

# Secure Communications & Federal Bridge

Russell Davis

FDIC

September 16, 2003

# 2003 Objectives

- Deployment of the Extranet Certificate Server
- Upgrade of the Intranet PKI to Entrust version 6.0
- Start paper process for Federal Bridge Cross-Certification at the low assurance level
- Certificate support for Financial & Banking Information Infrastructure Committee (FBIIC) secure email
- State Bank Supervisor certificate issuance
- Secure Sockets Layer (SSL) Extranet certificate issuance
- Merge Directories

# Federal Bridge CA

- Deploy Border Directory (Completed)
- Complete Certification Practices Statement (Version 1.1 completed)
- OIG audit of CPS to Certificate Policy (CP) (Ongoing)
- Accreditation
- Application for Cross-Certification (September – October)

## Where We Are Today (September 2003)

- Approximately 300 Directory Entries
- 239 Issued
- 150 requested and/or issued to the States

Since June 2003

# Clients Supported

- Microsoft Outlook
- Novel Group wise
- IBM Lotus Notes
- Web Browsers

# Points of Contact

- [MBenardo@fdic.gov](mailto:MBenardo@fdic.gov) E-Banking Users
- [PatNovack@fdic.gov](mailto:PatNovack@fdic.gov) State Banking Agencies
- [KKrichbaum@fdic.gov](mailto:KKrichbaum@fdic.gov) FBIIC (Financial & Banking Information Infrastructure Committee)

# Federal Bridge Operational Authority Report (September 9, 2003)

- Completed Testing: Department of Treasury, NASA, USDA/NFC, DOD & DOD KMI
- Current: DOD End Entity & Government of Canada
- Future: Department of Labor, State of Illinois, Department of Energy & Department of State
- To get on the Future list, an application must be submitted

# Extranet CA

- Used to generate Web and secure email certificates
- Located in the Virginia Square server room





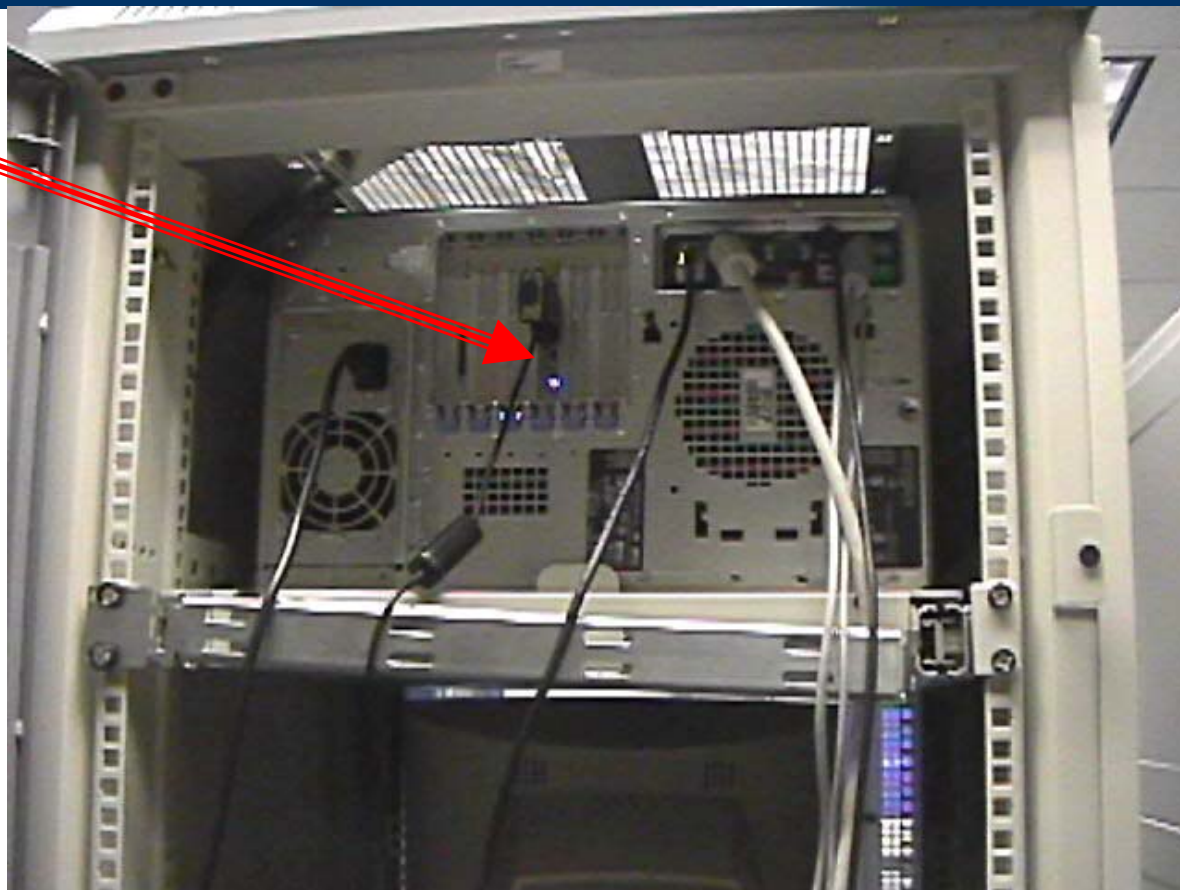
# X.500 Directory

- Full X.500 Directory
- Operates on a Sun V480 computer



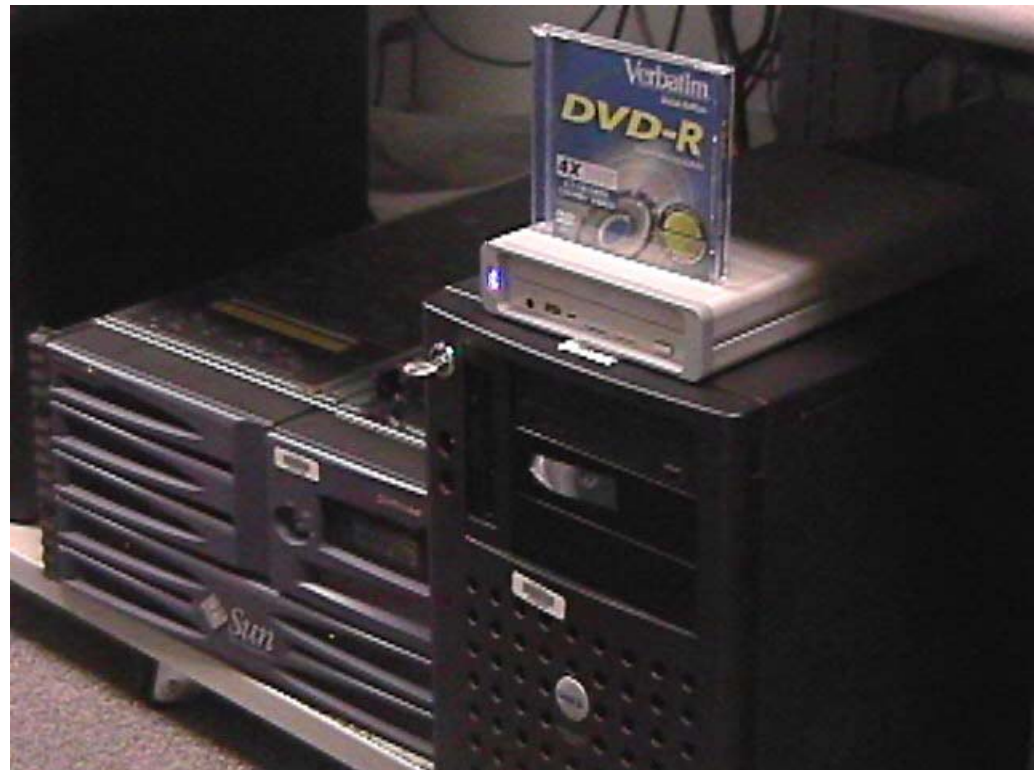
# Back of the Rack

Crypto  
Card



# DVD Burner

- Files archived directly to the DVD
- DVD USB connected to the CA
- NARA Retention 10 years & 6 months





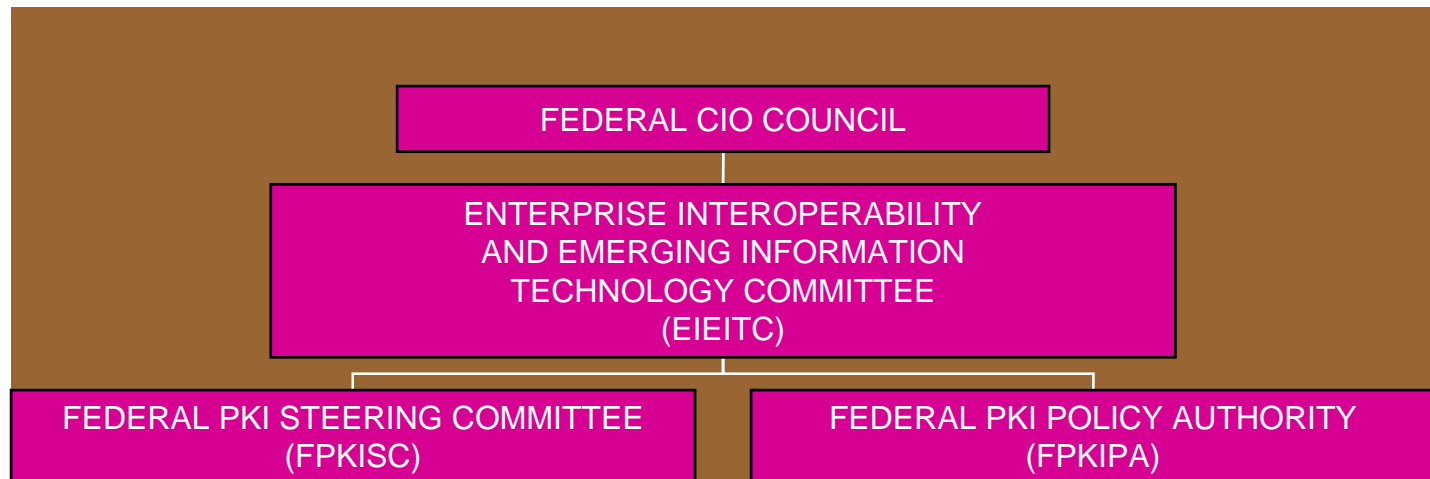
## Federal Public Key Infrastructure Policy Authority

- Application for Cross Certification with the Federal Bridge Certification Authority
- Memorandum of Agreement (MOA)
- Letter of Authorization to Cross-Certify the United States Department of [Bureau] with the Production FBCA



# Federal Public Key Infrastructure Steering Committee

## Organization



# Agency Requirements For Interoperation

- Must Have Operational/Planned PKI With Certification Authority
- Must Have CP, CPS, And Directory Structure Description
- Must Map CP Assurance Levels To FBCA CP Levels

# Agency Requirements For Interoperation (Cont.)

- Perform Independent PKI Audit
- Enter Into Moa With Federal PKIPA

# Apply For Interoperation

- Complete Application And Submit To FPKIPA For Review
- FPKISC Afforded Opportunity To View
- Majority Vote Needed For Approval
- If Accepted, FPKIPA Enters Into MOA With Agency



# Memorandum Of Agreement

- Responsibilities Of FPKIPA And Agency
- How Main Fields/Extensions Of FBCA Certificates Will Be Populated
- How Principal Certification Authority Cross-certs To FBCA Will Be Populated
- How Agency Interoperates Its Directory(s) With FPKI Bridge

# Looking Back to 1988

## *Exploring Computer Viruses 4<sup>th</sup> ACSAC*

- *“Knowledge of the software itself offers opportunity for exploitation if a known weakness exists.”*
- *“A program written in Pascal or Ada, which create large executable files, could be replaced by one written in C or assembly...”*
- The year the Robert T. Morris Worm shut down the Internet (October 1988)

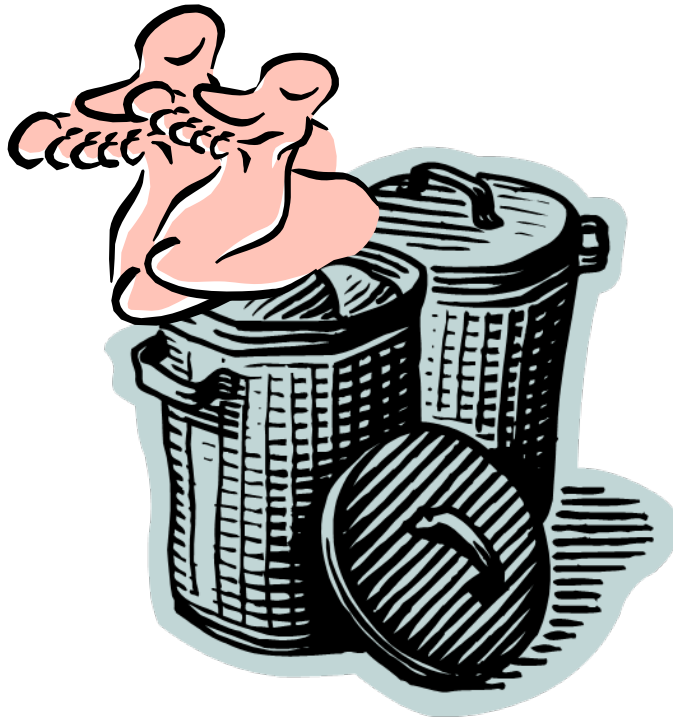
# Observations

- 1988 - More of a curiosity rather than a legitimate threat
- Currently Viruses have followed original predictions and are now considered a significant threat

# Identity Theft

- American Victims
  - 27.3 Million (last 5 years)
  - 9.9 Million (last year)
- Cost
  - \$46 Billion (Financial Institutions)
  - \$5 Billion (Individuals)

# There is the Dumpster Diver

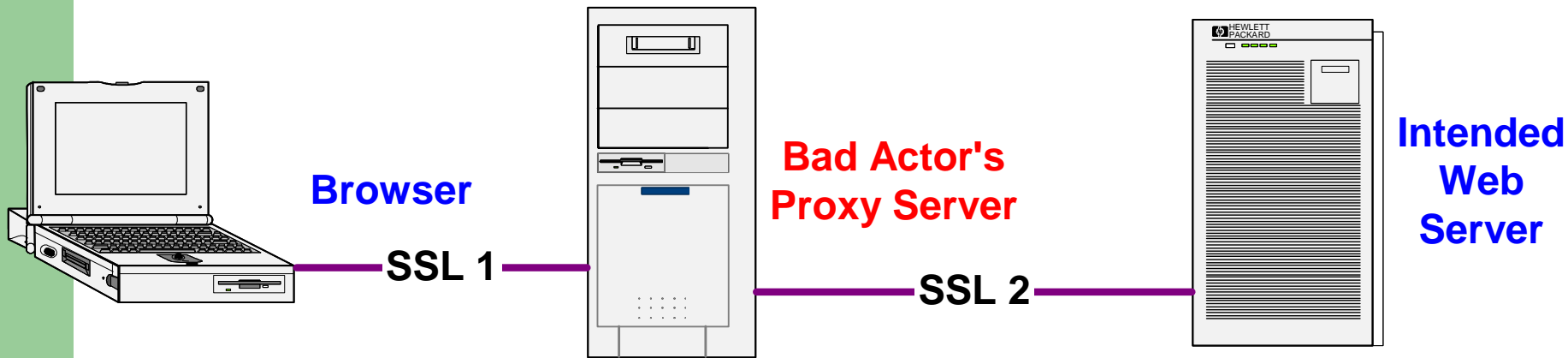


- But what about online Attacks
- Server attacks
- Man-in-the middle attacks

# Predictions

- Man in the middle attacks will be recognized as a significant threat
- Congress will mandate more control and oversight
- We will have more work to do

# Man in the Middle Attacks



With client side certificates, the SSL 2 connection cannot be established.

# Why PKI

- Enable commercial off-the-shelf security features
  - Mitigates Man-in-the-middle Attacks
  - Secure email outside the FDIC
  - Secure Web technologies
- Support customer base
- Comply with Statutory drivers
  - GPEA
  - e-Sign
  - e-Government
  - Interoperability



# Questions

Russell Davis  
(703) 516-5107  
[RDavis@FDIC.Gov](mailto:RDavis@FDIC.Gov)  
[RJDavis@FCC.Net](mailto:RJDavis@FCC.Net) (Using S/MIME)