



Alabama Middleware Workshop

Sponsored by UAB and the NSF/Alabama EPSCoR
Internet2 Initiative, Grant No. 0091853.



UAB Public Key Infrastructure

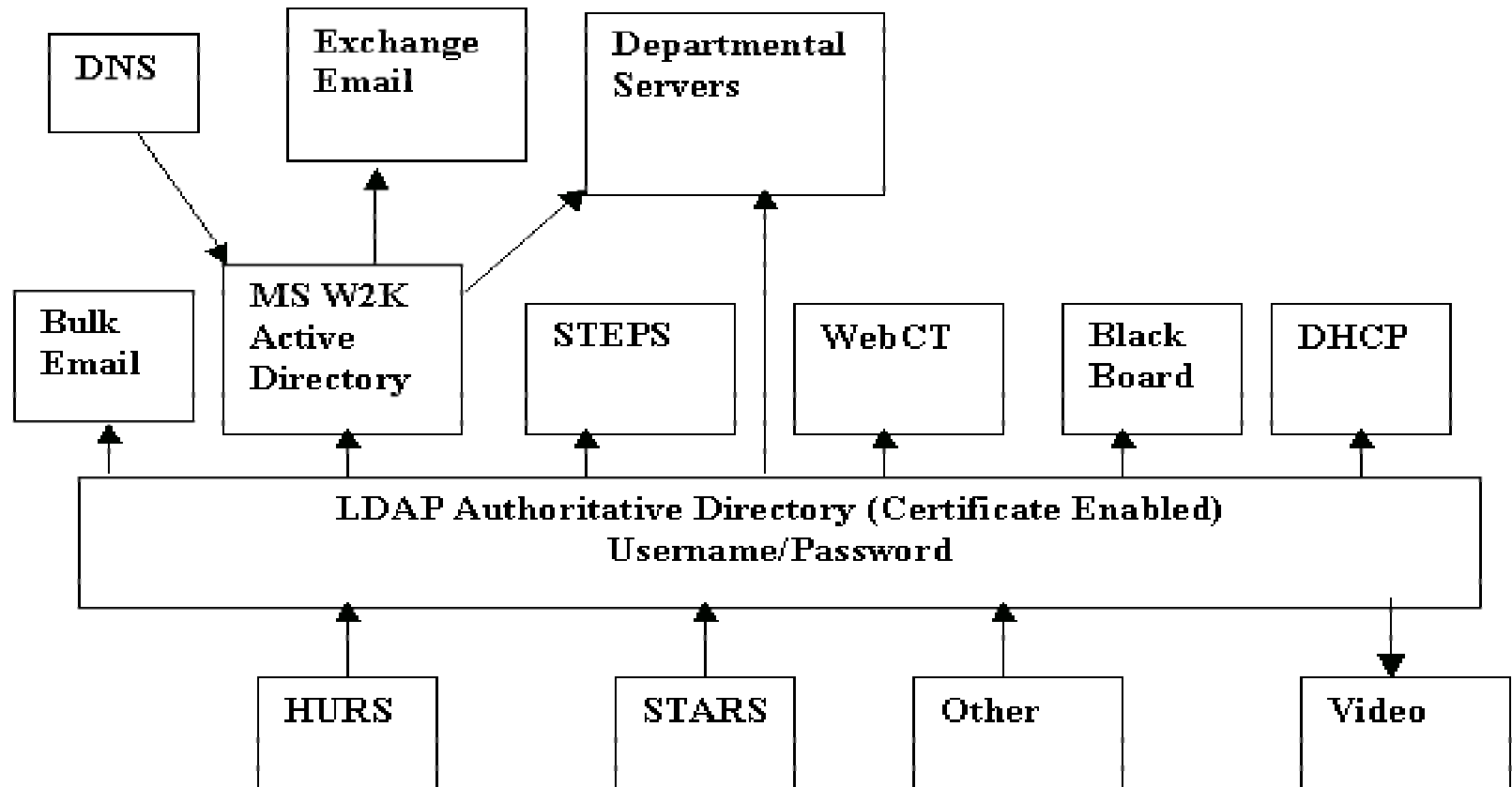
Tim Brown

Director, IT Infrastructure Services

University of Alabama at Birmingham

tbrown@uab.edu

UAB Middleware Infrastructure





UAB Public Key Infrastructure

- Two uses for keys
 - Digital signatures
 - Certificate guarantees I am who I say I am
 - Encryption



Project Milestones

- Contracted with Digital Signature Trust to provide both Personal and Server Certificates
- Immediately began issuing server certificates
- Developed application for distribution of DST Personal Certificates
- Digital Signature Trust purchased by Identrus



Pilots Proposed for Signatures

- Authentication\Access
 - Network (ResNet)
 - Systems (Firewalls, servers)
 - Application (WebCT, Virtual Desktop)
- Authorization
 - EDUCAUSE – NIH PKI Interoperability Pilot Project



Current\Proposed Uses for Encryption

- Immediately began issuing server certificates
 - Allows for secure 128-bit SSL encryption
 - To date, we have issued certificates for various versions of IIS and Apache
 - Immediate goal is to have no unencrypted passwords sent across our network
 - Ultimate goal is to have no passwords sent across network and to use Personal Certificate for authentication
- Can be used to encrypt e-mail
 - Must have recipient's public key to send an encrypted message



Problems so far...

- Installation scheduled for week after Sept. 11
- Application development
 - DST changed protocols for issuing certificates at install time
 - Documentation was spotty at best...
- Server Certificates
 - DST certificates did not work well with older browsers (IE 5.0 and earlier)
 - Decided this was a benefit, as older browsers did not support 128-bit encryption. 128-bit is now required.



Problems so far...

- Key escrow for encryption
 - Scenario: Employee is unavailable and access is needed to vital, encrypted, information.
 - How does the institution access that information?
 - Does the institution store the private key? How?
 - Possible solution: Use two separate key pairs, one for signature and another for encryption. Escrow the encryption key while keeping the signature key secure.



Questions?
