



Higher Education PKI Initiatives

(Scott Rea)

Securing the eCampus - Hanover NH

July 28, 2009

Overview

- What are the drivers for PKI in Higher Education?
 - Stronger authentication to resources and services of an institution
 - Better protection of digital assets from disclosure, theft, tampering, and destruction
 - More efficient workflow in distributed environments
 - Greater ability to collaborate and reliably communicate with colleagues and peers
 - Greater access (and more efficient access) to external resources
 - Facilitation of funding opportunities
 - Compliance



PKI - Public Key Infrastructure

- Security is a chain; it's only as strong as the weakest link. The security of any system is based on many links and in a PKI they're not all cryptographic. People are involved
- PKI requires co-ordination across the following 3 areas:
 - Technology (T)
 - Policy & Procedures (P)
 - Relationships & Liability (L)

LOA: Levels of Assurance

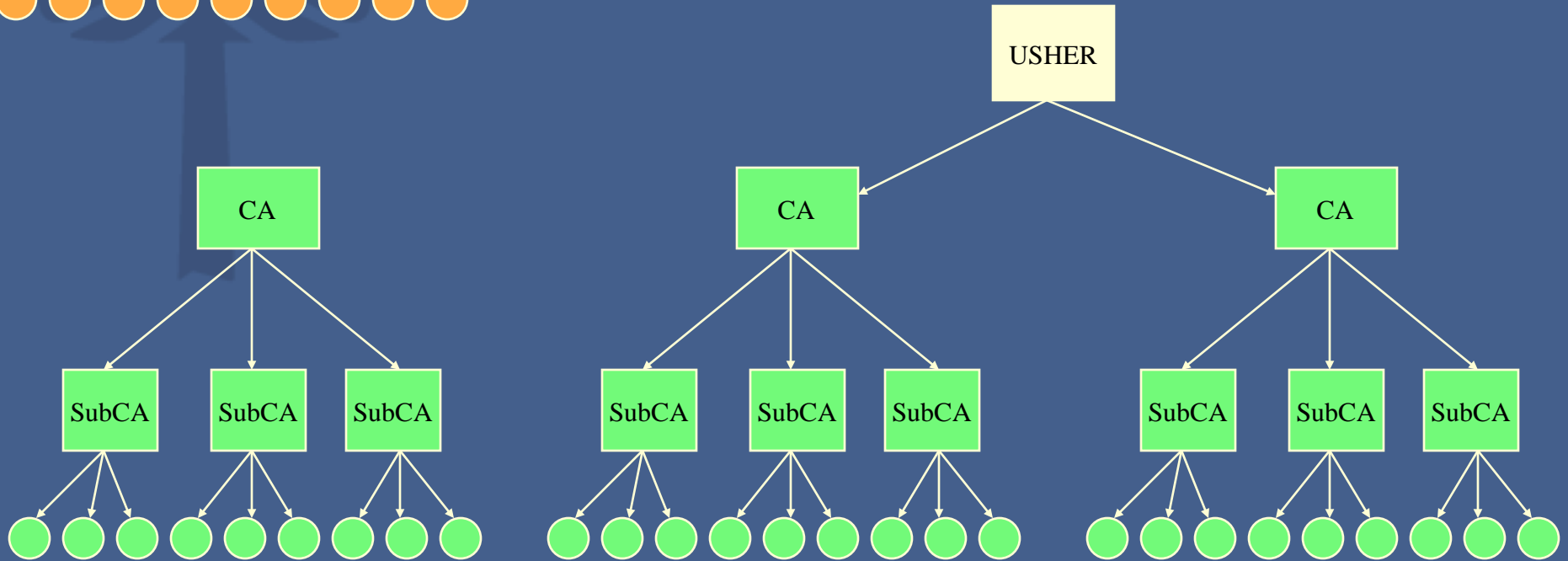
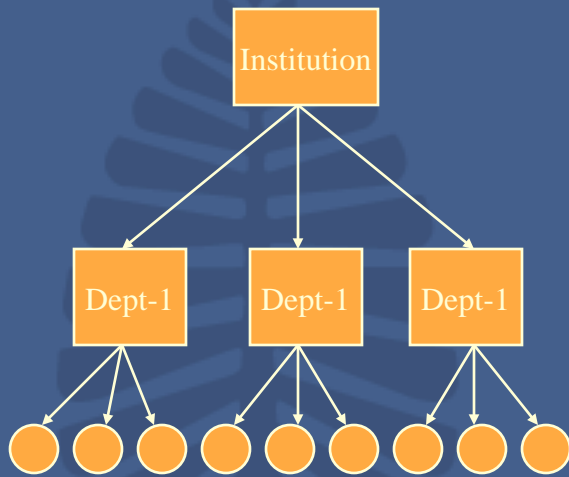
- Not all IdPs are created equal
 - Policies adhered to vary in detail and strength (P)
 - Strength of private keys (T)
 - Protection of private keys (PL)
 - Controls around private key operations (TPL)
 - Separation of duties (PL)
 - Trustworthiness of Operators (L)
 - Auditability (TP)
 - Authentication of end entities (TPL)
 - Frequency of revocation updates (TP)



PKI Options

- PKI Choices for Higher Education
 - Outsourced everything
 - Outsourced managed services, internal RAs
 - Internal operations:
 - Community root | Campus root
 - Community Policy | Campus Policy
 - CA software: commercial | vender | open source | RYO

Creating Silos of Trust





USHER : US Higher Education Root

- Trusted Root for US Higher Education
- Internet2 funded initiative
- Only signs subordinate CA certificates
- Bootstraps institutional PKIs by providing policy infrastructure and a CA
- The USHER root CA and infrastructure created at Dartmouth College, now hosted with InCommon infrastructure at Internet2
- Facilitates inter-institutional trust between participating schools
- Different levels of assurance will be supported (just 1 rudimentary currently)



USHER Project

- The USHER Project will create and maintain four new Certificate Authority (CA) systems for Internet2
 - The four CA systems to be created are:
 - USHER Foundation CA (Now called CA1)
 - USHER Basic CA*
 - USHER Medium CA*
 - USHER High CA*
 - *Not officially named yet
 - The USHERs will be used to provide institutions of higher education PKI trust anchors with a common policy
 - The USHER CAs may also be potentially cross-certified with the HEBCA to allow interoperation outside the USHER community



USHER Policy Authority

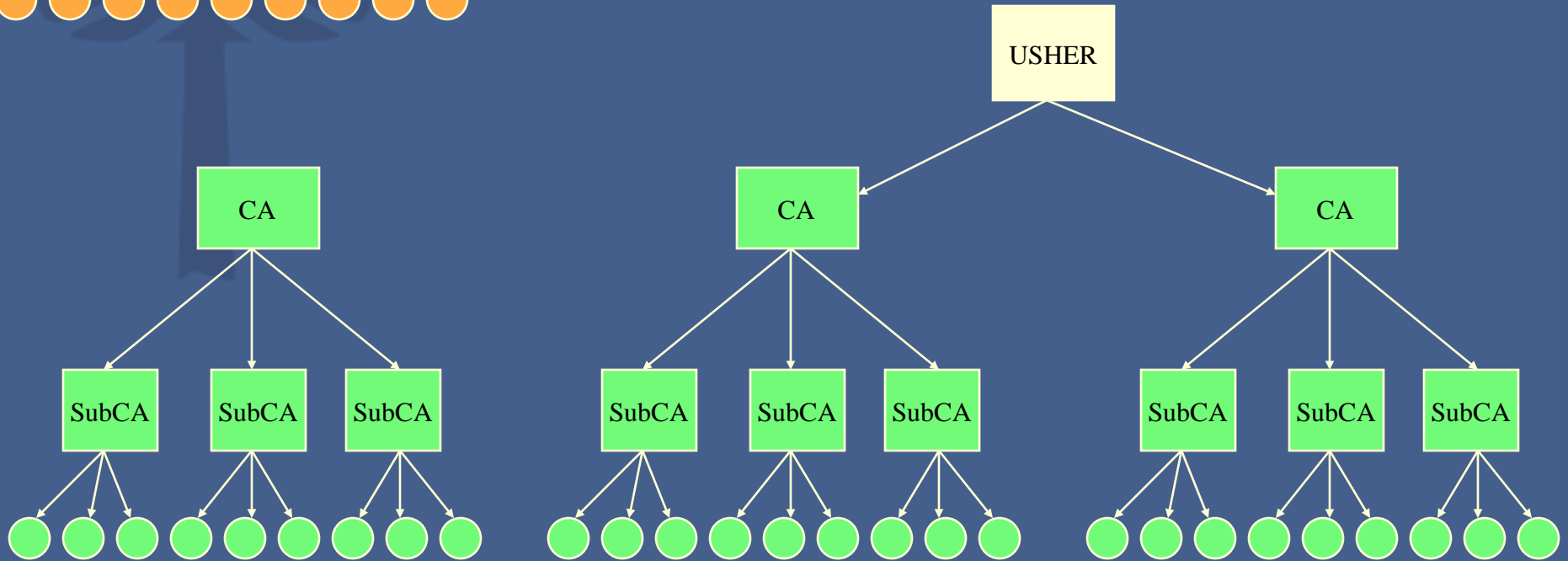
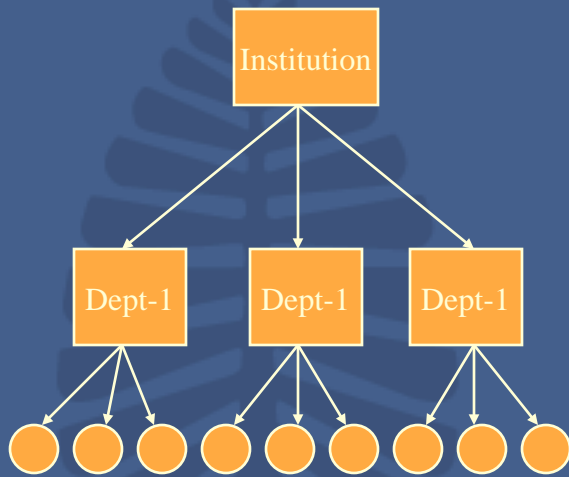
- The USHER PA establishes policy for and oversees operation of the USHER initiatives. USHER PA activities include...
 - approve and certify the Certificate Policy (CP) and Certification Practices Statement (CPS) for the USHER
 - set policy for accepting applications for CA issuance under USHER CAs
 - represent the USHER in establishing cross-certification with other PKI bridges e.g. HEBCA
 - set policy governing operation of the USHER CAs
 - oversee the USHER Operational Authority
 - keep the USHER Membership informed of its decisions and activities.



USHER Project -Progress

- Policy Authority formed
- Prototype USHER operational on the Prototype HEBCA infrastructure
- Production USHER CP produced
- Production USHER CPS produced
- Production USHER Foundation CA created (2/23/06) at Dartmouth College and distributed
- USHER Foundation being embedded in applications (e.g. Lionshare)
- USHER Foundation run from InCommon infrastructure from 2007
- Community contract documentation sufficiently baked
- USHER Campus root available for current InCommon Members

Creating Silos of Trust



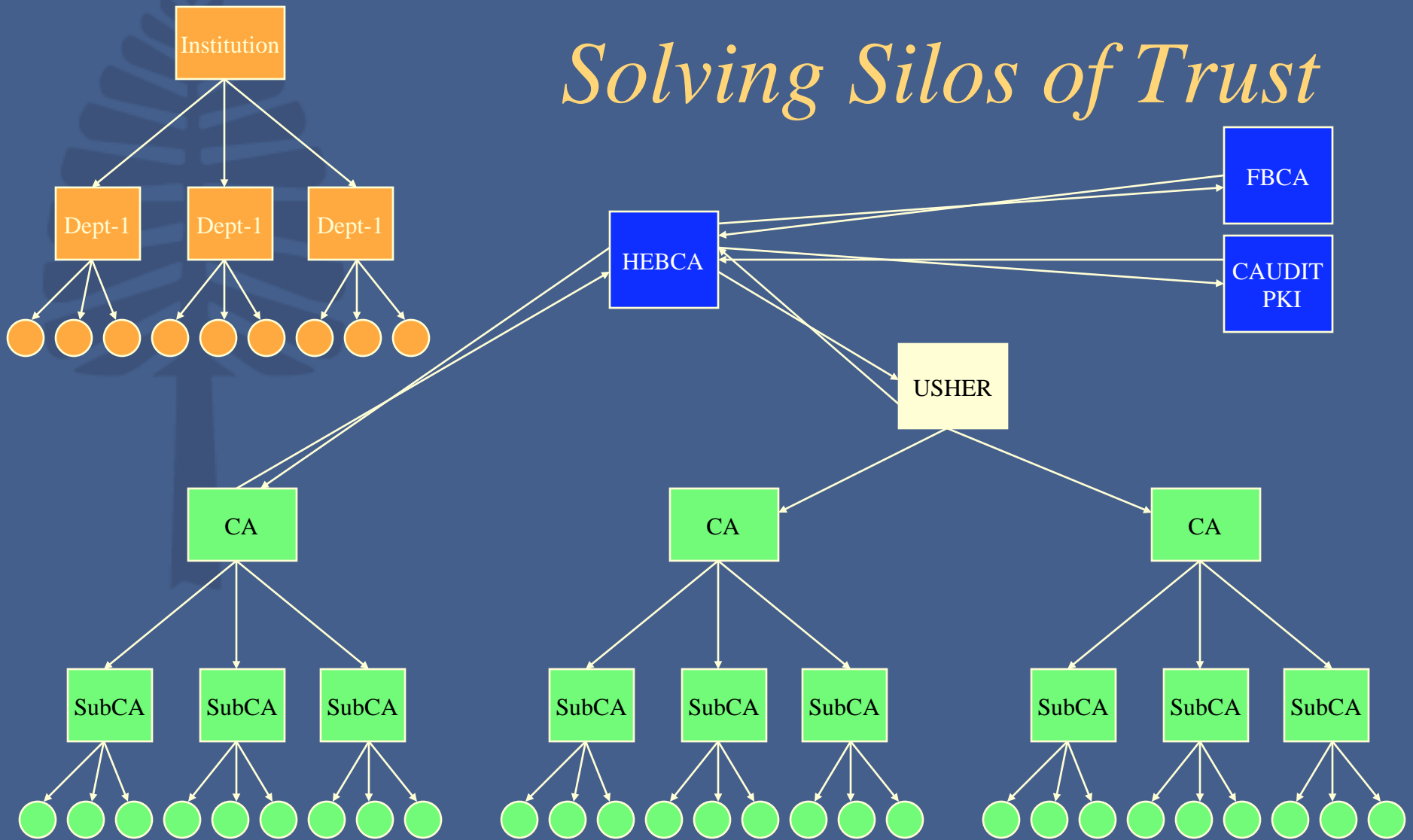
HEBCA : Higher Education Bridge Certificate Authority

- Bridge Certificate Authority for US Higher Education
- Modeled on FBCA
- Provides cross-certification between the subscribing institution and the HEBCA root CA
- Flexible policy implementations through the mapping process
- The HEBCA root CA and infrastructure hosted at Dartmouth College
- Facilitates inter-institutional trust between participating schools
- Facilitates inter-federation trust between US Higher Education community and external entities

HEBCA

- What is the value presented by this initiative?
 - HEBCA facilitates a trust fabric across all of US Higher Education so that credentials issued by participating institutions can be used (and trusted) globally e.g. signed and/or encrypted email, digitally signed documents (paperless office), etc can all be trusted inter-institutionally and not just intra-institutionally
 - Extensions to the Higher Education trust infrastructure into external federations is also possible and proof of concept work with the FBCA (via BCA cross-certification) has demonstrated this inter-federation trust extension
 - Single credential accepted globally
 - Potential for stronger authentication and possibly authorization of participants in grid based applications
 - Applicable for institutions whose policies can not be covered by community efforts e.g. USHER

Solving Silos of Trust





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 Project - Progress

- What's been done so far?
 - Operational Authority (OA) contractor engaged (Dartmouth PKI Lab)
 - MOA with commercial vendor for infrastructure hardware (Sun)
 - MOA with commercial vendor for CA software and licenses (RSA)
 - Policy Authority formed
 - Prototype HEBCA operational and cross-certified with the Prototype FBCA (new Prototype instantiated by HEBCA OA)
 - Prototype Registry of Directories (RoD) deployed at Dartmouth
 - Production HEBCA CP produced
 - Production HEBCA CPS produced
 - Preliminary Policy Mapping completed with FBCA
 - Test HEBCA CA deployed and cross-certified with the Prototype FBCA
 - Test HEBCA RoD deployed
 - Infrastructure has passed interoperability testing with FBCA



HEBCA Project – Next Steps

- What are the next steps?
 - HEBCA to be hosted by commercial CA
 - Provide long term viability
 - Provides an operating platform that leverages economies of scale to keep operational costs down
 - Allows for operation in accordance with defined policies such that meaningful cross-certifications can occur at desired LOA
 - Facilitates reduced audit expenses



HEBCA – A Case Study

- 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

- 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

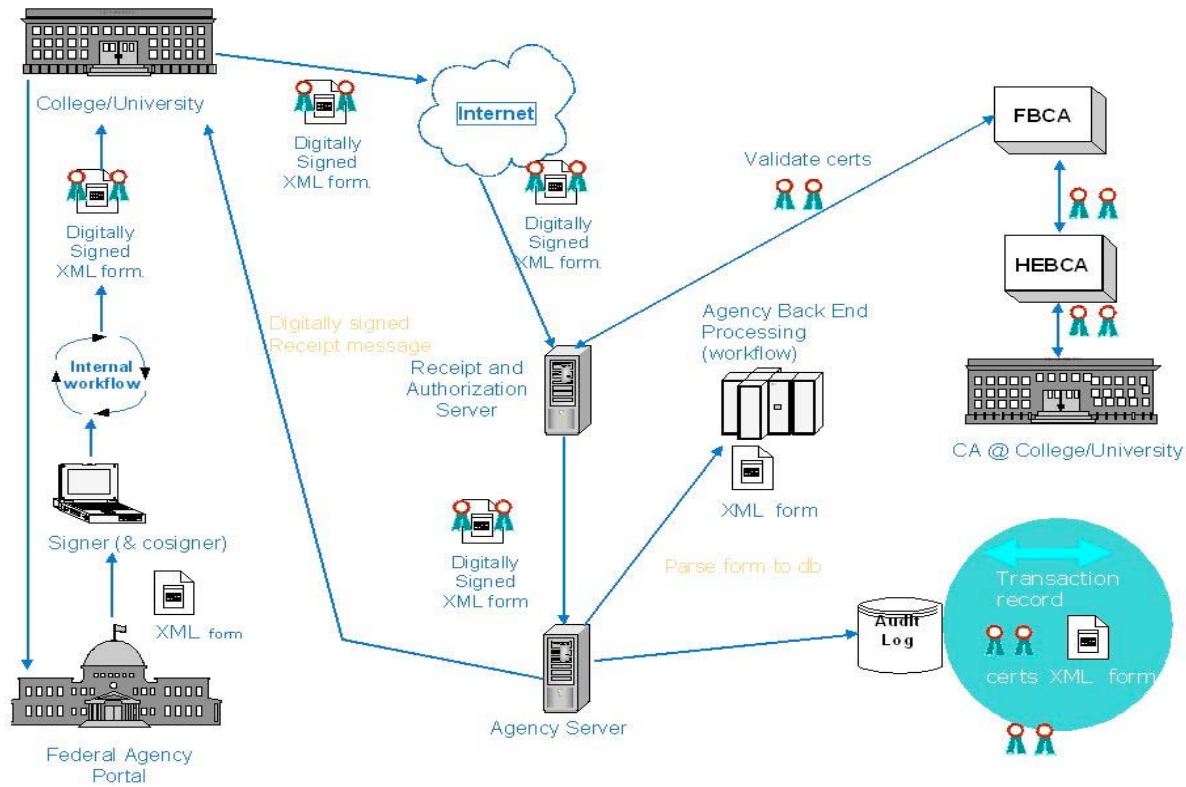
- HEBCA provides an efficient way for participating organizations to establish trust of any identities issued by other participants
- HEBCA uses technological and policy-based processes to assert the level of assurance that community members can place in a given identity certificate.
- As each participant 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

- 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

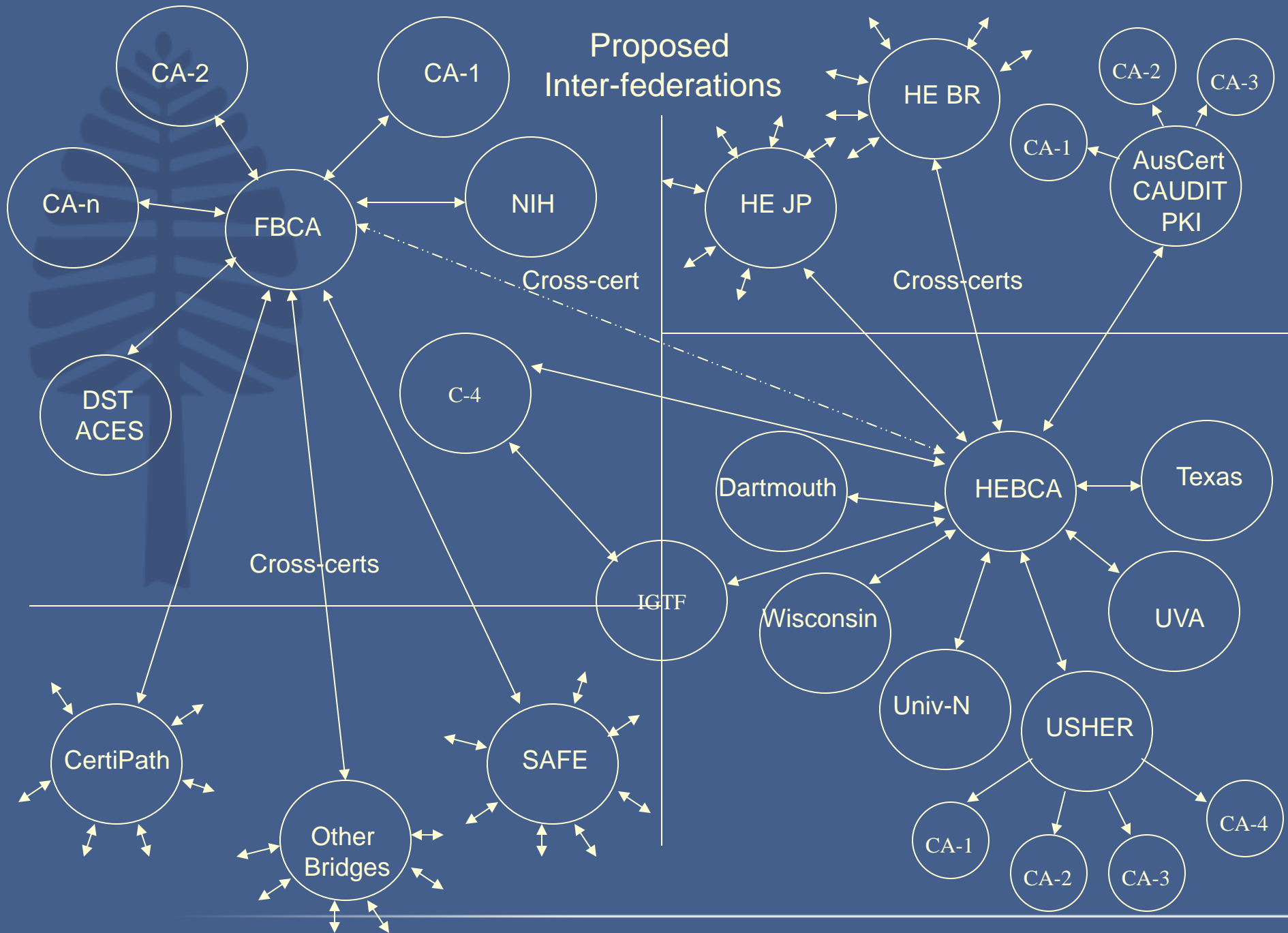
Database is the gateway to the Agency business processes (workflow)



HEBCA – A Case Study

- 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

Proposed Inter-federations





The Four Bridges Forum (4BF)

- The 4BF is an existing infrastructure that facilitates trusted electronic business across major federal agencies, pharmaceutical and healthcare companies, aerospace and defense contractors and colleges and universities
- The 4BF is a federation of PKI identity providers
- It was formed by the nation's leading federated identity trust hubs
- Each 4BF trust hub asserts the identity of participants across the entire federation.

Who is the 4BF

- Federal PKI Architecture (Federal Bridge), serving the major Federal agencies
- CertiPath, serving the aerospace and defense industry
- SAFE-BioPharma Association, serving the biopharmaceutical and healthcare industries
- HEBCA, serving the higher education sector in the United States





How Does The 4BF Work?

- Each 4BF trust hub comprises multiple organizations using comparable policies and procedures to authenticate the identities of its participants
- Each authenticated identity is protected using public key cryptographic technology
- Once authenticated, the identity is uniquely linked to a digital certificate, permitting digital signatures
- The digital certificates from 4BF members are honored across the 4BF federation



The Benefits of the 4BF

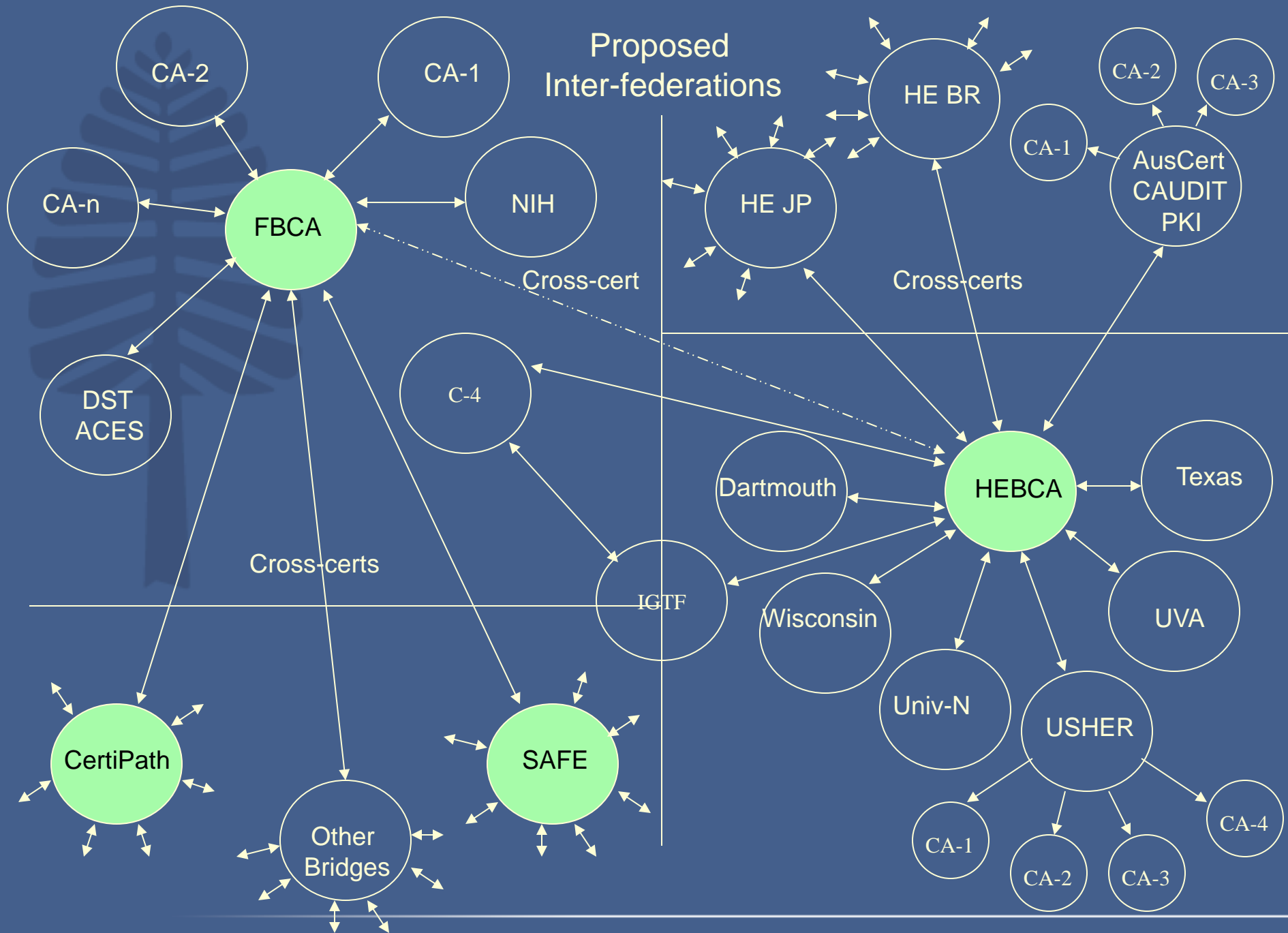
- The identity can be trusted across its originating hub and all other hubs with which it is linked. This allows for trusted interoperability between separate and disparate systems.
- The identity can be used to authenticate individuals to access a variety of resources and to conduct other important business transactions.
- The digital certificates bearing the identity can be used for digital signatures that can be trusted across the federation.
- The digital certificates can also be used to facilitate confidential messages between 2 previously unconnected parties with the federation.



Summary

- There are multiple PKI initiatives within US higher education that cater to different communities of interest
- USHER is an Internet2 initiative that allows interoperability amongst its HE members based on adoption of a common policies
- HEBCA is an EDUCAUSE initiative that allows interoperability amongst its HE members based on policies that are mapped to various Levels of Assurance
- The 4BF is also based on policy mapping, but allows the HE community to interoperate with communities of interest outside HE e.g. Federal government, pharmaceutical industry, aerospace and defense industry
- USHER is a member of HEBCA, HEBCA is a member of 4BF

Proposed Inter-federations





For More Information

- HEBCA Website:

<http://hebca.dartmouth.edu/>

- 4BF Website:

<http://www.the4BF.com/>

Scott Rea - Scott.Rea@dartmouth.edu