Department of Defense High Assurance PKI Implementation & Operations

RSA Conference

17 January 2000

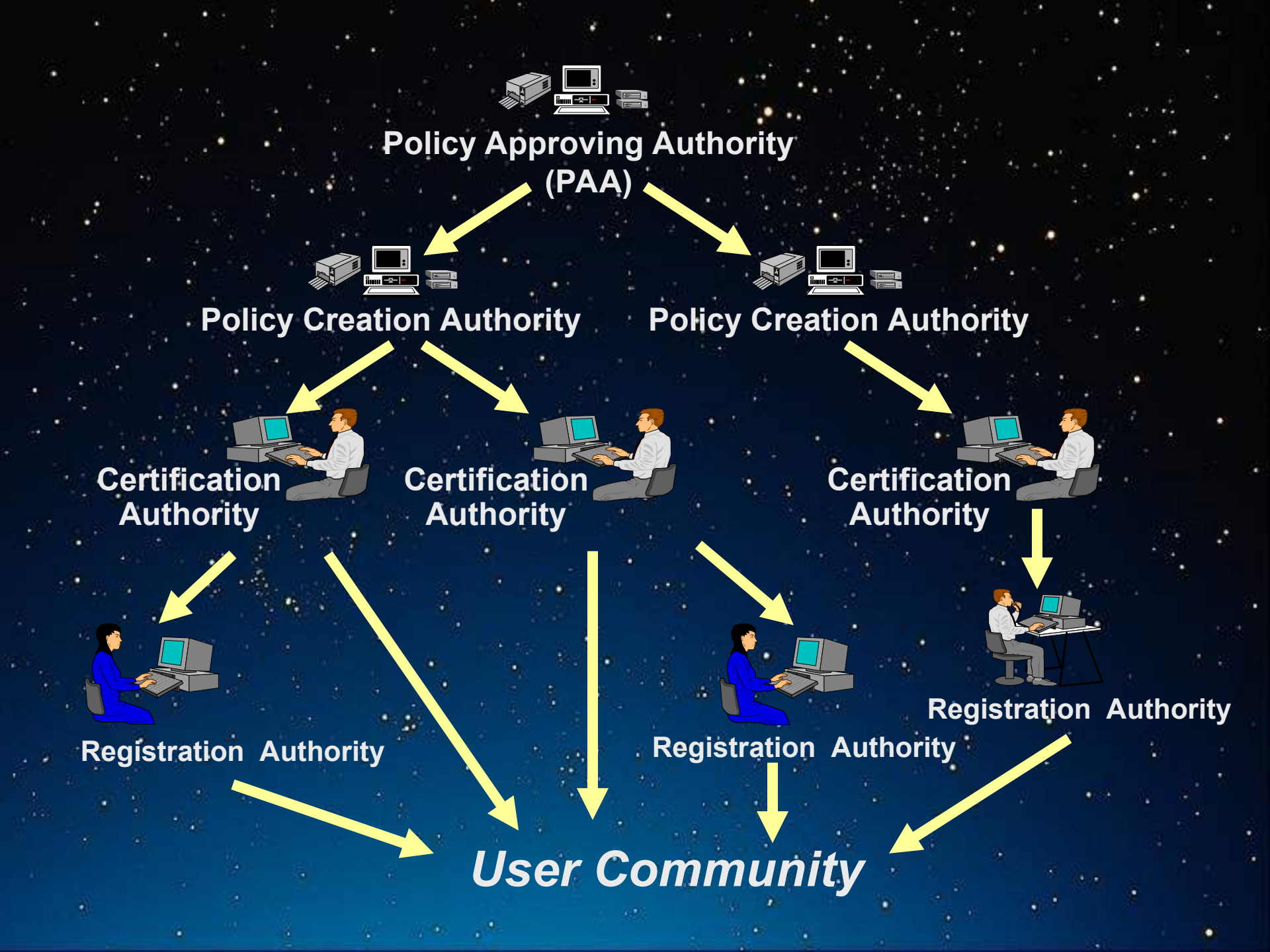
Petrina Gillman
(410)854-4527
plgillm@radium.ncsc.mil

Operational Requirements

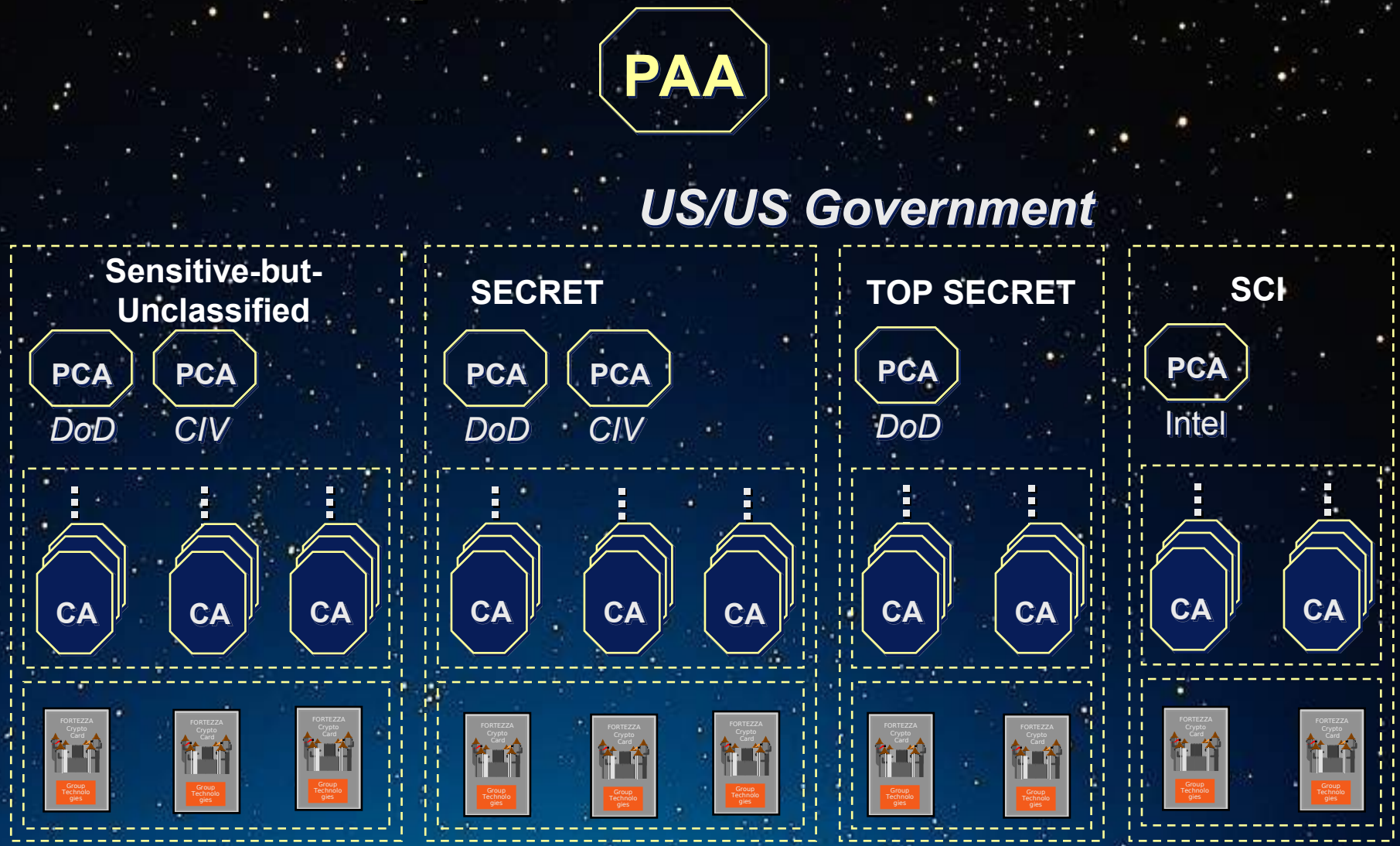
- Provide high assurance security
- Scaleable to 2 million users
- Immediate PKI service
- Flexible & deployable

Selected Technology - 1995

- V1 Jumbo x.509 certificate
- Certification Authority Workstation
- Fortezza hardware tokens


Policy Approving Authority
(PAA)
Policy Creation Authority
Policy Creation Authority
Certification
Authority
Certification
Authority
Certification
Authority
Registration Authority
Registration Authority
Registration Authority
User Community

Operational PKI



What security should a PKI provide?

The primary purpose is to establish TRUST

- I am who I say I am
- I hold the private key that corresponds to the public key in my certificate
- I am allowed to be a part of the community

Public Key Infrastructure Operations

- Trusted Registration & Establishment Process
- Privilege Management
- Ordering
- Key and Certificate Generation
- Distribution
- Certificate Repository/Directory
- Rekey, Renew and Update

Public Key Infrastructure Operations

- Accounting/Tracking
- Compromise Management & Recovery
- Revocation
- Audit
- Archive
- Data Recovery
- Disaster Recovery
- Customer Support/Technical Assistance

Operational Challenges

PKI Operations must be trustworthy

- **Distributed Operations**
- **Trusted Registration & Establishment**
  - **CA establishment**
  - **User registration**
- **Privilege Management**
- **Compromise Management & Certificate Revocation**

Operational Challenges

- Audit
- Archive
- Cross Certification
- Disaster Recovery
- Technical Assistance

Trusted Distributed PKI Operations

- **Challenge:** Secure and trustworthy certificate management operations across a distributed infrastructure of over 700 Certification Authorities

- **Solutions:**
  - Mandatory Initial and Upgrade Training
  - Comprehensive operational documentation and procedures

Certificate Management Operational Policy

- Security Policy/Certification Practice Statement
- Infrastructure Concept of Operations
- Certification Authority Establishment Guide
- Certification Authority Procedural Handbook

Trusted CA Establishment Process

- **Challenge:** Trusted process for enrolling new Certification Authorities

- **Solution:** Implemented process requiring an accountable third party to authorize the request

Privilege Management

- **Challenge:** Provide Certification Authority with appropriate privileges
- **Solution:** Establish policy setting minimums for security critical privileges. Allow local specification of other privileges with third party approval.
- **Technical Mechanism:** The Root CA establishes privileges of the subordinate CA by generating and digitally signing a configuration file

User Registration Process

- **Challenge:** Establish a process which promotes and supports the PKI security goals
- **HARD PROBLEM:** Direct trade-off between security and operational flexibility/ease-of-use
- **Decision:** Security requires in-person verification through contact with Certification Authority/ Registration Authority

Compromise Management & Certificate Revocation

- Effective mechanisms for removing users from the infrastructure

- Two lists
  - Certificate revocation list
  - Compromised Key List

Lessons Learned
Compromise Management & Certificate Revocation

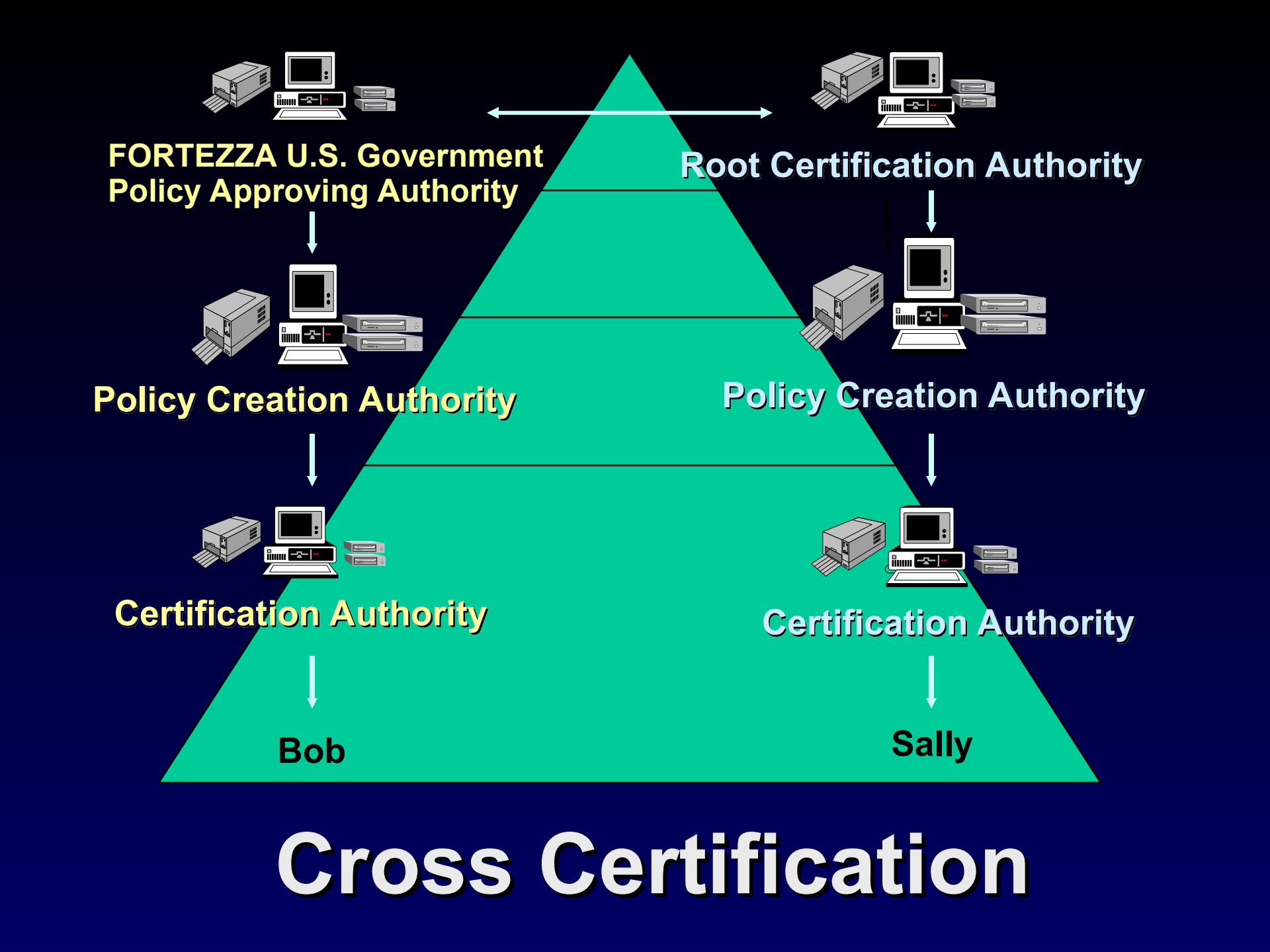
- Push Distribution by PKI to users is hard
- Pulling by users is unlikely
- Near-term solutions: Servers (web and directory), Self-subscribing mail lists, direct mail
- *Significant technical and operational challenge*

Audit

- *Challenge: Ensure only authorized individuals performing authorized actions.*
- *Solutions:*
  - *ISSO audit of CA with audit tool*
  - *Root CA audit of subordinate CAs*
- *Goals:*
  - *User friendly audit processing tool*
  - *On-line audit system for PKI*

Archive

- **Challenge:** Long-term archival storage of certificate management information
- **Interim Solution:** Weekly storage of complete system backups and signed archive utility data
- **Goal:** Legal system and technologist partnership to devise permanent solution



Cross Certification

Disaster Recovery

- **Challenge:** Rebuild infrastructure components and operations in case of site disaster.

- **Solutions:**
  - Dedicated back-up site for Root CA levels of hierarchy
  - Off-site storage of CA system backup

Customer Support/Technical Assistance Center

- **Challenge:** Provide end users and certification authorities with technical assistance

  - 24/7 Telephone support
  - E-mail Support
  - Web site documentation and forms
  - Fax-back support via Enterprise Communication Server
  - Fed Ex or U.S. Postal Service

Lessons Learned

- Need a complete solution
- Limit the number of CAs
- Mandatory user education
- Large scale, timely dissemination of compromise management and certificate revocation is difficult

Lessons Learned

- Meaningful Audit Analysis is tough
- Archive Requirements must be defined
- Cross Certification Operational Feasibility Unclear
- Need to plan and fund Disaster Recovery
- Need to plan and fund Technical Assistance

What's next in 2000

- Transition PKI to new certificate policy and practice statement
- New software support for Version 3 Certificates and V2 CRLs
- Enhanced access controls
- Implement Indirect Certificate Revocation List Authority

Questions?

RSA Conference 2000

San Jose McEnery Convention Center

JANUARY 16-20, 2000