identity and Cross-Credentialing Systems

DCCIS

Defense Cross-Credentialing Identification System

- http://www.dmdc.osd.mil/iao/pages/dccis/dccis_main.html
- DCCIS was developed to address specific physical access control needs shared by the DoD and its industry partners. The DCCIS application provides web access to different DCCIS member organization databases, making it possible for them to authenticate visitors carrying authorized ID cards from fellow DCCIS member organizations. To compensate for differences in identification badge system and credentials used, the system is designed to make it possible to read a range of media and to accept a range of credentials.

Authentication

SECURE GOVERNMENT ACCESS ONLINE

- President’s Management Agenda
  - One of 24 E-Gov Initiatives
  - Legal Document Suite
  - Technical Architecture
  - Shared Service
  - Use credentials issued by trusted third parties
  - Citizen to Government
- **E-Authentication Mission:**
  Public trust in the security of information exchanged over the Internet plays a vital role in the E-Gov transformation. E-Authentication makes that trust possible.

  E-Authentication is setting the standards for the identity proofing of individuals and businesses, based on risk of online services used. The initiative will focus on meeting the authentication business needs of the E-Gov initiatives, building the necessary infrastructure to support common, unified processes and systems for government-wide use. This will help build the trust that must be an inherent part of every online exchange between citizens and the Government.
- Interesting Features
  - Handling of Liability
  - Interoperability Testing

Authentication

SECURE GOVERNMENT ACCESS ONLINE

- http://www.cio.gov/eauthentication/index.htm
- NIST 800-63 (http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)
- NIST 800-53 (http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf)

ELECTRONIC AUTHENTICATION PARTNERSHIP

- http://eapartnership.org/
- The goal of EAP is to provide organizations with a trusted means of relying on digital credentials issued by a variety of e-authentication systems. The EAP will not duplicate the e-authentication work of other organizations nor does it seek to replace individual industry wide authentication protocols.
- The EAP takes a public/private multi-sector approach to trust assurance. Most efforts to create reciprocal e-authentication have been made within an industry (such as banking or health care), but not across industry lines, nor among all interested industries, nor with a broad range of government partners. The EAP combines relying parties, technology companies, and service providers to bring together all interested parties – private sector, public sector, and government.
- Federation of Federations

Welcome to InQueue

- http://inqueue.internet2.edu/
- The InQueue Federation, operated by Internet2, is designed for organizations that are becoming familiar with the Shibboleth software package and the federated trust model. Participating in InQueue permits an organization to learn about the Shibboleth software via the experience of multi-party federated access, while integrating its services into the organization's procedures and policies. It is also available as a temporary alternative to sites for which no suitable production-level federation exists.
- The InQueue federation is specifically **not** intended to support production-level end-user access to protected resources. Organizations providing services are strongly discouraged from making sensitive or valuable resources available via the Federation. **Specifically, certificate authorities with no level of assurance may be used to issue certificates to participating sites, and therefore none of the interactions can be trusted.**

- InCommon® eliminates the need for researchers, students, and educators to maintain multiple, password-protected accounts. Built using Shibboleth® authentication and authorization technology, InCommon enables cost-effective, privacy-preserving collaboration among InCommon participants. The InCommon federation supports user access to protected resources by allowing organizations to make access decisions based on the user's home institution exchanging agreed upon traits with the resource provider.
- Shibboleth http://shibboleth.internet2.edu/

Signatures and Authentication for Everyone
SAFE™
SAFE-BioPharma Association

- http://www.safe-biopharma.org/index.php?option=com_frontpage&Itemid=39
- SAFE is a member-governed, not-for-profit enterprise that
  - Manages and promotes the SAFE standard
  - Provides a legal and contractual framework
  - Provides technical infrastructure to bridge different credentialing systems
  - Provides SAFE identity credentials, both directly and through vendors
  - Supports vendors who supply SAFE-enabled products.
- SAFE members exchange SAFE-signed documents with each other, secure in trusting the identity at both ends of the electronic connection. We use SAFE signatures, confident that they have the same legal weight as ink signatures. We submit electronic regulatory documents without a paper backup. We use SAFE-certified products from vendors, certain that they comply with the SAFE standard.
- SAFE white paper http://www.safe-biopharma.org/images/stories/safewhitepaper%20stelex%20final.pdf
- Certificate Policy http://www.safe-biopharma.org/images/stories/safe%20certificate%20policy%20v2-0.pdf

Signatures and Authentication for Everyone
SAFE™
SAFE-BioPharma Association

MEMBERS

- **Biopharma Companies**
  Abbott Labs
  Amgen
  AstraZeneca – Founder
  Bristol-Myers Squibb – Founder
  GlaxoSmithKline – Founder
  INC Research
  Johnson & Johnson – Founder
  Merck – Founder
  Pfizer – Founder
  Procter & Gamble – Founder
  Sanofi-Aventis – Founder
  TAP Pharmaceuticals
- **Association Sponsors**
  Pharmaceutical Research & Manufacturers Association
  European Federation of Pharmaceutical Industries & Associations
  International Federation for Animal Health
- **Governments**
  National Cancer Institute
  Food and Drug Administration
  European Medicines Evaluation Agency
  Irish Medicines Board
  Medicines Evaluation Board: Netherlands
  EOF: Greece
  Veterinary Medicines Directorate: United Kingdom
- **Research Sites & IRB's**
  Memorial Sloan Kettering
  Mayo Clinic
  City of Hope National Medical Center
  Women & Infants Hospital of Rhode Island
  H Lee Moffitt Cancer Center
  Sidney Kimmel Cancer Institute
  Shulman & Associates
  Western IRB