



Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

Identity Management in the Federal Government

Paul Grant

Judith Spencer
Agency Expert - IDM
Office of Governmentwide Policy
GSA
Judith.Spencer@GSA.Gov

ICAM Mission

- Fostering effective **government-wide** identity and access management
- Enabling **trusted** online transactions through **common** identity and access management **policies and approaches**
- **Aligning federal agencies** around common identity and access management practices
- **Reducing the identity and access management burden** for individual agencies by fostering common interoperable approaches
- **Ensuring alignment** across all identity and access management activities that cross individual agency boundaries
- Collaborating with **external identity management** activities through **inter-federation** to enhance interoperability

4 Sectors for Government Interaction

Government to Citizen

Government to Business

E-Authentication Guidance (M-04-04)

Government to
Government

Internal Effectiveness
and Efficiency
HSPD-12

Increasing the Trusted Credential Community

- Back to Basics – M-04-04 and NIST 800-63 are still the foundational policy/technical guidance for identity management.
- Establish unified architecture for Identity Management
- Expanding our use of Assertion-based solutions (Levels 1 & 2)
 - Partnering with Liberty Alliance
 - Stronger industry alignment for trust and technology standards
- Federal Bridge will continue to play a role at Levels 3 & 4
 - External Shared Service Providers
 - Four Bridge Forum (FBCA, Certipath, SAFE-BioPharma, HigherEd)
 - Transglobal Secure Collaboration Program
- Outreach to communities of interest
 - Explore natural affinities

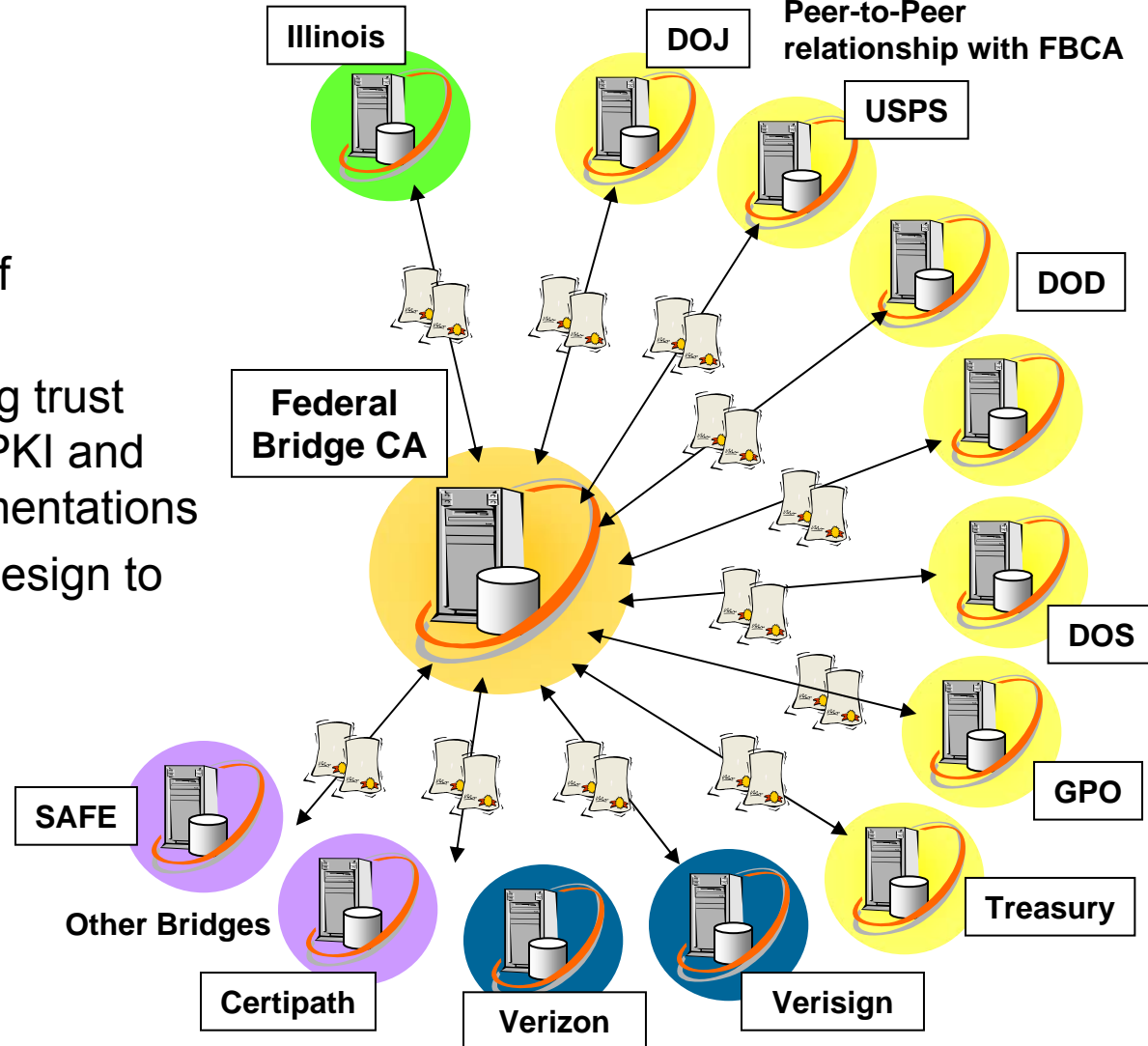
Assurance Levels

M-04-04:E-Authentication Guidance for Federal Agencies
OMB Guidance establishes 4 authentication assurance levels

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity	Some confidence in asserted identity	High confidence in asserted identity	Very high confidence in the asserted identity
Self-assertion minimum records	On-line, instant qualification – out-of-band follow-up	On-line with out-of-band verification for qualification Cryptographic solution	In person proofing Record a biometric Cryptographic Solution Hardware Token

Federal Bridge CA

Legacy Agencies in
Peer-to-Peer
relationship with FBCA



- Peer-to-Peer interoperability mechanism for PKI
- Acts as a trust facilitator
- Operates at multiple layers of assurance
- Chief mechanism for enabling trust between industry (external) PKI and Federal (internal) PKI implementations
- Undergoing upgrade and redesign to be completed this year

Summary

- Identity and Access Management Are Foundational to Information Sharing and Collaboration
- Shared Guidance is Improving: Still a work in progress
 - Clear, Concise, Consistent, Published
 - For Ourselves and Our Mission Partners
- Industry Partners are Fielding Identity Credentials as well as Creating Federations for Sharing & Collaboration
- Progress Depends on Public-Private Partnering
 - Domestically
 - Internationally

Interagency Advisory Board

Meeting Agenda, June 23, 2009

1. **Opening Remarks**
2. **The Four Bridges Forum**
 - a) ***Tim Pinegar, FCBA***
 - b) ***Jeff Nigrini, Certipath***
 - c) ***Gary Secrest, SAFE-BioPharma***
 - d) ***Scott Rea, HEBCA***

-----BREAK-----
3. **PIV Standards Update (Bill MacGregor, NIST)**
4. **Federally Interoperable Credentialing in Illinois (*Dennis Glavin, CGN PM*)**
5. **Closing Remarks (*Tim Baldrige, NASA*)**

The Federal Bridge and The Four Bridges Forum (4BF)

A Brief Overview



Why Fed PKI?



- ***E-Gov (2002)***: government's need for assured identity in electronic transactions with citizens, businesses, governments, itself;
- ***E-Authentication / M-04-04 (2003)***: established four levels of assurance (LOA) for the authentication of identities in electronic transactions. Achieving any M-04-04 LOA requires PKI.
- ***HSPD-12 / FIPS201 (2004)***: established common identity standards for Fed employees and contractors; minimum control and security requirements for Federal Personal Identity Verification (PIV) systems; requiring PIV cards to contain PKI based authentication data .

Why A Bridge?



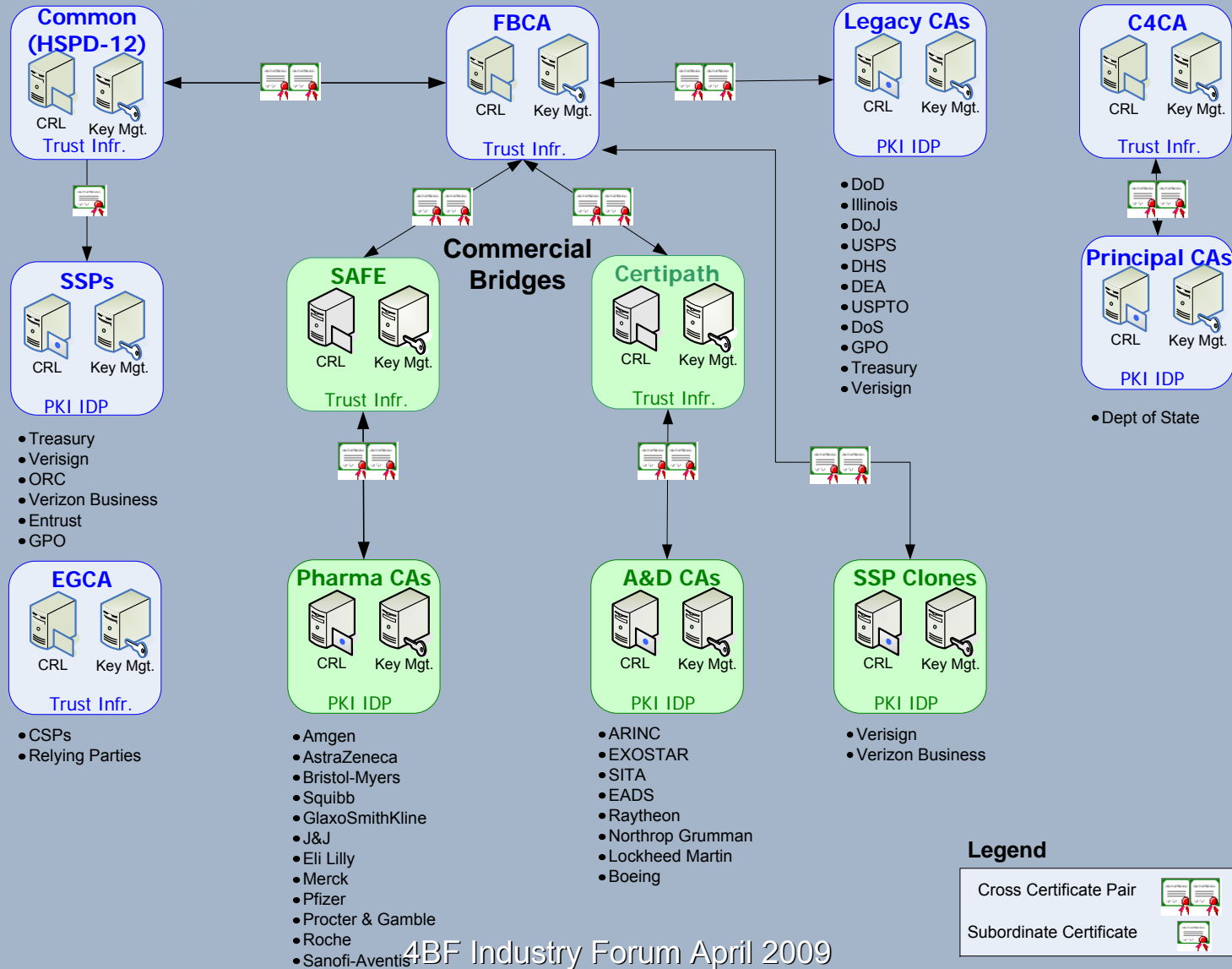
- Allow trust among members **at known levels of assurance of identity**;
- Expand trust easily and **minimize administrative burden and cost** of cross-domain interoperability;
- Members continue to **control their own domains and relationships** (non-hierarchical).

Why The Federal Bridge?



- **Source of interoperability** for ALL Federal Agency HSPD-12 credentials (6.2 million and counting as of 3/2009);
- Enable Agencies to validate each other's PIV cards for **physical access**
- Validate desktop and network **logins**
- Support high assurance **authentication** to Agency **Level 3 & 4 applications** from government and private sector credentials

Fed PKI: View from 20,000 ft



Why the 4BF?



- **Source of interoperability** with a wide variety of business partners in critical business sectors using a GPEA-, E-Sign-, E-Gov- and E-Authentication-compliant solution.
- Trust of 4BF identity credentials provides “**real time**” **scalability**;
- Leverage PIV certificates to **improve the ROI of PIV system infrastructure**;
- And, with **more mainstream PK-enabled COTS** products, agencies can deploy applications faster and in increasingly more sophisticated, robust, and value-added ways.

Interagency Advisory Board

Meeting Agenda, June 23, 2009

1. **Opening Remarks**
2. **The Four Bridges Forum**
 - a) *Tim Pinegar, FCBA*
 - b) *Jeff Nigrini, Certipath*
 - c) *Gary Secrest, SAFE-BioPharma*
 - d) *Scott Rea, HEBCA*

-----BREAK-----
3. **PIV Standards Update** (Bill MacGregor, NIST)
4. **Federally Interoperable Credentialing in Illinois** (*Dennis Glavin, CGN PM*)
5. **Closing Remarks** (*Tim Baldrige, NASA*)

The 4BF

The Four Bridges Forum

Federated PACS

A Physical Access

Use Case for Bridges

FIPS 201/PIV-I PACS

Interoperability

April 28th, 2009



3 Forms of Identity Assertion



Corporate / Public Network



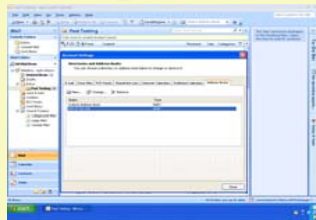
2. Federated Assertion



Service Provider (SP)



1. End-Entity Assertion



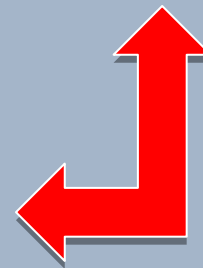
3. Credential Assertion



PACS

LACS

Convergence



LACS vs. PACS



LACS

- Relatively mature WRT strong identity management
- Able to leverage credentials issued by other organizations
- Highly scalable via federation

PACS

- Strong identity credentials are unusual across the PACS landscape
- PKI is virtually unheard of for PACS
- Visitors using their own organizational issued badges does not exist (federation)

Required Validation Process



- Path Discovery (SCVP) – discover path from certificate to trust anchor
- Signature Verification – certificates in path are genuine
- Certificate Verification – certificate data check (data integrity, validity date, expiration date, etc.)
- Private Key Challenge – certificate is bound to card (not copied or cloned)
- PIN/BIO Check – credential is bound to cardholder

System Highlights

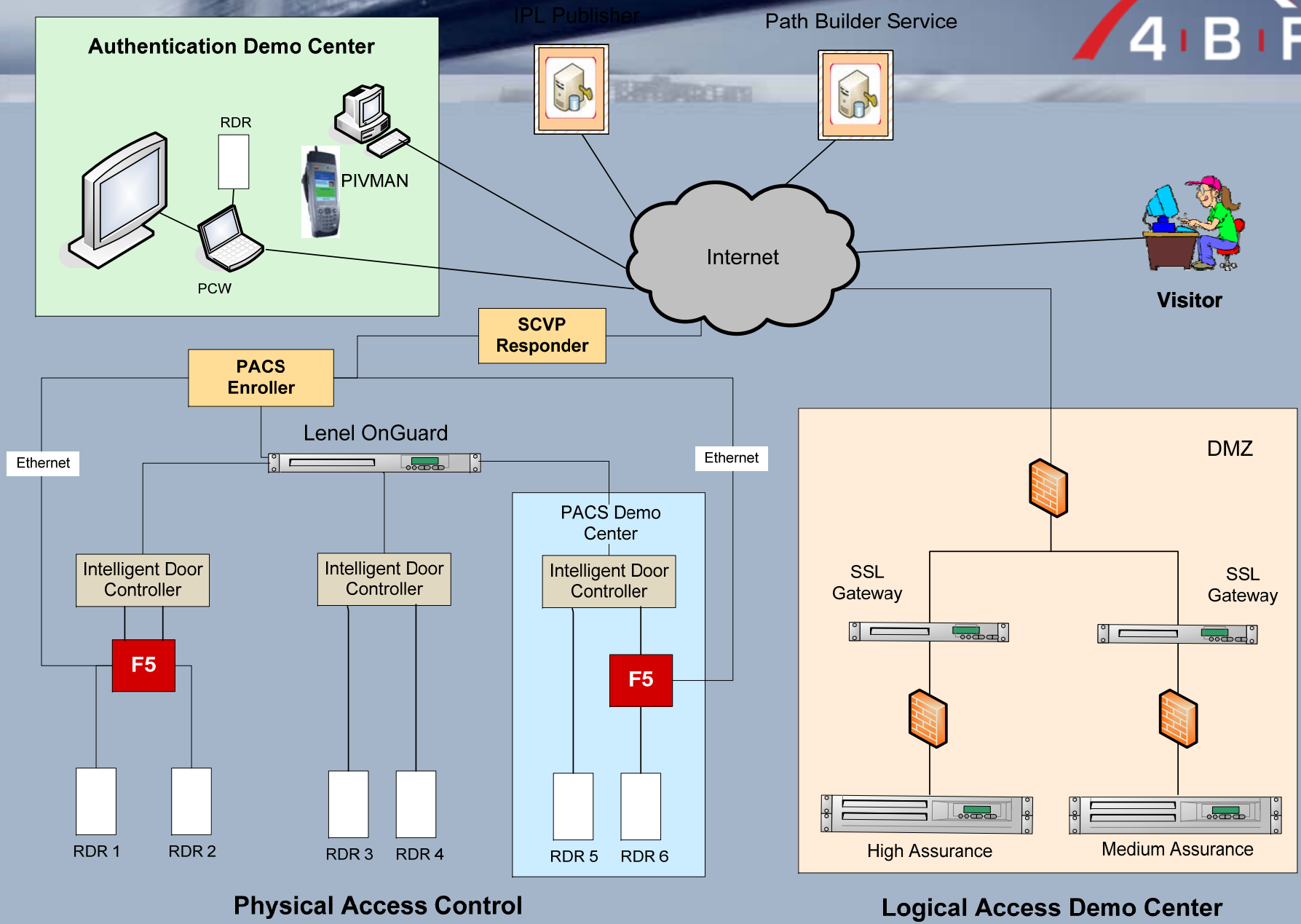


- Supports a heterogeneous credential environment where the following is true about the credentials
 - A trust path can be created and validated for Federal agencies via the FBCA and commercial entities via the CertiPath Bridge
 - The token conforms to FIPS-201, PIV-I, CertiPath PIV-I or DoD CAC NG
- Visitors to facility do not require onsite enrollment
 - Onsite is supported but not required
- Current deployment in Dulles, VA (DD) is being deployed at SP 800-116 maturity level 4 and contain three area profiles
 - Controlled
 - Limited
 - Exclusion

System Highlights (cont.)



- Guests with unescorted access within the controlled area will be given “re-assignable” smartcards but a fingerprint will be captured
- The controlled area allows single factor CAK during 8-6pm weekdays but switches to CAK+BIO afterwards
- DD will have additional demo lab that contains a reader that will output to a large display the real-time checks and path validation done to verify and validate credentials






Physical Access Control

Logical Access Demo Center

Reader Options



<p>Reader</p>	<p>Contact Contactless PIN</p> 	<p>Contact Contactless PIN BIO</p> 	<p>Contact Contactless PIN BIO</p> 
<p>Assurance Level</p>	<p>Controlled</p>	<p>Limited</p>	<p>Exclusion</p>
<p>Authentication Mechanism(s)</p>	<p>VIS & CHUID or CAK</p>	<p>BIO or BIO-A or PKI</p>	<p>CAK and BIO(-A) or PKI and BIO(-A)</p>
<p>Authentication Operation(s)</p>	<ul style="list-style-type: none"> • Cert Signature Check • Private Key Challenge 	<ul style="list-style-type: none"> • Bio Signature Check/Match • Cert Validation/Sig. Check • Private Key Challenge 	<ul style="list-style-type: none"> • Bio Signature Check/Match • Cert Validation/Sig. Check • Private Key Challenge

An Identity “Trifecta”



- Meetings are a common place to share data verbally and visually
 - Essentially access to data outside of a “ACL” controlled environment
- Common to not know everyone around the table
 - Even less common to be sure of the employment status of all visitors and guests
- Next version of MS Outlook allows for “labeling” meetings
 - Conference room doors become last enforcement point



Supporting Organizations



Interagency Advisory Board

Meeting Agenda, June 23, 2009

1. **Opening Remarks**
2. **The Four Bridges Forum**
 - a) *Tim Pinegar, FCBA*
 - b) *Jeff Nigrini, Certipath*
 - c) *Gary Secrest, SAFE-BioPharma*
 - d) *Scott Rea, HEBCA*

-----BREAK-----
3. **PIV Standards Update** (Bill MacGregor, NIST)
4. **Federally Interoperable Credentialing in Illinois** (*Dennis Glavin, CGN PM*)
5. **Closing Remarks** (*Tim Baldrige, NASA*)

The 4BF

The Four Bridges Forum

The SAFE-BioPharma Digital Identity and
Signature Standard



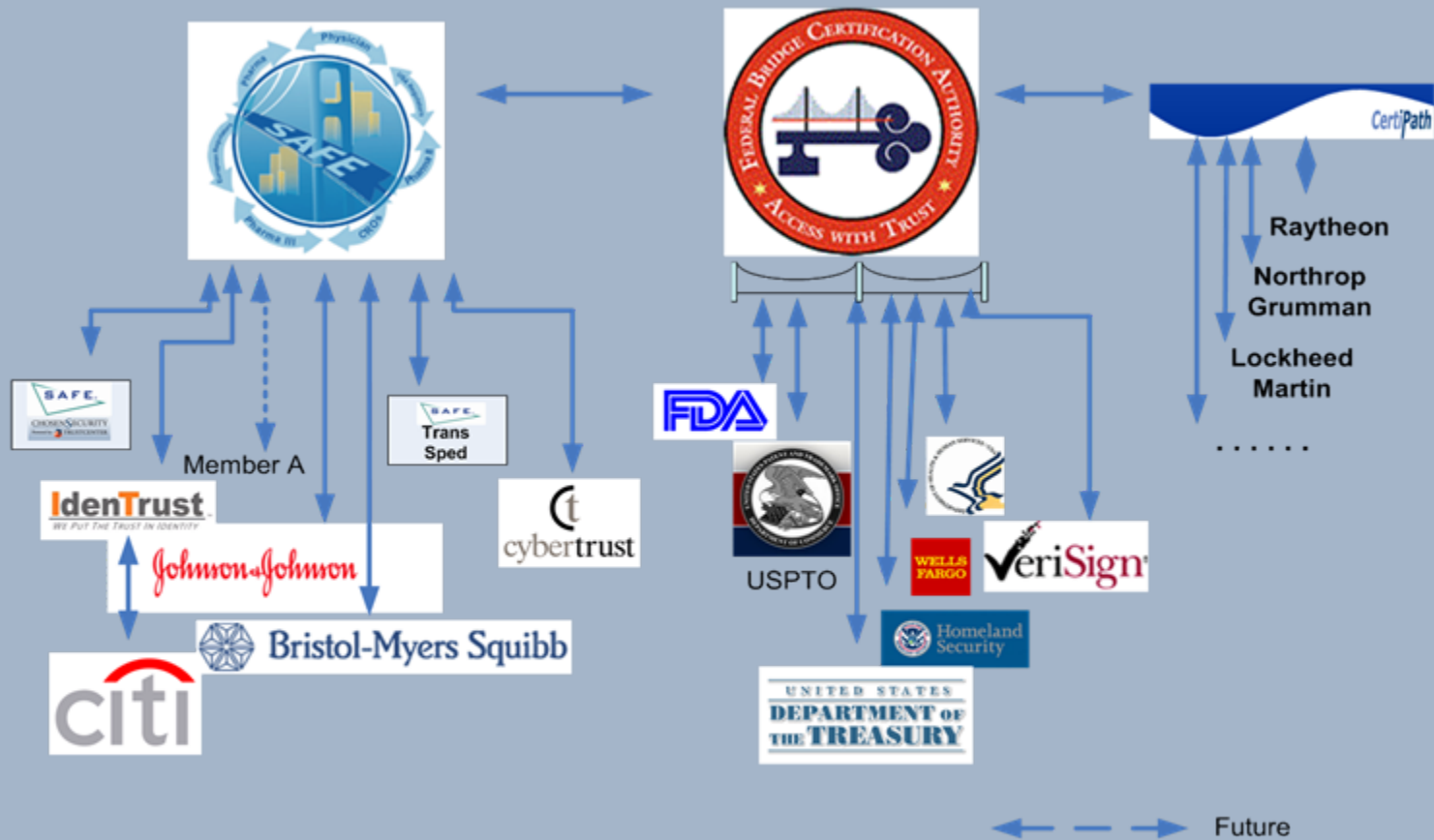
Why an Industry Digital Identity and Signature Standard?



- Revolution in life sciences and medical technology:
 - Costly, complex, many partners, global
- Need to improve safety, quality, development times:
 - Need to achieve process efficiencies & improvements.
- Government imperative – soon to be mandated for regulatory submissions and healthcare.
- Fundamental to sensitive electronic exchanges of information are trusted identities and legal signatures.
- Special issues/barriers for biopharmaceutical industry – legal, global, clinical researchers, regulatory, risk mitigation.

- 2005: Strategic initiative to transform industry business and regulatory processes to fully electronic
 - Member-governed non-profit collaboration
 - Standard for trusted identity and non-repudiable digital signature based on same standards as used by Federal Govt.
 - Contract-based system -- Risk mitigation scheme, regulatory requirements, global applicability
 - Technology and vendor neutral
 - 2006-2007, pilots and early adopters
 - 2007-2008, expansion of standard; increased implementations and use cases
 - 2008 cross-certified with FBCA
 - 2008 Member establishment of tiered services
 - Shared infrastructure to provision employees, external partners (researchers), at low cost
 - Identity-proofing and digital signing technologies for healthcare professionals
 - Fee structure revisions – small entity, non-profit, government, special use
 - Growing implementations and use cases -- clinical research, alliance management, purchasing, legal, research notebooks, investigator portals
 - Maturing technology and supportive policy environment

SAFE-BioPharma Bridge Infrastructure



Options for Flexible Use

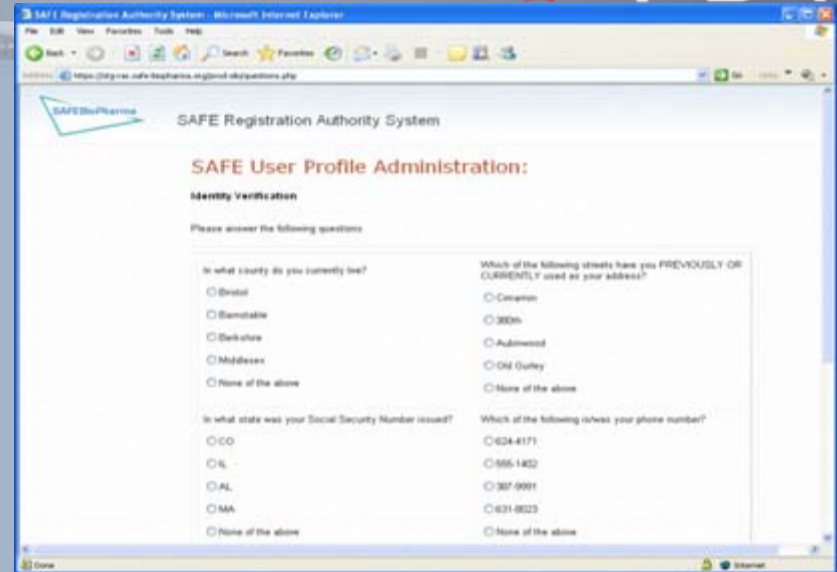
- Two levels of trust:
 - Basic Assurance for authentication
 - Medium Assurance for trusted identity uniquely linked to digital signature and EU-qualified
- Three digital signing technologies:
 - Software
 - Hardware (zero footprint now undergoing FIPS certification)
 - Roaming
- Three identity-proofing options
 - Antecedent – enterprise and on-line
 - Trusted agent
 - Notary – including office/home notary services

On-Line Antecedent Process



■ ID Vetting Successful:

- Applicant Passes 3rd Party Antecedent identity proofing
- Moved to RA queue for processing and Certificate Issuance steps.
- It's a matter of minutes end-to-end.



▶ ID Vetting Not Successful:

- Unable to verify identity via 3rd Party Antecedent
- Process reverts to Notary Process with two service options:
 - User locates notary
 - RAS/NNA will have a local notary contact the Applicant directly

I would like to:*

Schedule my own Notary appointment

Please have a licensed Notary in my area contact me to schedule an appointment

Your Email Address	demo.cp1@kernworld.org
Your Phone Number	777 - 666 - 5555
Alternate Phone Number?	<input type="text"/>
I prefer to be contacted by:*	<input checked="" type="radio"/> Phone <input type="radio"/> Email
The best time to contact me is: *	<input type="radio"/> Anytime (9 AM - 9 PM) <input type="radio"/> Business hours- Morning (9 AM-Noon) <input type="radio"/> Business hours- Afternoon (Noon-5 PM) <input type="radio"/> After business hours- (5 PM-9 PM)
Please enter any additional information that will help expedite scheduling a Notary appointment:	<input type="text"/>

SAFE-BioPharma and Regulators

- EMEA and FDA are on paths to require fully electronic submissions within the next few years
- FDA helped write SAFE-BioPharma standard; engaged since inception
 - FDA has received 10,000s of SAFE-BioPharma submissions since 9/06
- EMEA engagement since inception – helped write standard
 - EMEA to use SAFE-BioPharma for access to Safety Reports Database
 - eSubmissions now underway
- SAFE-BioPharma and the MHLW/PMDA
 - Expect to launch SAFE-BioPharma services in late 2009

Centers for Disease Control (CDC): Public Health Surveillance



Purpose

- Accelerate and simplify the Disease Investigation process
- Build a scalable framework aligned with the National Health Information Network (NHIN) architecture and structures
- Establish a cross-jurisdictional, credential compatible with the Federal Architecture and Federal PKI Policy Authority (FPKIPA)

Efficiency

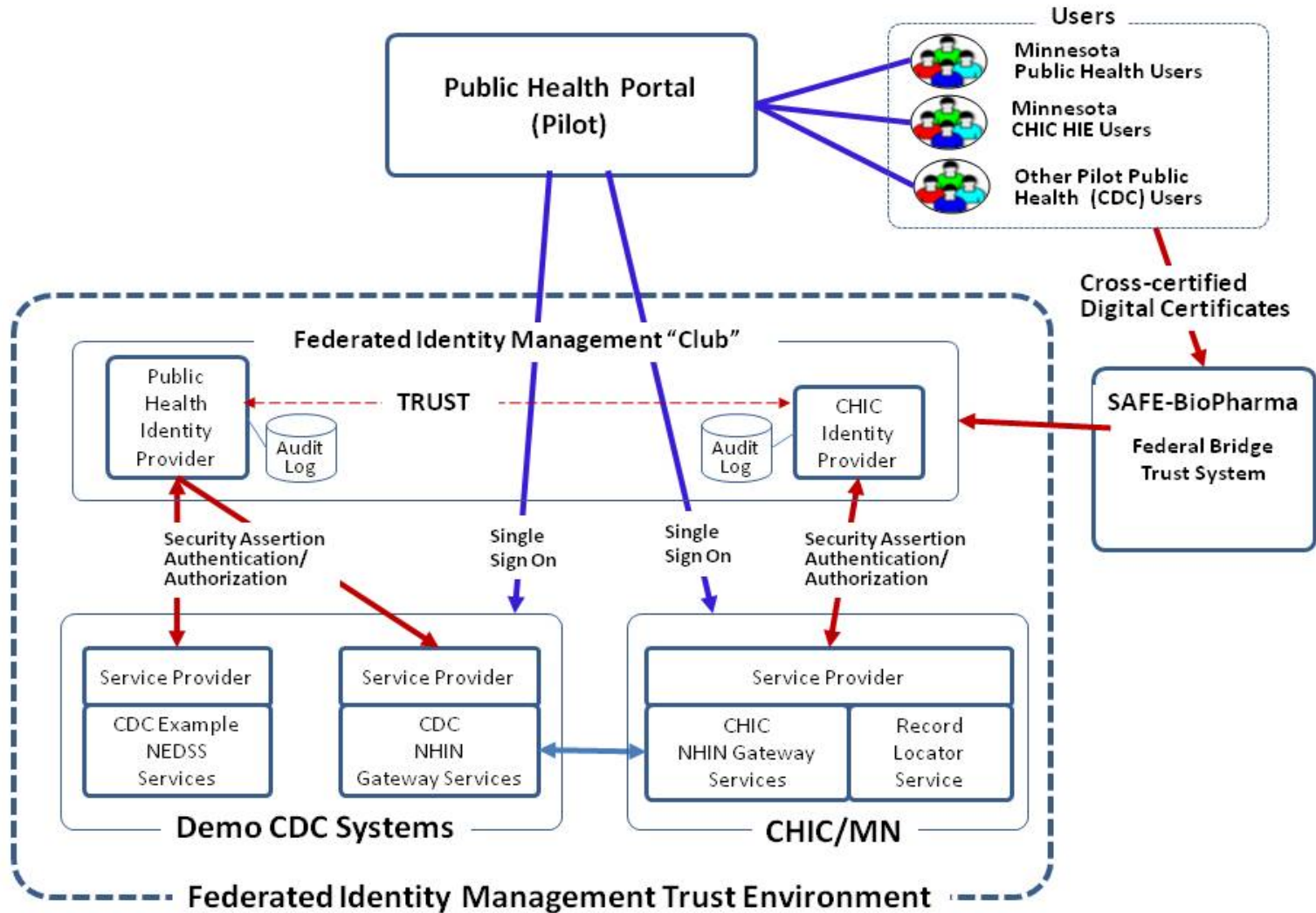
- Disease investigator can access state systems and query for meta data and request a CDA or CCD document back electronically.
- Reduction of phone calls, faxes and emails needed for routine investigation workflow.
- Overall time to track and close investigations should decrease.

Will be validated by ROI analysis in Pilot Phase

Cost

- Reduced cost due to increased efficiency of investigation workflow
- Reduced maintenance cost of security sub systems.
 - *Certificates not maintained by state investigator or CDC.*
 - *Federal Identity provider issues the certificates*

CDC Disease Investigation Federation Overview



Premier Purchasing

■ Company profile

- Largest Group Purchasing Organization (GPO) in U.S.
- Owned by non-profit hospitals
- Serves 2,000 U.S. hospitals and 53,000-plus other healthcare sites
- Buys from ~700 suppliers
- <http://www.premierinc.com/>

■ Scope:

- Eliminate overnight shipping, fax and related workflows for contract origination and amendments
- Provide SAFE-BioPharma credentials to Premier Sourcing/Procurement employees and their supplier colleagues for signing new and amended supplier contracts
- eContracting process ~700 companies and thousands of contracts and/or amendments

■ Future:

- Digitally sign and submit required reports to CMS

- ▶ SAFE-BioPharma makes end-to-end eBusiness and eRegulatory processes possible
 - Legal enforceability
 - Regulatory compliant (US, EU, Japan)
 - Global standard
 - In EU, SAFE-BioPharma digital signature is the legal equivalent of handwritten
 - Mitigates risk
 - Vendor, technology neutral
 - Secure
 - Record integrity
 - Only one digital identity per investigator or other user
 - Links Federal agencies to pharma and healthcare providers
 - Provides interoperability
 - Improves productivity
 - Improved auditability and compliance
 - Reduces cycle time
 - Facilitates collaboration

- ▶ Enabling technology to transform business and regulatory processes



Interagency Advisory Board

Meeting Agenda, June 23, 2009

1. **Opening Remarks**
2. **The Four Bridges Forum**
 - a) *Tim Pinegar, FCBA*
 - b) *Jeff Nigrini, Certipath*
 - c) *Gary Secrest, SAFE-BioPharma*
 - d) *Scott Rea, HEBCA*

-----BREAK-----

3. **PIV Standards Update** (Bill MacGregor, NIST)
4. **Federally Interoperable Credentialing in Illinois** (*Dennis Glavin, CGN PM*)
5. **Closing Remarks** (*Tim Baldrige, NASA*)

The 4BF

The Four Bridges Forum

Higher Education Bridge
Certificate Authority



HEBCA – A Brief History

- HEBCA started life as pilot project to validate PKI bridge-2-bridge transactions
- Modeled on the successful FBCA, but representing higher education
- Hosted at MitreTek, beginning 2001 with involvement from several HE institutions
 - Dartmouth College, University of Wisconsin, University of California
 - Berkley, University of Alabama, etc.
- EDUCAUSE provided sponsorship to instantiate the infrastructure for real
- Dartmouth College chosen as operating authority in May 2004



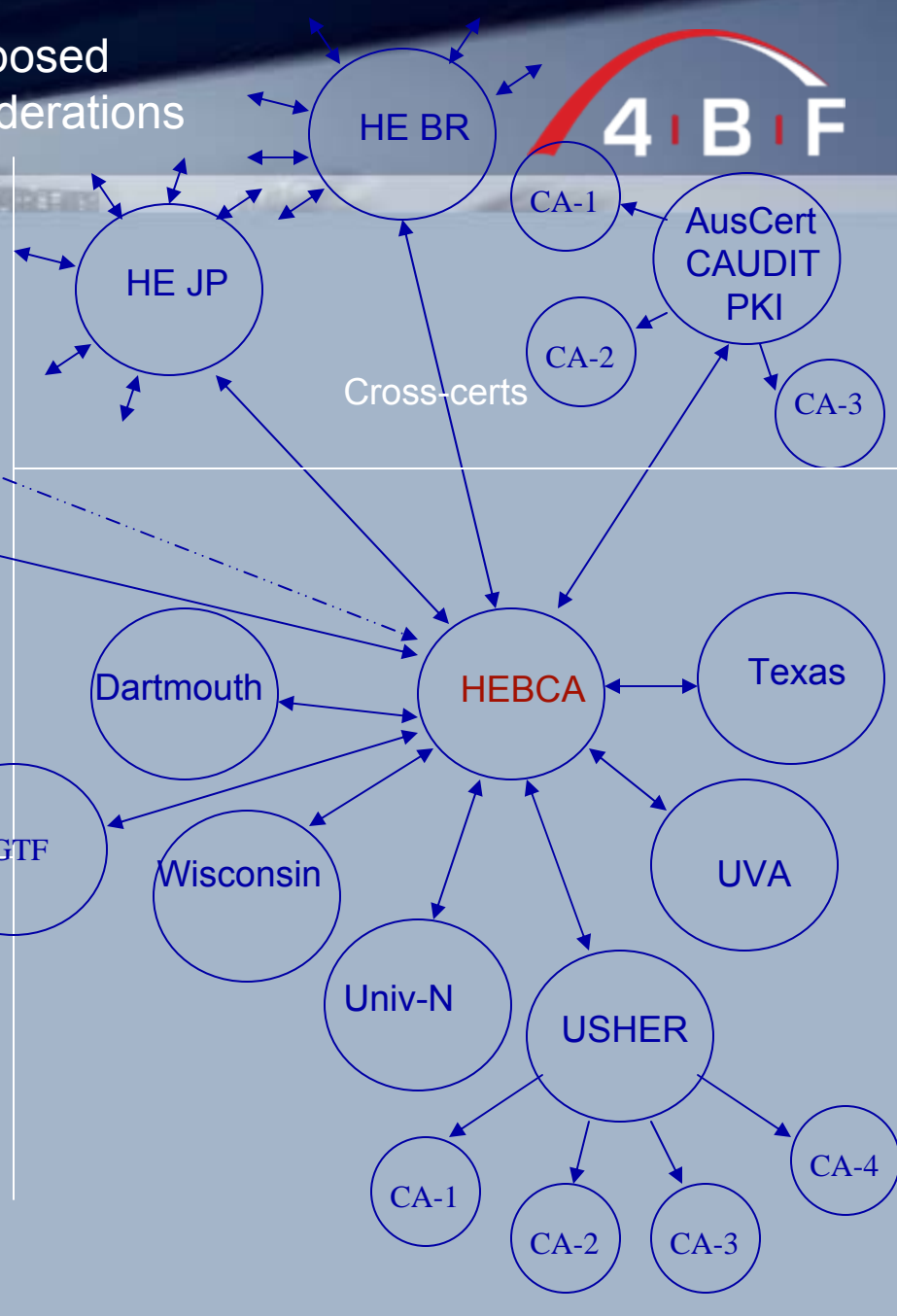
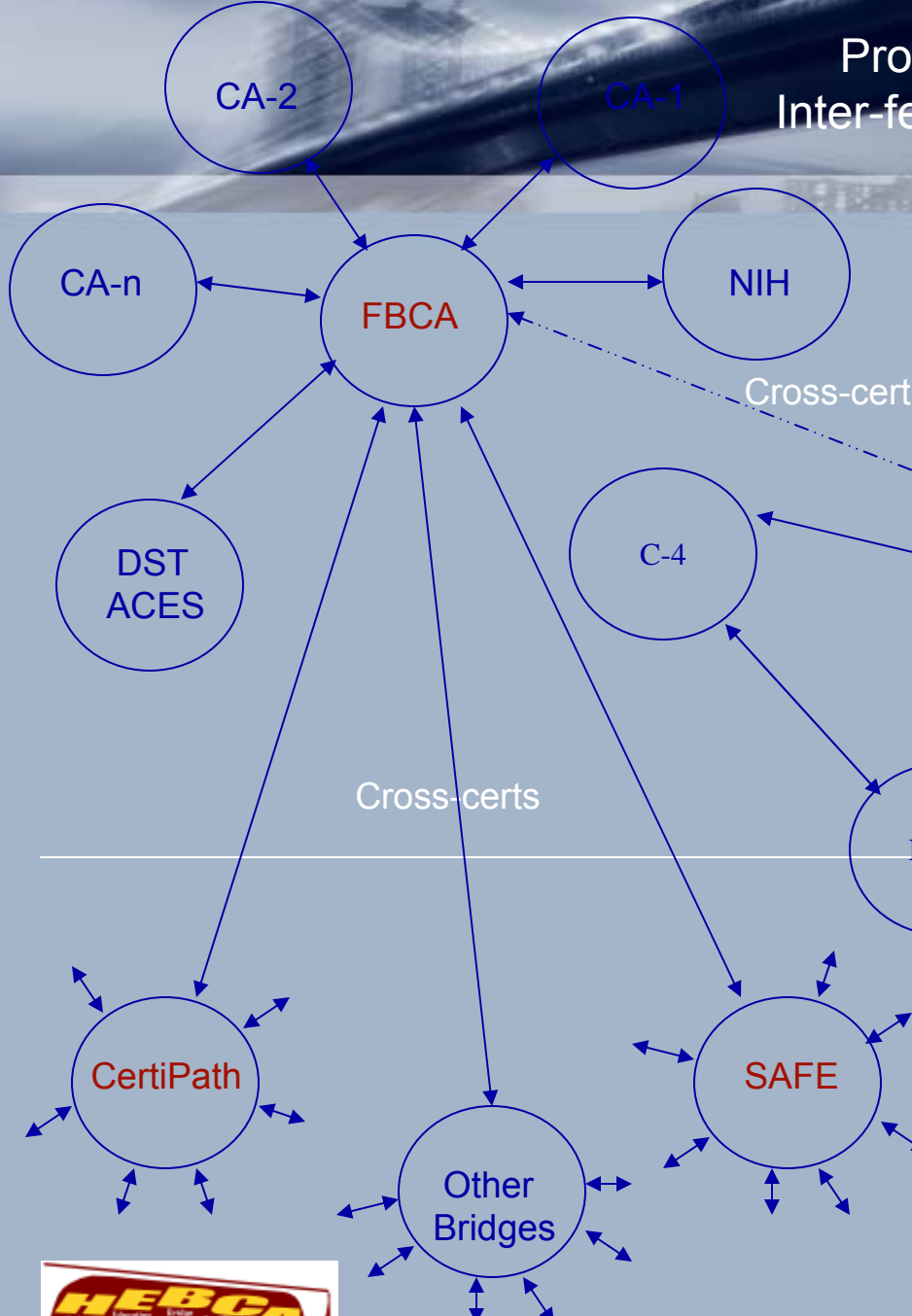
HEBCA – A Brief History

4 | B | F

- HEBCA rebuilt from the ground up based on prototype at MitreTek, but using different Certification Authority infrastructure
- Policy Mapping and technical interoperation completed with FBCA, cross-certification with a limited number of schools and related entities
- Internet2's USHER was created on the same infrastructure before being migrated to InCommon
- HEBCA is ready for production, but operates in a "Test" mode today
- Steps are underway to migrate infrastructure to a long term commercial operation



Proposed Inter-federations



HEBCA – A Case Study

4 | B | F

- E-Sign Law 2000 makes digital signatures equivalent to wet ink signatures
- Digitally signed documents enable paperless workflow, reducing costs, increasing speed and efficiency
- Digitally signed documents:
 - eliminate the need to handle, copy, ship and store paper documents
 - facilitate a higher conversion rate from customers at online portals
 - reduce the amount of manual input or reprocessing, (reduces errors)



HEBCA – A Case Study

4 | B | F

- Trust in digitally signed documents depends on a number of elements:
 - the set of policies defining how the digital certificate used to verify the signature was issued;
 - how that digital certificate is managed; and
 - how well the identity of the subject of that certificate was vetted
- Trusting certificates issued from a CA one is familiar with is straight forward, but how does the average user trust certificates from a CA they have no relationship with?
- Being able to trust digital identities from multiple disparate sources is essential to implementing an effective paperless document workflow



HEBCA – A Case Study

4 | B | F

- HEBCA provides an efficient way for participating organizations to establish trust of any identities issued by other participants
- HEBCA uses technological and policy-based processes to assert the level of assurance that community members can place in a given identity certificate.
- As each participant joins HEBCA, their identity credentialing processes are reviewed and an assurance value is assigned to their certificates on a scale recognized within the community.
- Instead of each member establishing bilateral trust agreements, and reviewing the policies and procedures of each of all the other participants, they can simply trust the validity of the identity which HEBCA has vetted and asserted across its entire system
- HEBCA's participation in the 4BF enables a far greater community of trust for its participants beyond just higher education



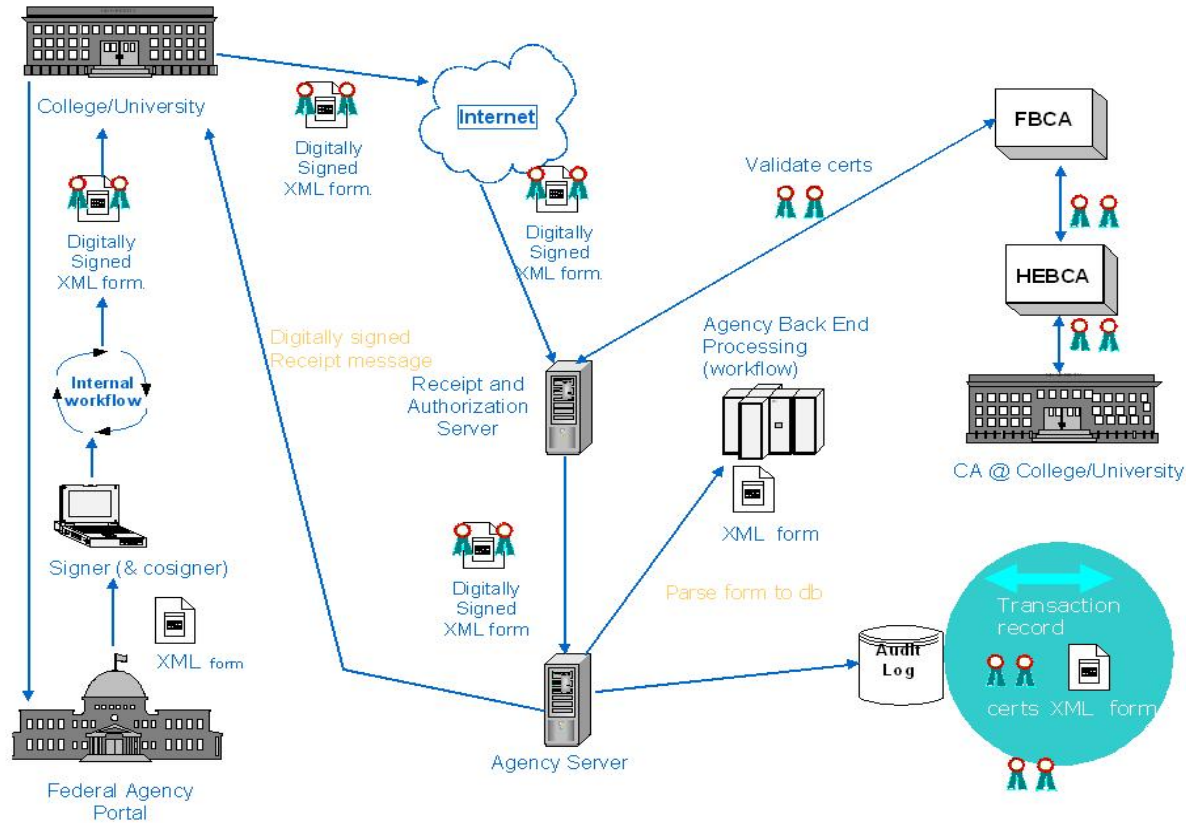
HEBCA – A Case Study

4 | B | F

- NIH-EDUCAUSE PKI Interoperability Project
 - Higher education researchers use certificates issued by their own schools to sign and submit grant applications to NIH
 - NIH accepted and validated the applications and provided a signed receipt back to the schools
 - The schools were able to validate and trust the receipt signed with the NIH certificate
 - NIH was able to begin auto-processing of the grant applications without manual data entry and the potential errors that process introduces



Process Flow



Applicant acquires e-form from government website

Applicant fills out form at desk

Applicant signs form with university ID credential

Applicant sends form to government website (FTP)

Government server receives signed application

Server validates digital certificate with university issuer

Server sends secure, digitally signed electronic receipt message to applicant

Server parses e-form into Agency database

Database is the gateway to the Agency business processes (workflow)

HEBCA – A Case Study

4 | B | F

- NIH-EDUCAUSE PKI Interoperability Project
 - Trust facilitated through HEBCA and FBCA in the same way 4BF now provides
 - Digital signatures provide exponential increase in the speed of transaction
 - Process saves costs through not having to handle, copy, ship, or store paper
 - The project was awarded an E-Gov Pioneer Award by the federal government



HEBCA



- HEBCA is still only operating in “Test” mode

