

PKI: Glue of Middleware

Michael R Gettes, Duke University

EuroCAMP

November, 2005

Landscaping

- PKI Hierarchies and Bridges
- National PKI
- HEBCA, USHER, InCommon
 - Gap Analysis
 - Development and Cost Sharing
 - EDUCAUSE and Internet2
- Federation Crosswalk
 - InCommon & US Federal Government eAuth (again!)
 - I-CIDM and JSF

Reminder ...

- SSL/TLS
- SAML
- Browsers
- Servers
- Shibboleth
- Client PKI issues, CRLs, authentication

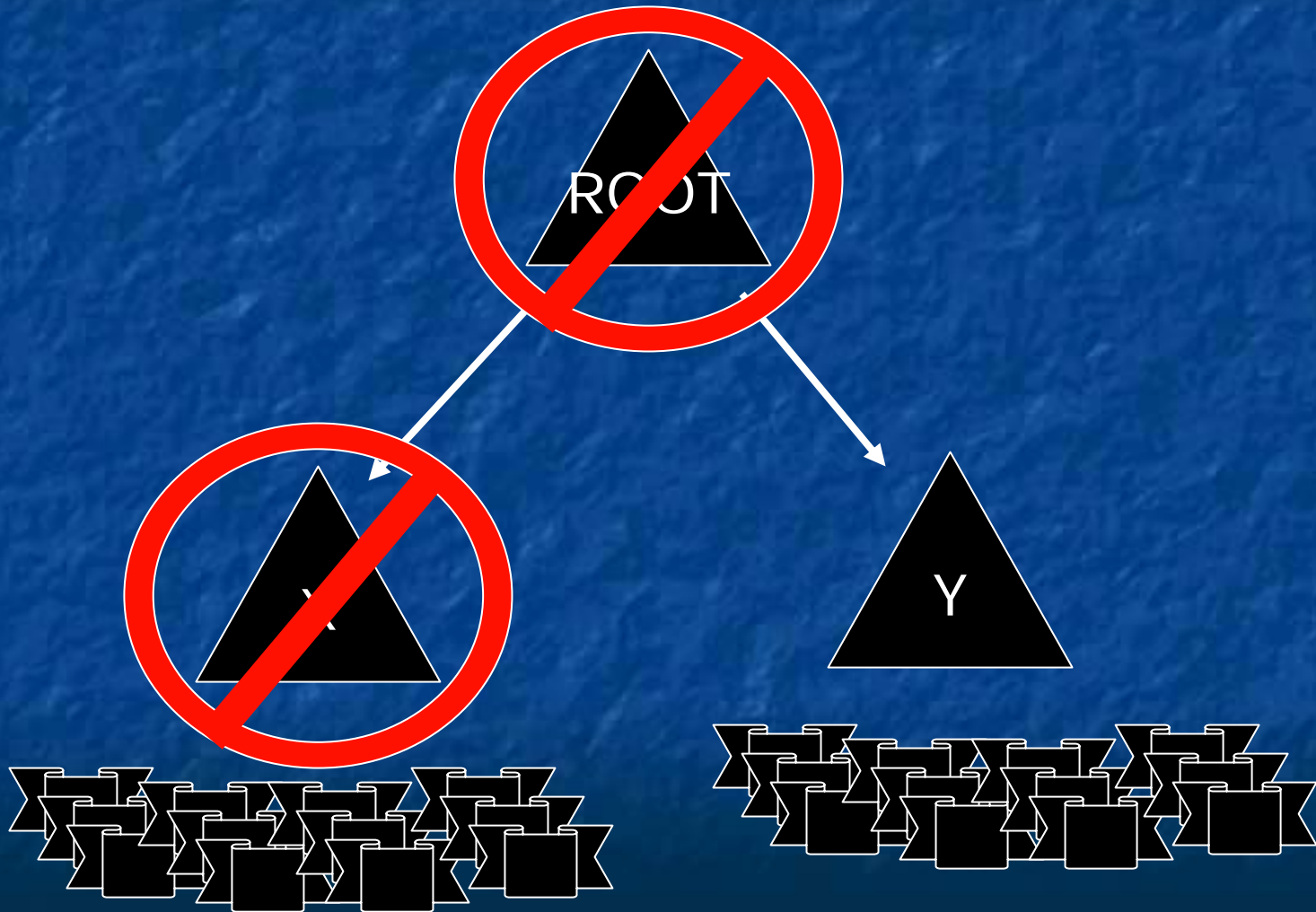
Directories *are* part of the I in PKI

- Directory
 - Centralized, automated Name Space
 - VERY carefully controlled
 - Users modify very little
 - Priv'd access highly restricted
 - Control considered necessary step for PKI to **trust** the directory
 - Eventually, client, server and other certs/CRLs will be published in the directory.

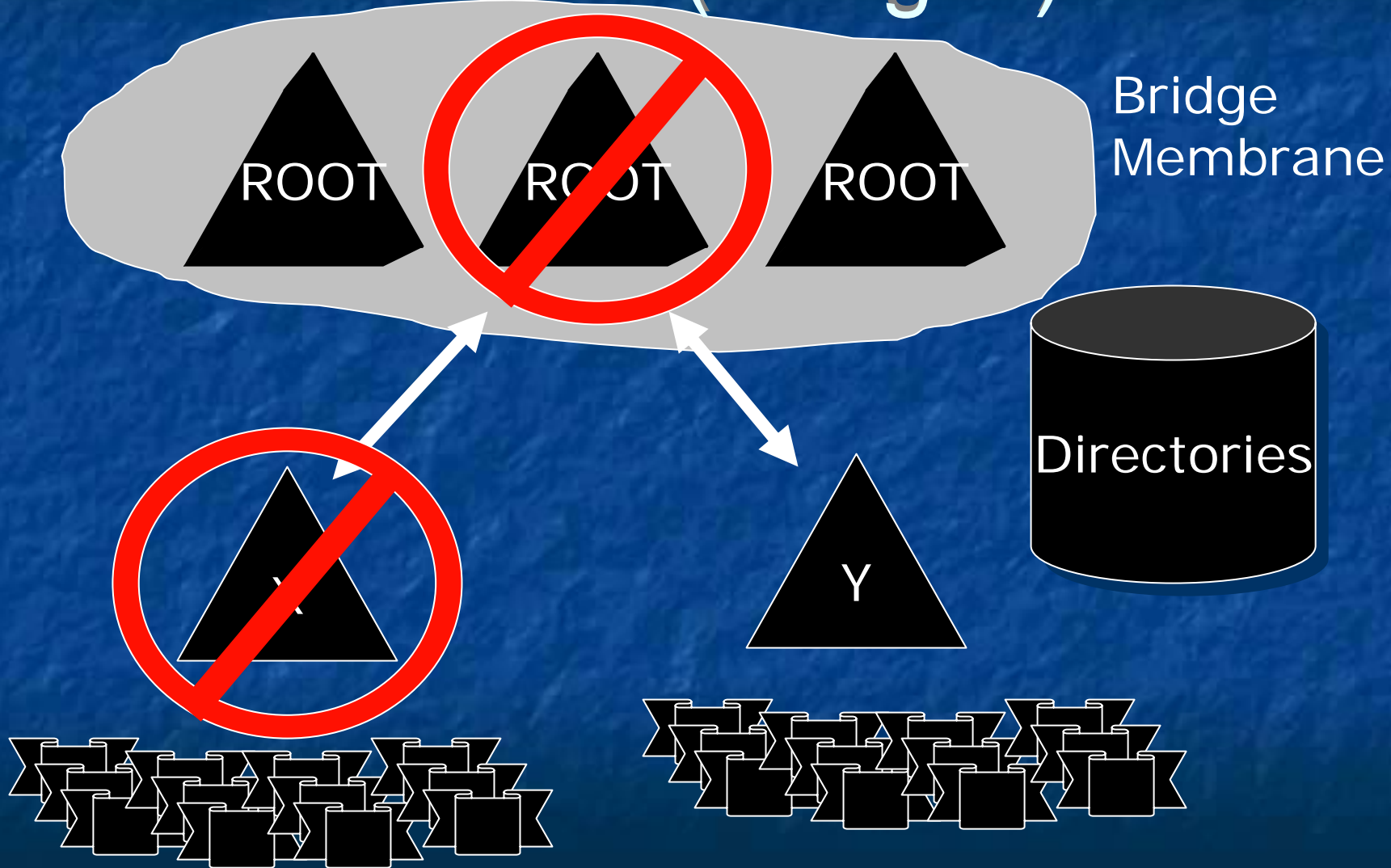
Are the Directories part of I in PKI?

- Kx509 (part of NMI distribution)
 - Short-lived Certificates
 - Avoids CRL and Directory Publications
- MIT
 - 1 year certs, but people can get all they need using Kerberos Authentication
- But... A namespace infrastructure is still assumed and they all have it.

PKI Basics (Hierarchies)

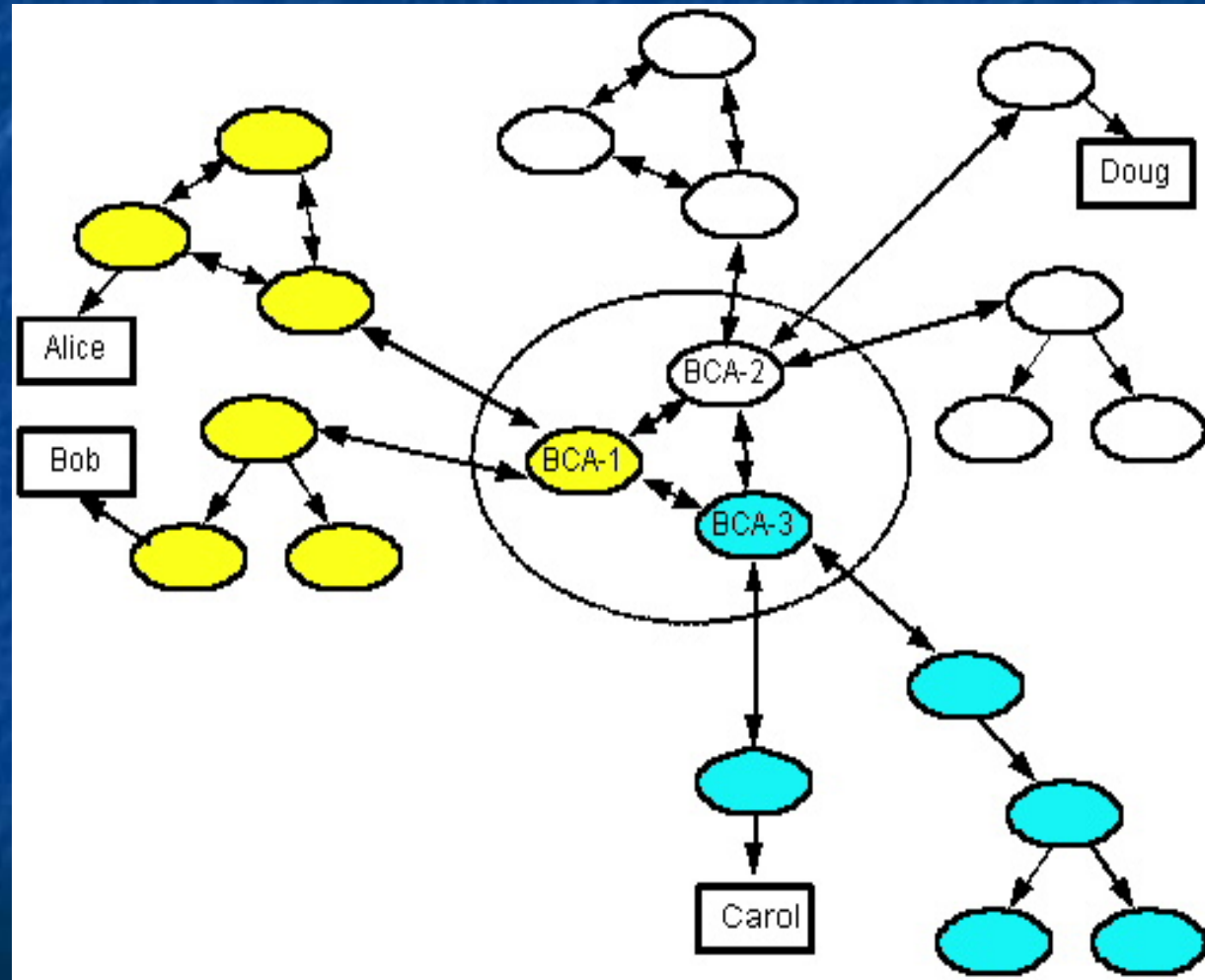


PKI Basics (Bridges)

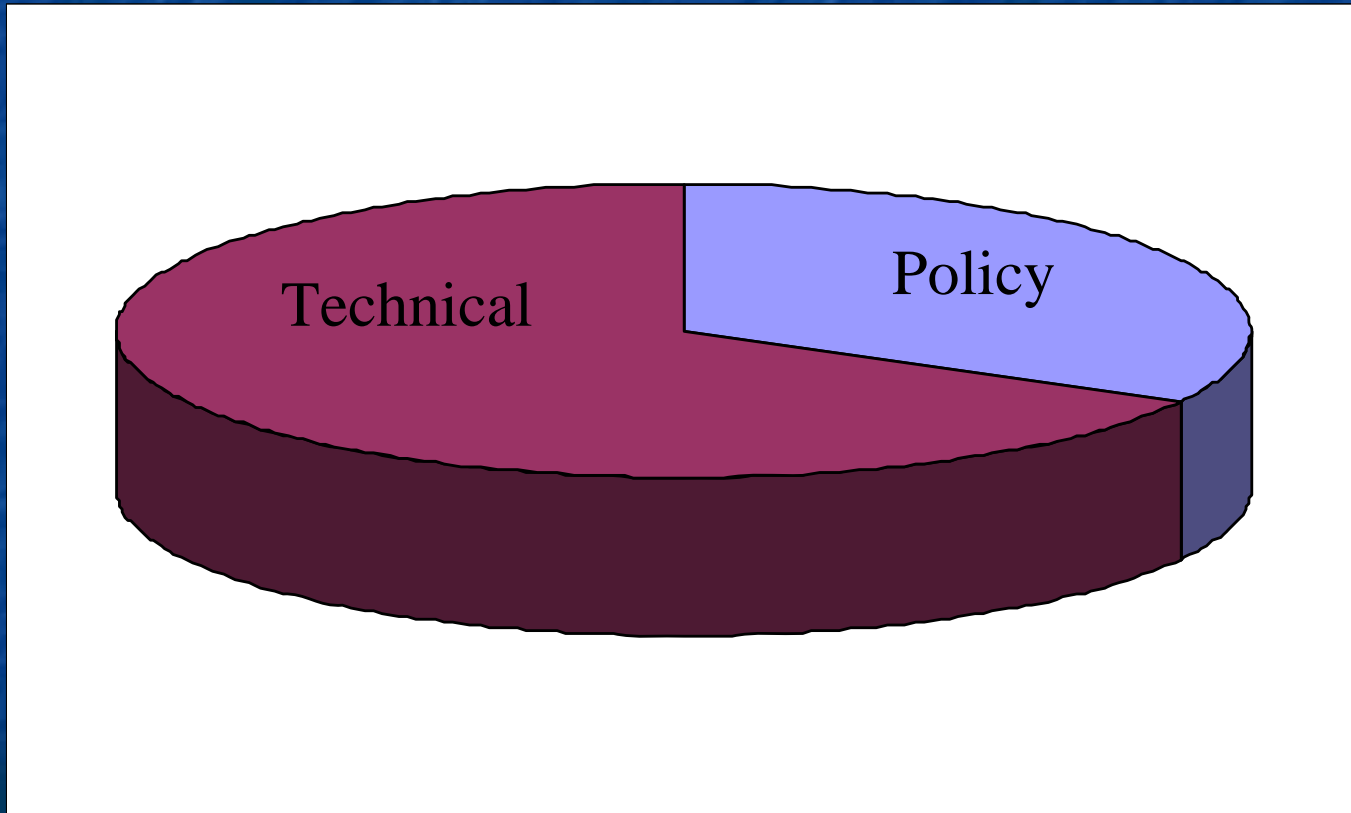


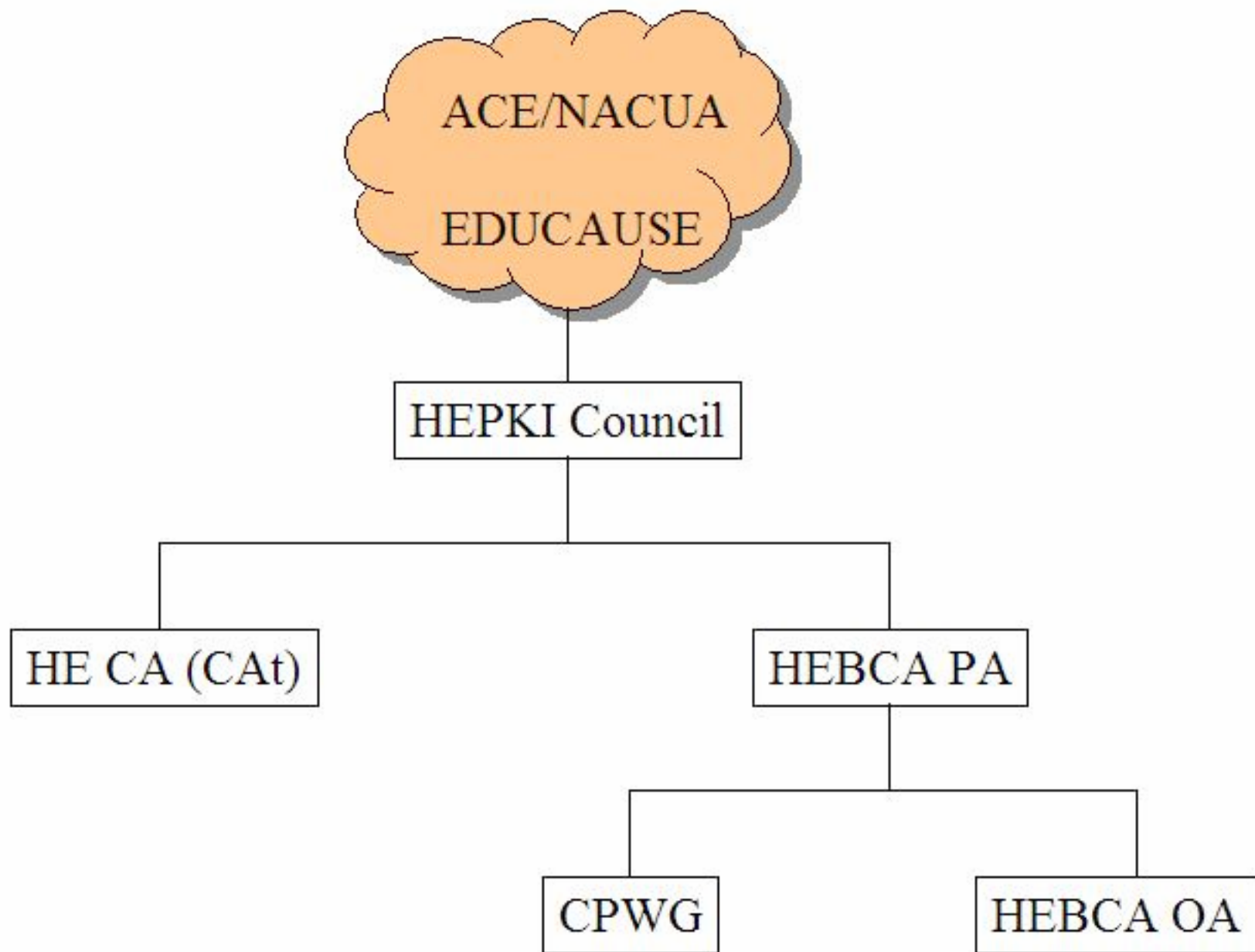
Multiple CAs in FBCA Membrane

- Survivable PKI
- Cross Certificates allow for “one/two-way policy”
- Directories are critical in BCA world.
- Clients changing



**PKI is
1/3 Technical and 2/3 Policy?
Right?**





HEPKI Council

- Jack McCredie, Chair, UC Berkeley
 - Michael Baer, Sr VP ACE
 - Rich Guida, Johnson & Johnson
 - Mark Luker, EDUCAUSE
 - Mark Olson, EVP of NACUBO
 - Dave Smallen, CIO @ Hamilton College
 - Nancy Tribbensee, Counsel @ ASU
- Not operational, policy and oversight
- Will approve the creation of the HEBCA Policy Authority
 - Completed November 15, 2004
- Charged with Higher Education direction and strategy for PKI initiatives, not just Bridge
- Rarely meets! Is this a problem?

HEBCA Policy Authority

- Created January 1, 2005
- Mark Franklin, Dartmouth College, Chair
 - Nancy Tribbensee (ASU & Counsel)
 - Sheila Sanders (UAB)
 - Mark Luker (EDUCAUSE)
 - David Wasley (UCOP)
 - Barry Ribbeck (Rice)
 - Keith Hazelton (Wisconsin-Madison & InCommon)
 - Michael Gettes (Duke)

On Campus

- End Entity: Some schools, MIT, Dartmouth, UTHSC
 - but not wide deployment in US. i2 trials on Doc Sigs
- Server Side and Infrastructure -- used all over the place but not yet well coordinated
- Lacking a national infra for Higher Ed
 - HEBCA/USHER/InCommon/SAML
- PKI is just 18 months away (again!) :-)

PKI in HE – 5 likely “Killer Apps”

- Signed E-mail
 - Stop identity spoofing from weak passwords, etc.
 - Increase use of electronic commerce at campus & Institutional & national levels
- Windows and Office Applications Interop
- Shibboleth
- GRID Computing Enabled for Federations
- E-grants
 - Faster, secured grant processing
 - Faster (e-)payments
 - More secured communications & fund Xfers
 - Federal focus is on this initiative

US Higher Ed Root:USHER

- To use ID Proofing policies of CREN augmented for InCommon
- Low Barrier to entry
- Coming from Internet2
- Should be X-Certified with HEBCA
- Analog to US Federal Root CA
- Approval to proceed Feb 27, 2005

HEBCA Current Status

- HEBCA Certificate Policy (brother Wasley)
 - Will develop CPS from this policy (have draft)
- Dartmouth College
 - Contracted to implement HEBCA in 12/03
 - EDUCAUSE funded
 - Received AEG from Sun Microsystems (\$50K)
 - Equipment ordered and received
 - Signing Hardware -- not yet.
 - Working software agreement with RSA as first CA in bridge
 - Maybe even further deal with Higher Ed for CA services & s/w
- Informal cross-certification with US Gov completed
- Will operate at High Level of Assurance

I-CIDM

- International Collaboration on Identity Mgmt
 - Joint Strike Fighter Program (big \$\$\$\$)
- Rules of Engagement
 - Citizenship, Legal, Technical, Policy & Process (Criteria & Methods, CP/CPS, Corporate Policy)
- Principal Parties
 - US Higher Education Bridge (HEBCA)
 - US Government Bridge (FBCA)
 - Pharmaceutical Industry (SAFE)
 - Commercial Aerospace (JSF, www.tscp.org)
 - Internationally Driven and Participation

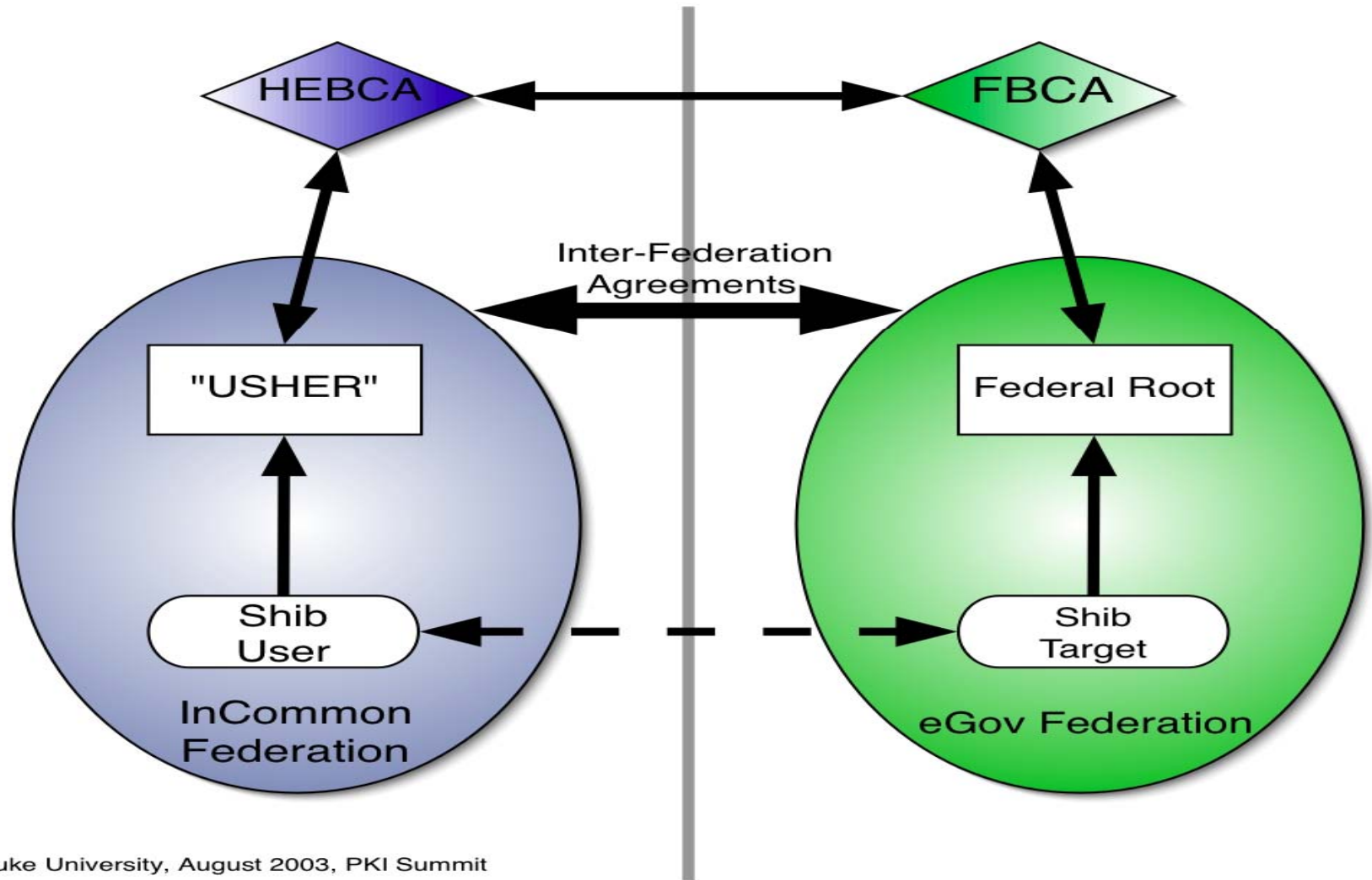
HEBCA/USHER Synergy

- Sun Hardware Donation
- RSA/Keon Software Donation
 - License covers Cert issuance for all PKI ops
- High Level of Assurance
 - Separation of Duties
 - Admin, Operator, Officer, Auditor
 - Revocation and Citizenship Issues
- Ops(Dartmouth); RA/Storefront(Internet2)
- Need to interoperate with US Feds

InCommon & eAuth

- Federation interop with Shib (PKI in SAML)
- To ultimately use Bridge PKI as means of validating and locating members of OTHER federations
- InCommon CA to X-Certify with HEBCA or be signed by USHER having been X-Certified with HEBCA
- Shib+Grid to address some Grid issues
- HEBCA+Grid considered but no work yet
- See next slide...

Leveraging a Global PKI (bridged) to allow for inter-Federation activities
(Example: assumes shib is bridge aware)



Federated Digital Signatures

- Proposed for Phase 5 of PKI Interop Project
- Use Local PKI for workflow and signatures
- When document leaves local domain, substitute institutional signature and XML blob describing roles, digital rights & IPR, archival status, etc (IFA)
- Why do this? Bridges + Inter-Federation Agreements (IFA) can address this -- something else to avoid Bridges. We need to figure out what goes into IFAs to make this useful.

RSA and Higher Education

- RSA has donated CA software for HEBCA
- RSA about to donate software for USHER
- RSA deal amounts to supporting National Security Infrastructures for Higher Education in USA
- Allowed to issue thousands of certs for purpose of managing PKI nationally, not locally.
- Next step -- get server certificates for all of HE in USA

PKI Viability

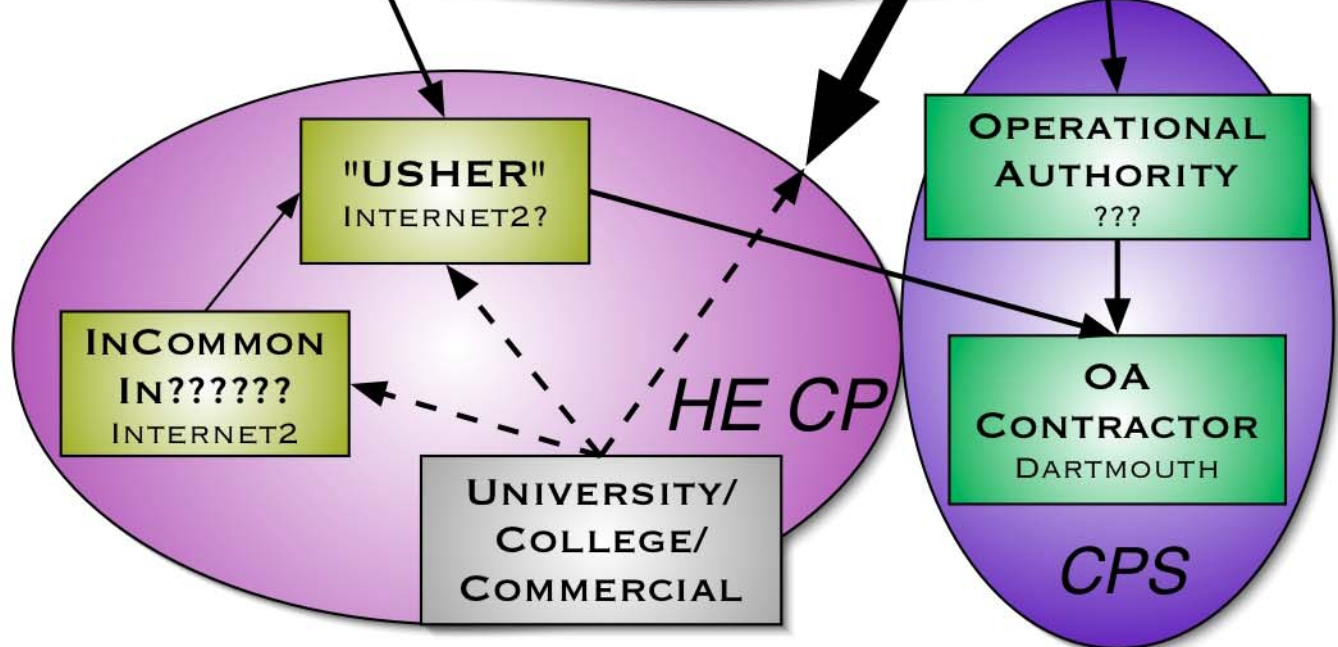
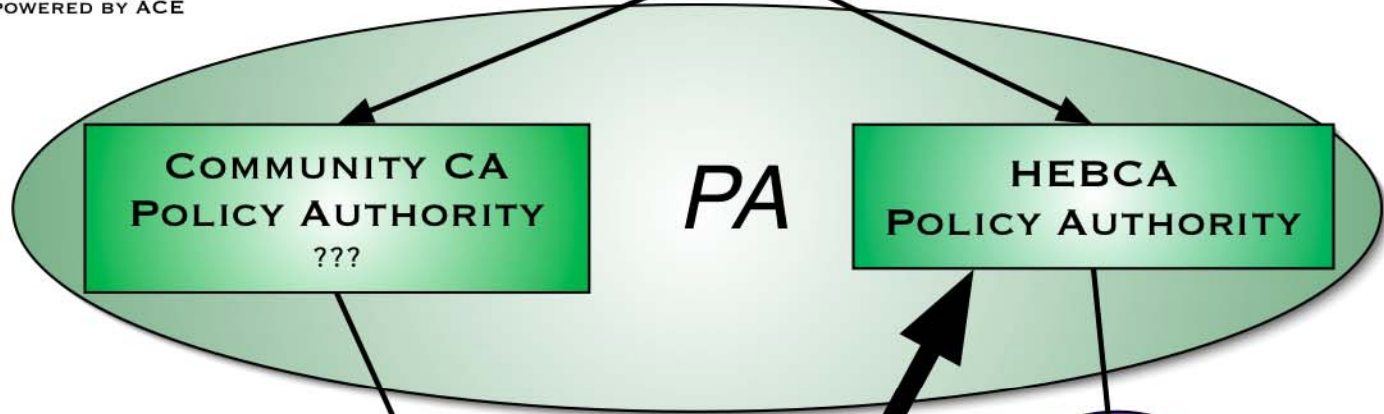
- Good for Infrastructure
 - Shibboleth
 - SAML
 - SSL/TLS for Web, LDAP, IMAP, SMTP ...
- Not good for end users
 - STILL too complex a technology
 - Human beings understand passwords
- Need to combine PKI with other techniques

HIGHER EDUCATION NATIONAL PKI & "TRUST" INFRASTRUCTURE

EDUCAUSE EMPOWERED BY ACE



It's LoA Expressions
and
Mapping All
the Way Down.



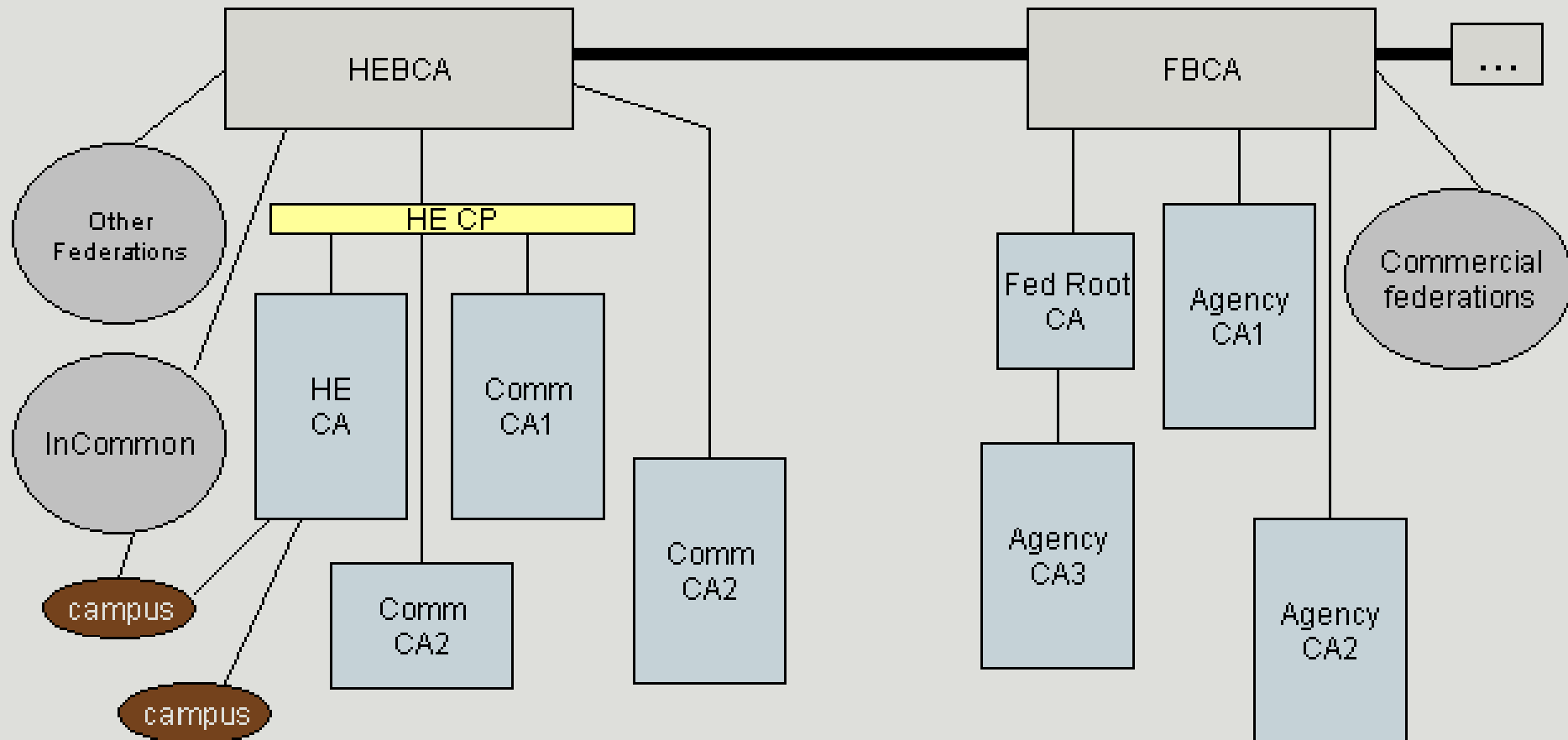
Marketing and
Business Plans
for BCA and
Comm CA
Services

TBD

maybe aligned
with HEPKI
Council

Global? Trust Diagram (TWD)

Trust diagram



US-Centric View of PKI World

