

# Next Steps in Two-Tiered PKI for SURAggrid

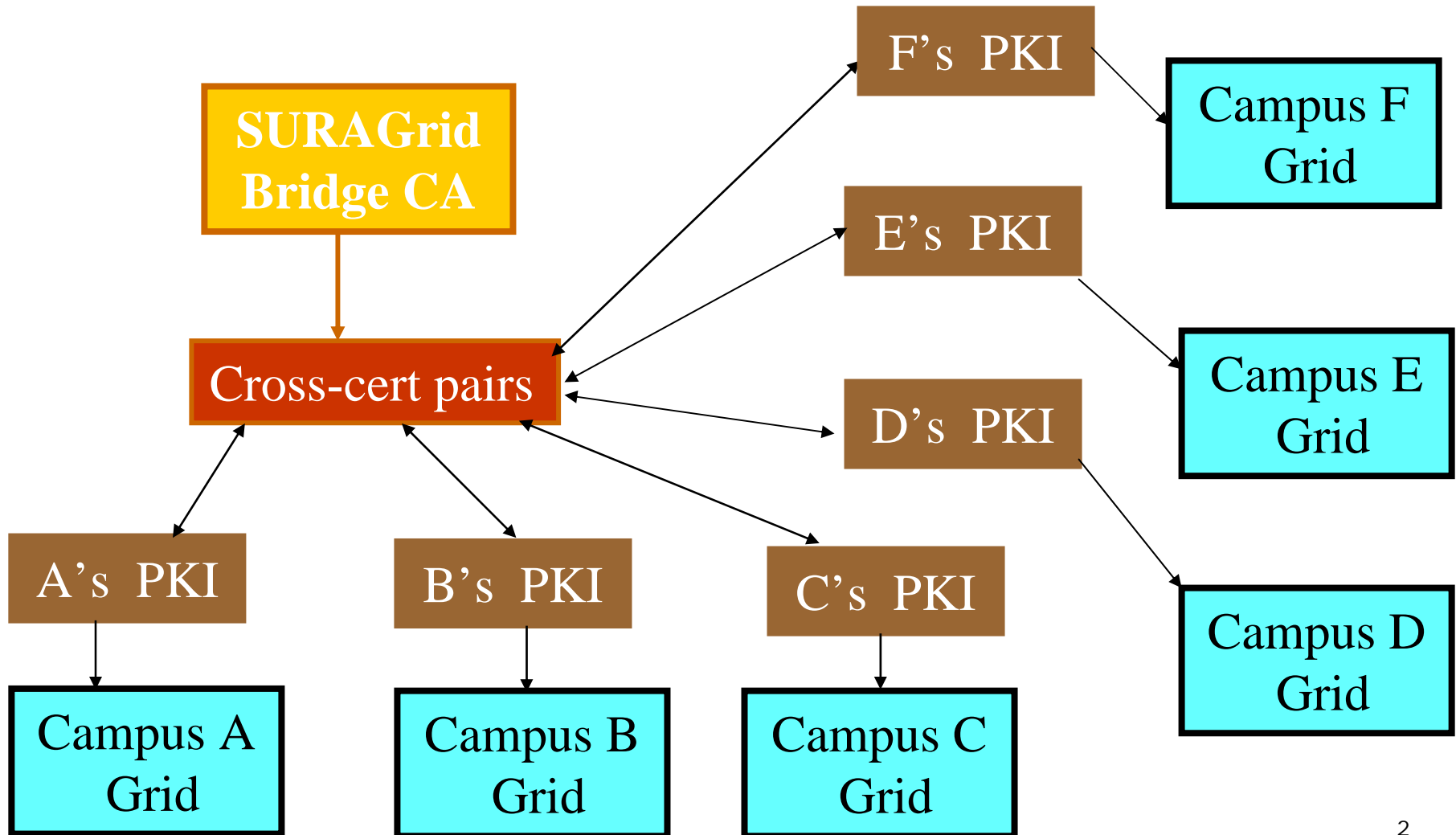


SURAggrid Meeting  
March 16, 2007

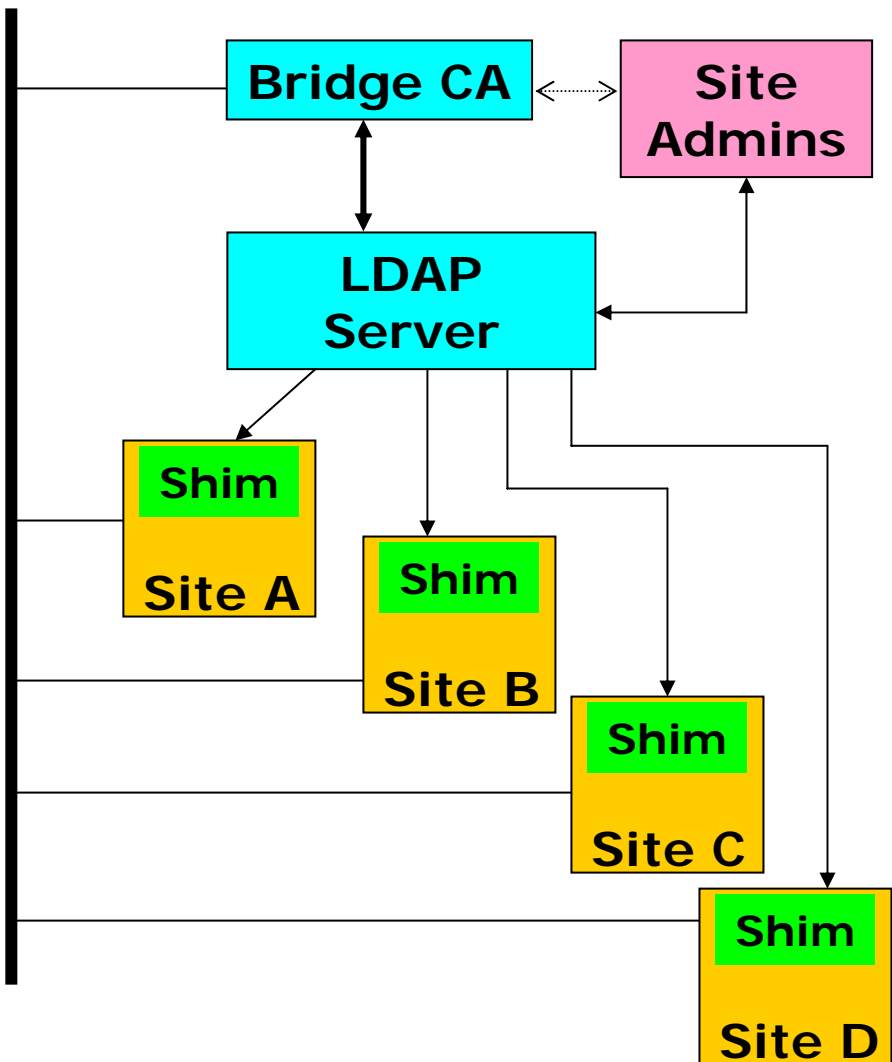
Jim Jokl  
University of Virginia

# Schematic of SURAGrid Globus PKI Integration

---

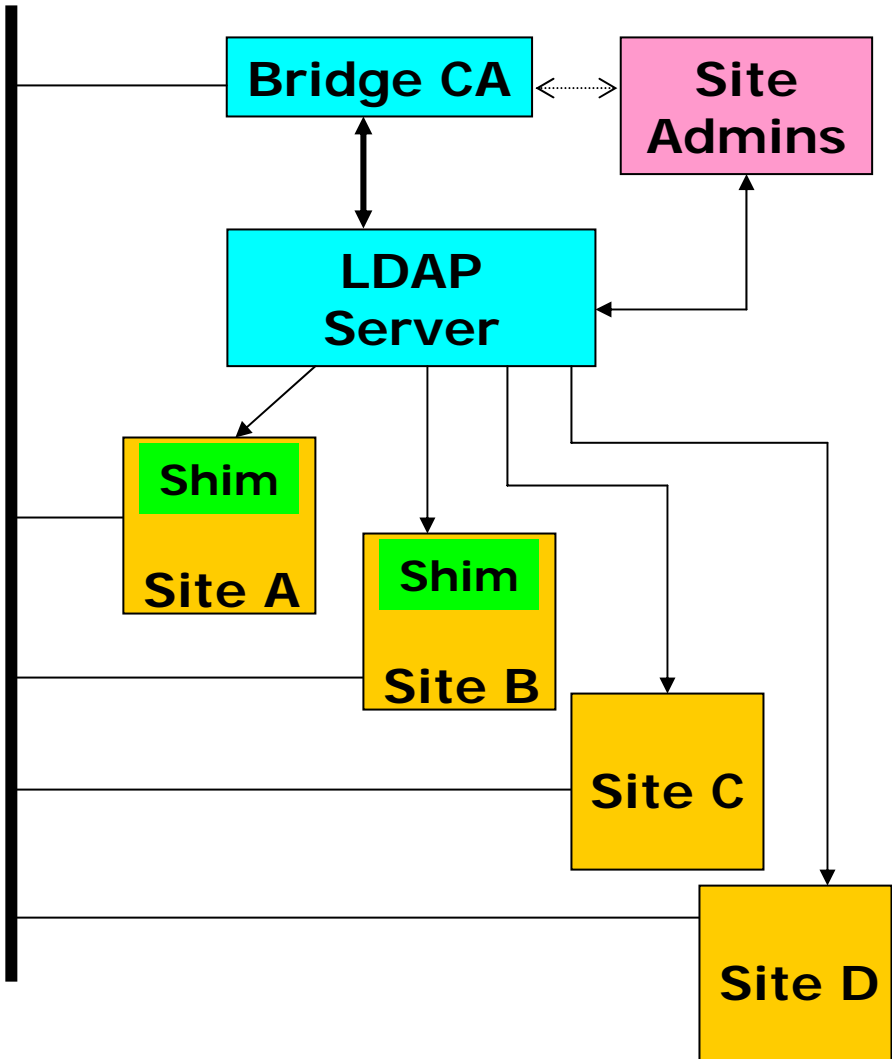


# SURAGrid: Original Plan



- Sites provide dedicated systems
  - Trust fabric via SURAGrid Bridge CA
    - Evolve to use HEBCA & USHER when ready
  - LDAP server(s) hold
    - Cross-certificate pairs
    - Globus policy files
    - Unix UID information
    - Unix login names using a naming convention
  - Shim Software
    - Automates grid\_mapfile
    - Manages Unix accounts
  - Site Administrators
    - Manage their own users enabling or disabling their access to SURAGrid

# SURAGrid: Current Architecture



- Some sites will dedicate systems, others will utilize shared resources
  - The Bridge CA, LDAP servers, and Site Admin infrastructure remain the same
  - Sites that dedicate resources will continue to use the Shim
  - Sites providing pieces of shared infrastructure will leverage the data in the LDAP servers as needed
    - Some tools are provided for grid-mapfile, cross-certs<sub>4</sub>, etc

# SURAggrid PKI Survey Results

---

- Sources of certificates
  - Campus CAs
  - Research group CAs
  - Strength of identity proofing and operations varies widely among SURAggrid meeting
- Many indicated a desire for a higher LoA
  - Few indicated current application requirements
- Credentials interoperability
  - Many sites want to be able to use their SURAggrid credentials elsewhere / everywhere

# Somewhat unclear SURAgrid sites are willing to do for a higher LoA

---

- ❑ Identity proofing requirements
  - In-person vs. derivative vs. ad-hoc
- ❑ CA operations
  - Formal Policies & Practices documents?
  - Separation of responsibility?
  - Revocation?
  - ...
- ❑ Protection
  - Private key protection hardware or off-line
  - Network level protections
  - ...
- ❑ How does the audit function happen?
  - Extensive documentation requirements

# Tiered PKI & SURAggrid

---

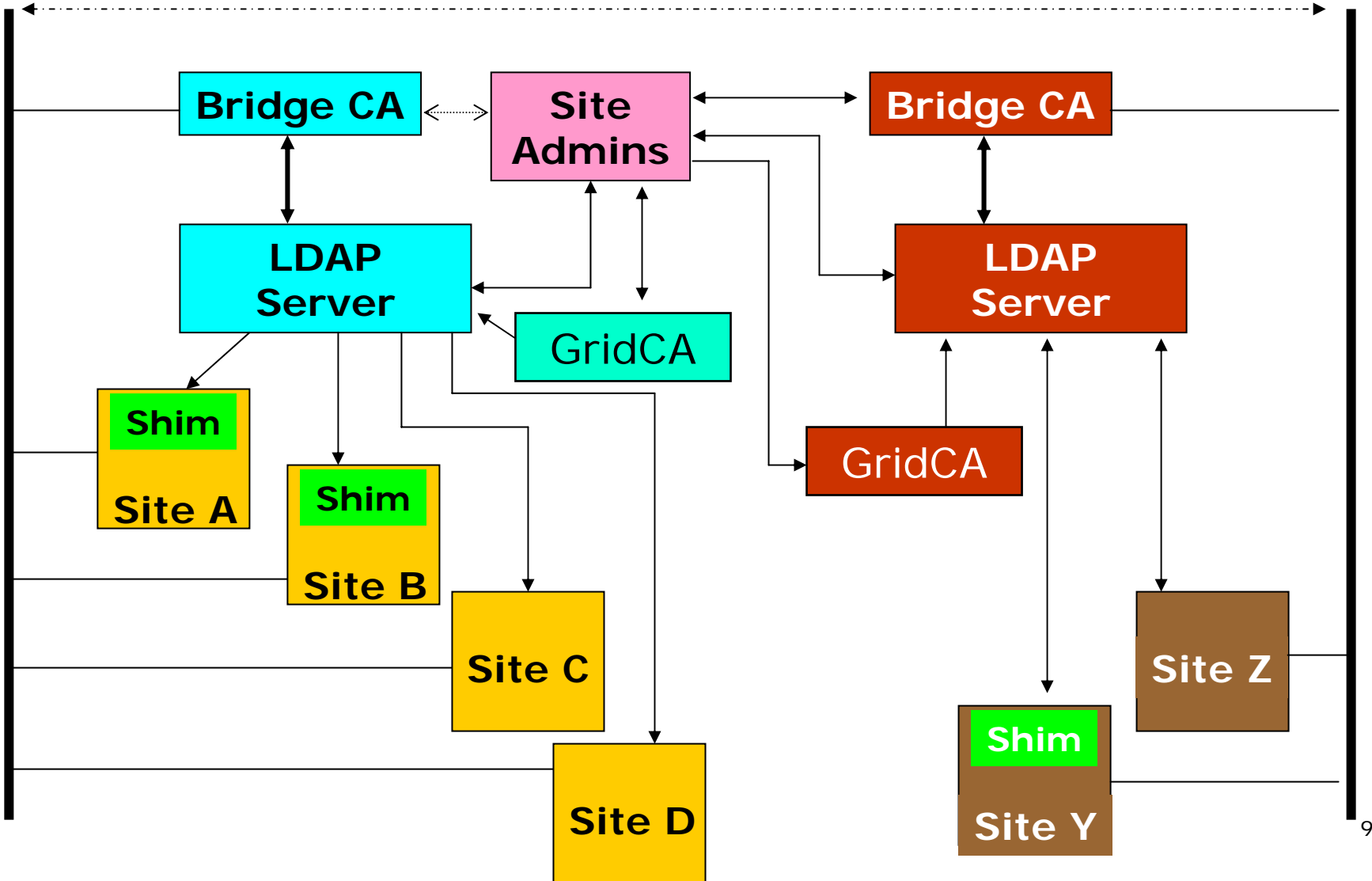
- Support the use of different Levels of Assurance (LoA) on SURAggrid
  - The existing “we trust each of the members of our community” model
  - Something stronger (e.g., USHER practices)?
    - HEPKI PKI-Lite
    - USHER-foundation & Expected Practices
  - A higher LoA that matches the IGTF Classic PKI profile?

# What should we do next?

---

- Add an existing LoA SURAGrid CA?
  - Help with the guest credentials
- Strong AuthN for SURAGrid Site Administrators?
  - 2-factor PKI hardware tokens (likely SafeNet iKey)
  - Access to the SURAGrid Directory (does single sign-on)
  - Submission of CSRs
  - Certificate signing requests
- A Bridge infrastructure that operates at a much higher LoA?
  - How many sites plan to operate CAs at this level?
- A SURAGrid CA that is IGTF/TAG-PMA certified?
  - Directly issues User and Server certificates
  - Still retains campus ID proofing issues
- Others
  - ....
  - ....

# A Future Picture?



# What are the priorities (what is next)?

---

1. Suragrid CA that issues certificates based on site-admin vouching (e.g., site-based RA)
  1. Could be at one or both LoAs
  2. InCommon could be reasonable for ID Proofing for direct issue for existing SURAGrid LoA certificates
2. Strong identification for Site Admins
  1. Hardware tokens
  2. Provides Idap single sign-on
3. ...