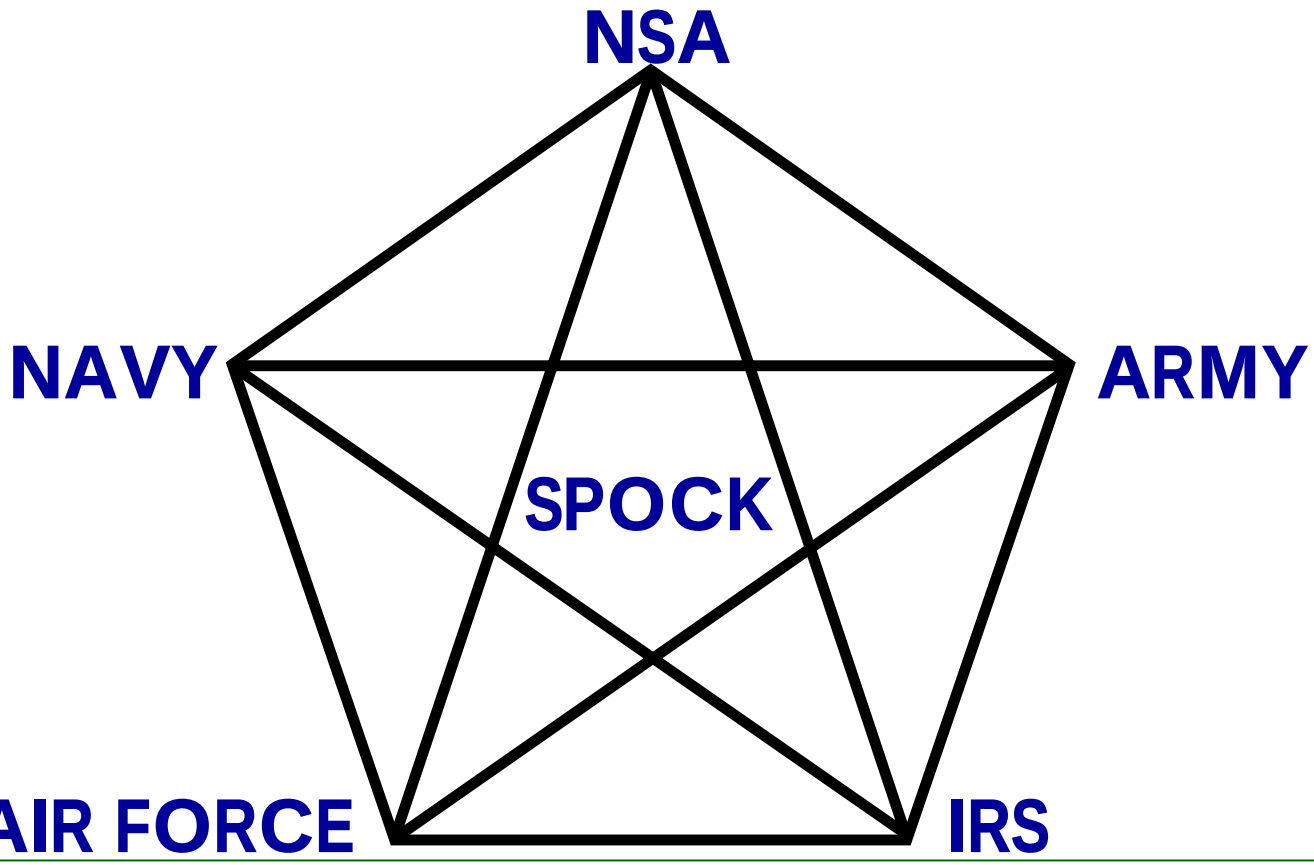
SPOCK Demonstration of Entrust PKI



MAJ Michael W. Davis, 410-859-6318
mdavis@gibraltar.ncsc.mil

AGENDA

- What's the SPOCK Program
- Past Accomplishments
- Who's in SPOCK
- What does the SPOCK team do
- Demonstration Process
- SPOCK PKI Architecture
- PKI Claims and Results
- Lessons Learned
- Return on Investment
- Summary

What's SPOCK ?

"A Consortium of Product Developers and Government System Integrators interested in exploring INFOSEC *commercial* solutions and Enabling Technologies"

PAST ACCOMPLISHMENTS

1995-1998

- 32 Consortium Meetings - Over 1500 Attendees
- 96 Emerging Topic Areas Briefed
- 8 Diverse Solutions Demonstrated
- Established Zones of Cooperation
  - Over 40 Government System Integration Communities
  - Over 100 Solution Developers
- Input for the President's Quality Award
- Nominated for SECDEF's Team Excellence Award

Who's in SPOCK

- **Army - BCBL-G, LIWA, DISC4**
- **Navy - SPAWAR, NAVSEA, NIA FIWC, NIWA, NRL**
- **Air Force - AFIWC, 609 IWS, AFOSI CPSG**
- **Joint - J6, DISA**
- **Non DoD - NASA, DoJ**
- **NSA - V, Y, X, C**

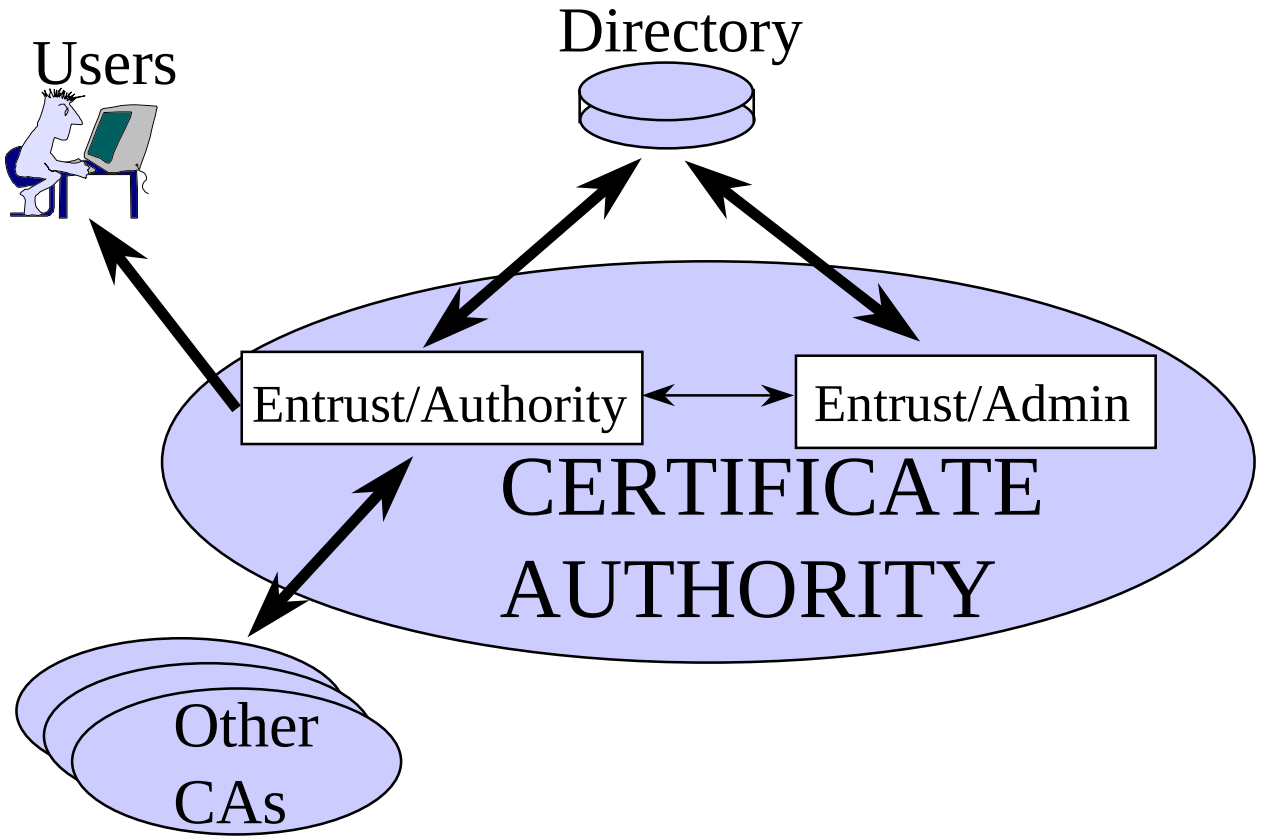
What's the SPOCK Team do ?

- **Attend monthly briefings on Warfighter Architectures and Solutions**
- **Demonstrate Security Claims in Warfighter Architectures**
- **Write SPOCK Demonstration Reports**
- **Develop Draft Security Targets and Protection Profiles**

DEMONSTRATION PROCESS

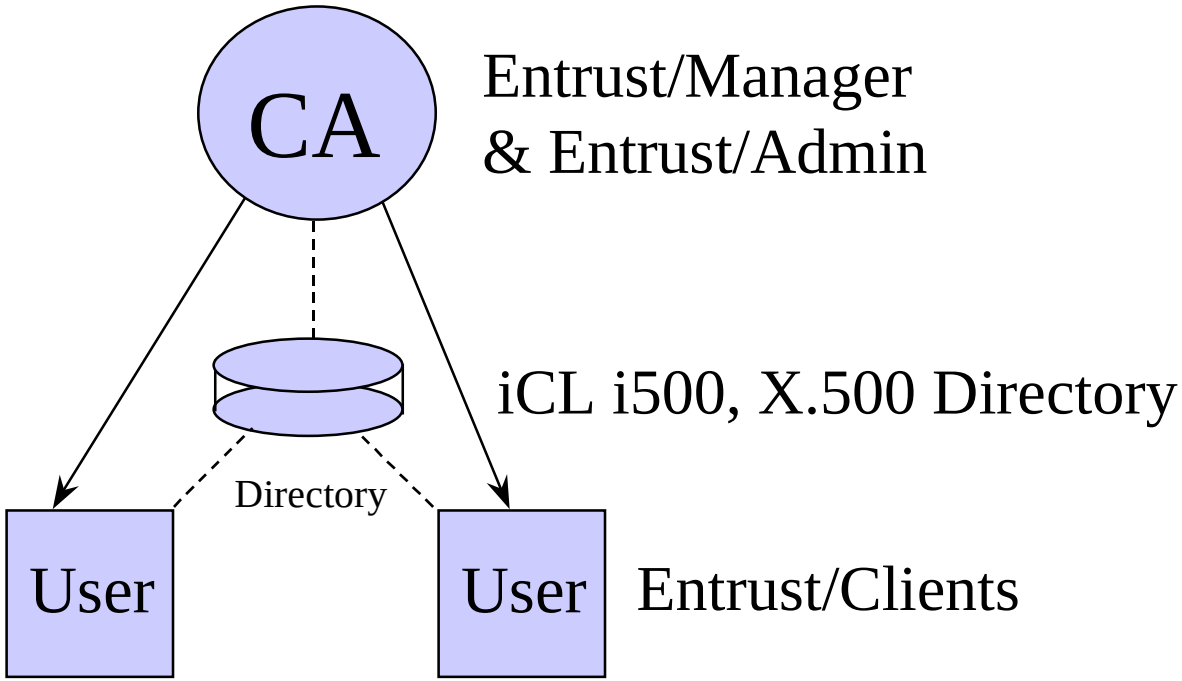
1. **Solution/Developer Identified.**
2. **Developer briefs the Solution during meeting.**
3. **Developer presents Security Claims, Architecture, and Equipment Requirements.**
4. **SPOCK prepares Scripts to demonstrate Claims.**
5. **SPOCK demonstrates Security Claims in Government Architectures.**
6. **SPOCK writes the Demonstration Report, signed by Chief, NSA V2.**

ENTRUST CA ARCHITECTURE



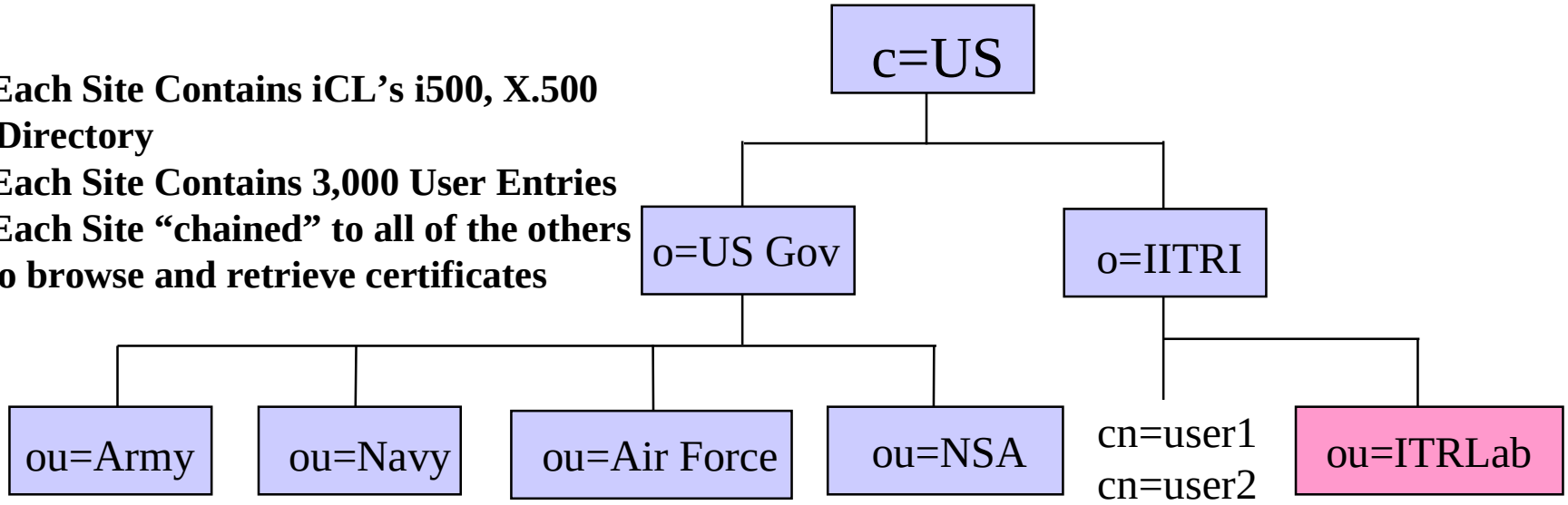
MAJ Michael W. Davis, 410-859-6318
mdavis@gibraltar.ncsc.mil

SPOCK PKI COMPONENTS



SPOCK PKI Directory Schema

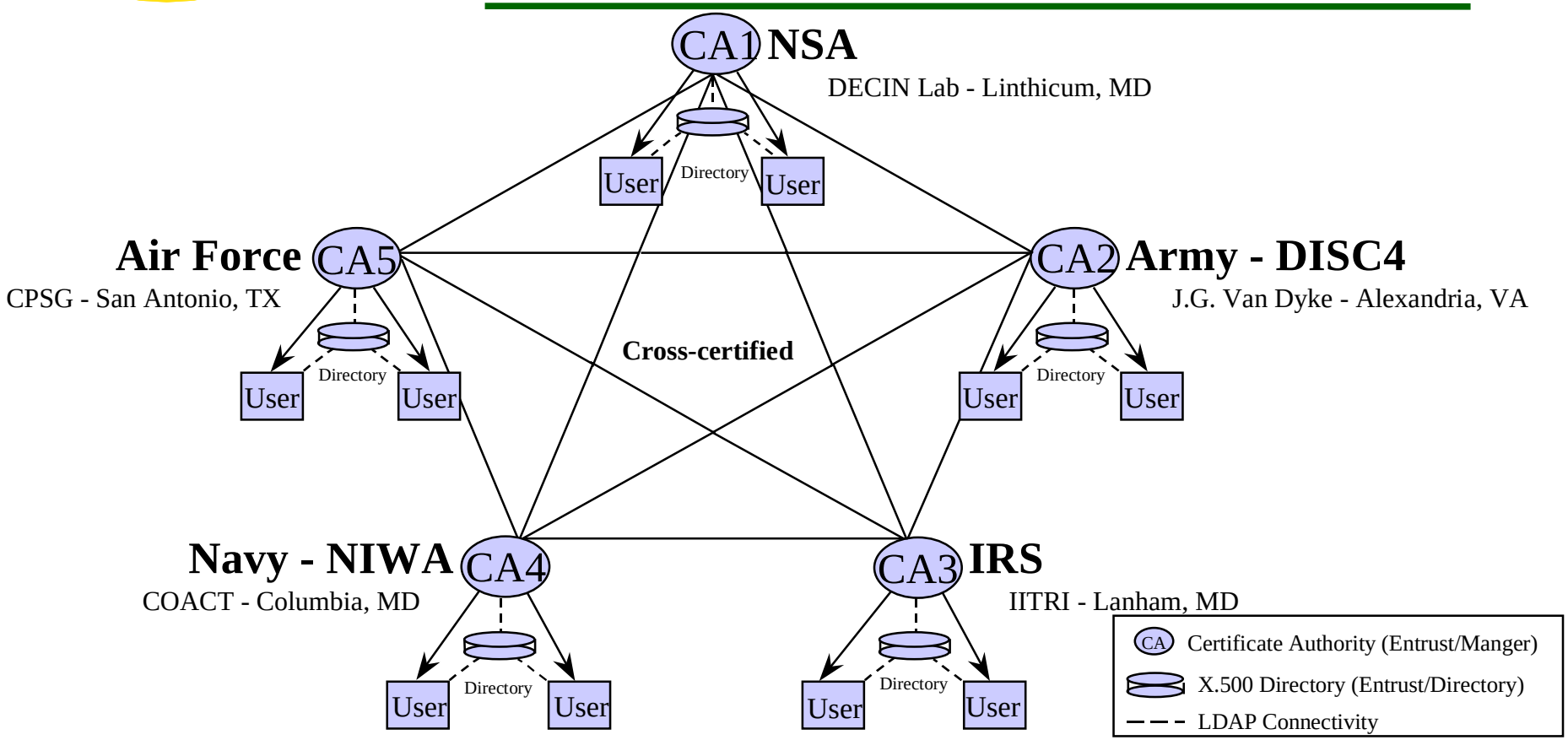
- **Each Site Contains iCL's i500, X.500 Directory**
- **Each Site Contains 3,000 User Entries**
- **Each Site "chained" to all of the others to browse and retrieve certificates**



KEY
c=country
o=organization
ou=organizational unit
cn=common name

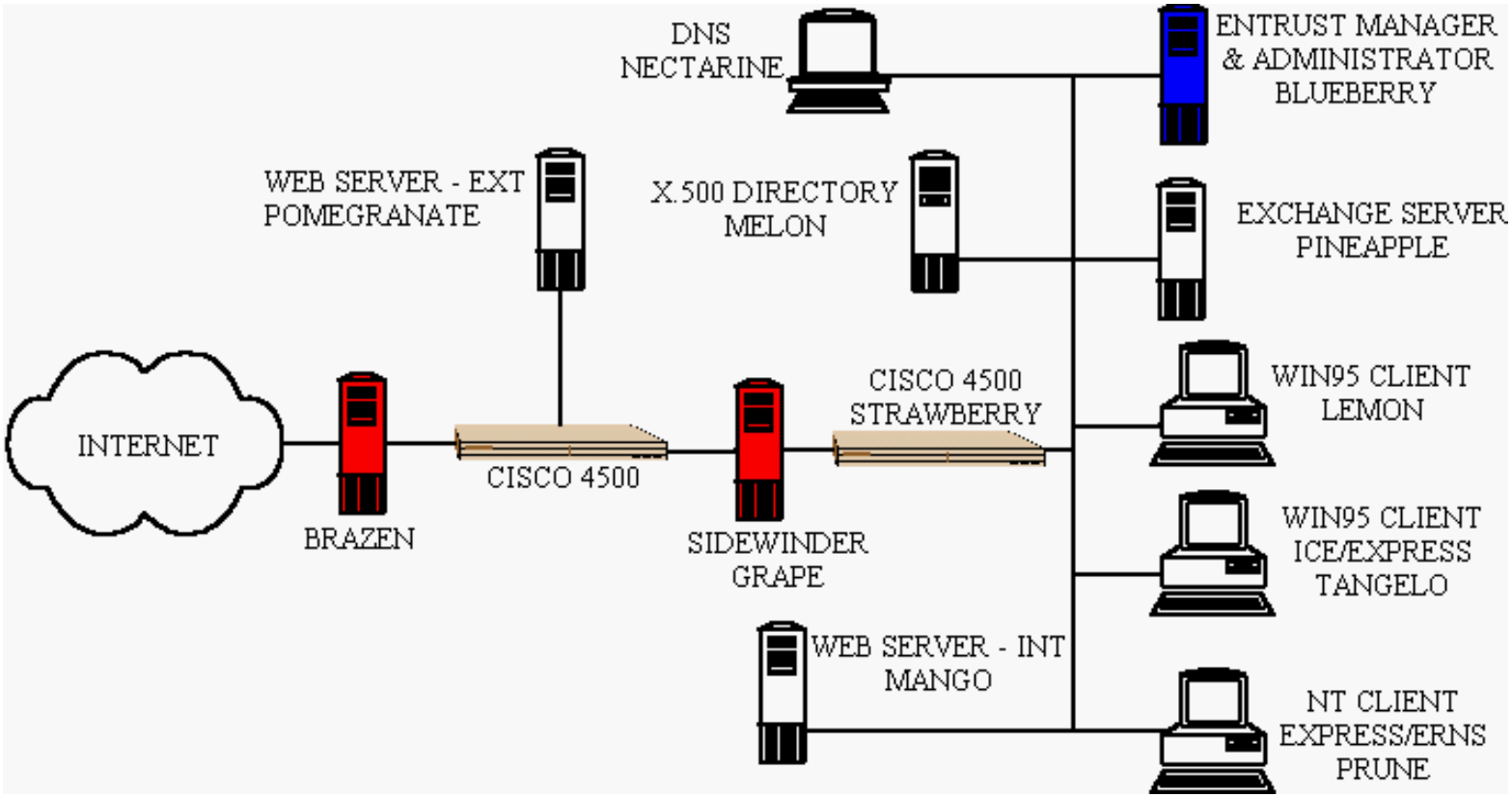
MAJ Michael W. Davis, 410-859-6318
mdavis@gibraltar.ncsc.mil

SPOCK PKI ARCHITECTURE



MAJ Michael W. Davis, 410-859-6318
mdavis@gibraltar.ncsc.mil

DECIN Lab ARCHITECTURE



ENTRUST PKI CLAIMS

1.1 Key Management Transparency

1.2 Secure Key Recovery

1.3 Auto Key Update

1.4 Client Key Initialization

1.5 Certificate Revocation

1.6 Support Cross-certification

1.7 Entrust Scalability

1.8 Hardware Tokens Option

1.9 Support Multiple Algorithms

1.10 Support Multiple Applications

Key Management Transparency

Claim: Users should be able to use security product without understanding cryptography or key management

Method: E-Mail - Signed and Encrypted E/Express
Desktop File Encryption E/ICE

Result:
1. Claim verified. The management of keys is transparent to users.
2. Searching the Directory, is NOT transparent.

Secure Backup & Key Recovery

Claim: Entrust provides the ability to recover keys in cases where a valid user has forgotten their password or an employee has left the company

Method: There are three general cases for “key recovery”. Send Authentication Code, Reference Number “out of band” to authorized individual.

Result:

1. Claim verified. Recovered files and email.
2. Entrust Key Recovery solution is best suited for Authorized user that has forgotten their password.

Automatic Key Update

Claim: Certificates are updated without user involvement.

Method: Set Encryption and Verification period to 2 months
Set Signing Private to 10 percent.

Result: 1. Claim verified. User informed by message box.
2. If renewal period is missed, key recovery is required.

Client Key Initialization

Claim:	Clients are initialized using a secure “pipe”. Clients can be set up remotely over a network.
Method:	Run installation program over the network. Requires: Authentication Code, Reference Number and access to install program and entrust.ini file.
Result:	SEP was not verified. Claim verified. Remote install in 20 minutes.

Certificate Revocation

Claim: Entrust provides the ability to revoke certificates.

Method: Revoke user. Attempt to send and receive email. Attempt to access web server. Attempt to use ICE.

Result:
1. Claim verified after modifications.
2. Express does not verify certificate prior to sending.

Support Cross-Certification

Claim:	Certificate Authorities are able to cross-certify.
Method:	Establish Search base by “chaining” directories Use Entrust Managers to Cross Certify Send encrypted mail/files to another domain.
Result:	1. Claim verified. 2. Problems searching the Directory

Scalability

Claim: Quickly add 3,000 users within each domain.

Method: "Bulk Load" using a disk loaded with 3,000 names and serial numbers. Real users were loaded individually.

Result: Claim verified.

Hardware Tokens Biometrics

Claim: Support Tokens for storing profiles and Biometrics for authentication of users.

Method: Use DateKey smart card to store user's profile. Use Biometrics device instead of a password to authenticate users

Result: Hardware Token claim verified. Biometrics device vendor could not provide correct drivers.

Multiple Algorithms

Claim:	Entrust supports multiple algorithms for hashing encryption and digital signature.
Method:	Use Entrust Manager to select hashing and digital signature algorithms. Use Entrust Client and Applications to select different encryption algorithms. Send email and files to other users.
Result:	1. Claim verified within the abilities of the SPOCK Team.

Single Password Many Applications

Claim:	Entrust uses the single password for a user's certificate to logon to secure applications.
Method:	Start Client, enter password. Start ICE, enter same password. Start Express, enter same password. Start Entrust-Ready Netscape, enter same password.
Result:	Claim verified. Automatic logoff time is set for each application.

LESSONS LEARNED

- The significance of the X.500 Directory.
- "Open" Security Policy.
- Key Recovery.
- Significant Firewall configuration issues.

RETURN ON INVESTMENT

- **SYSTEM INTEGRATOR**
  - Quick look at emerging technology
  - Solution strengths and weaknesses are demonstrated in *THEIR* warfighter configurations
- **GOVERNMENT**
  - Learn about and influence emerging solutions
  - Insight into future architectures (requirements)
- **INDUSTRY**
  - Better understands Warfighter's needs
  - Rapid exposure of solution in Warfighter Architecture

SUMMARY

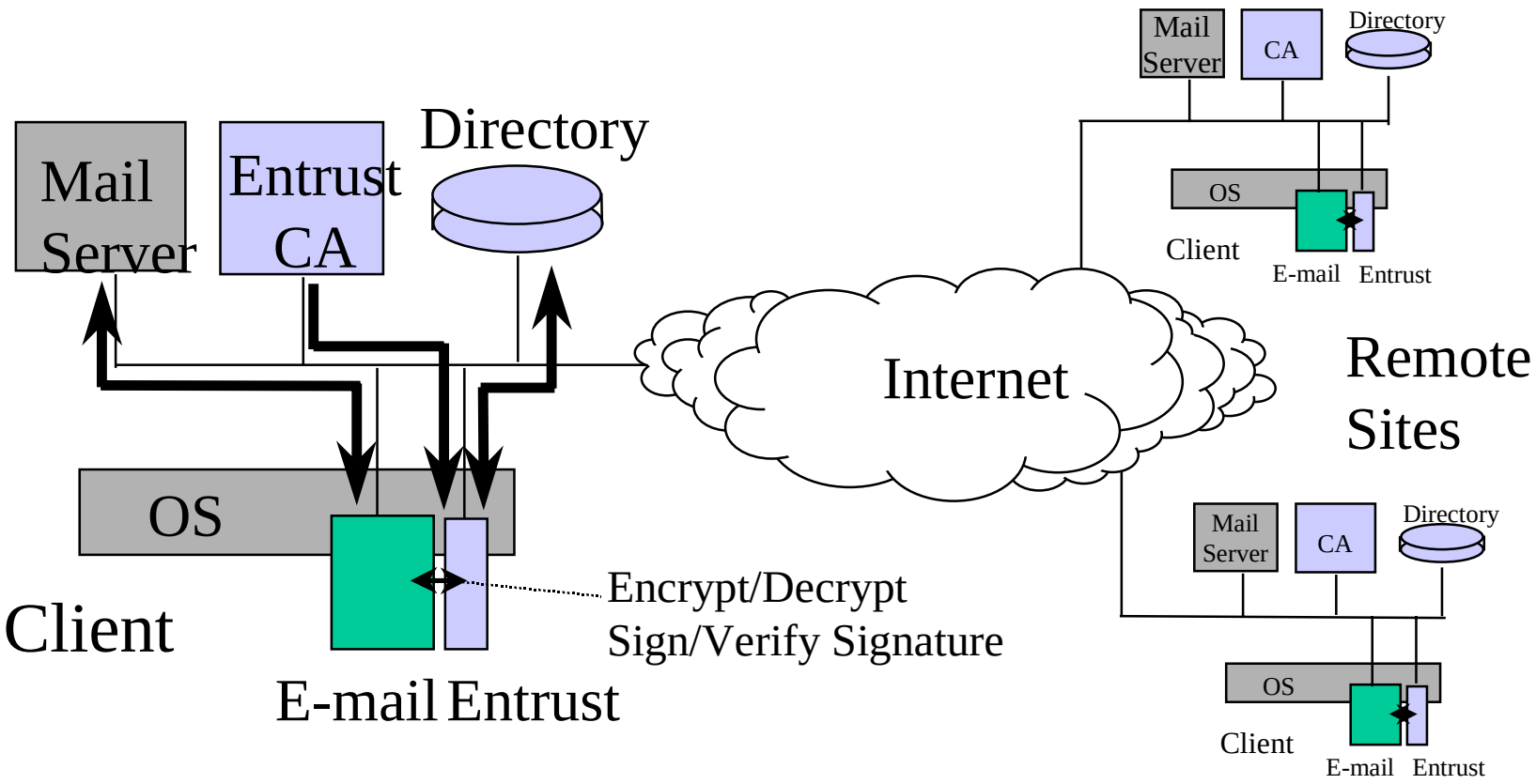
- **SPOCK focuses on commercial INFOSEC solutions and emerging technologies**
- **SPOCK demonstrates security in legacy and contemporary architectures**
- **SPOCK "teams" to demonstrate security in operational architectures**
- **SPOCK supports development of Protection Profiles and Security Targets**

QUESTIONS & COMMENTS

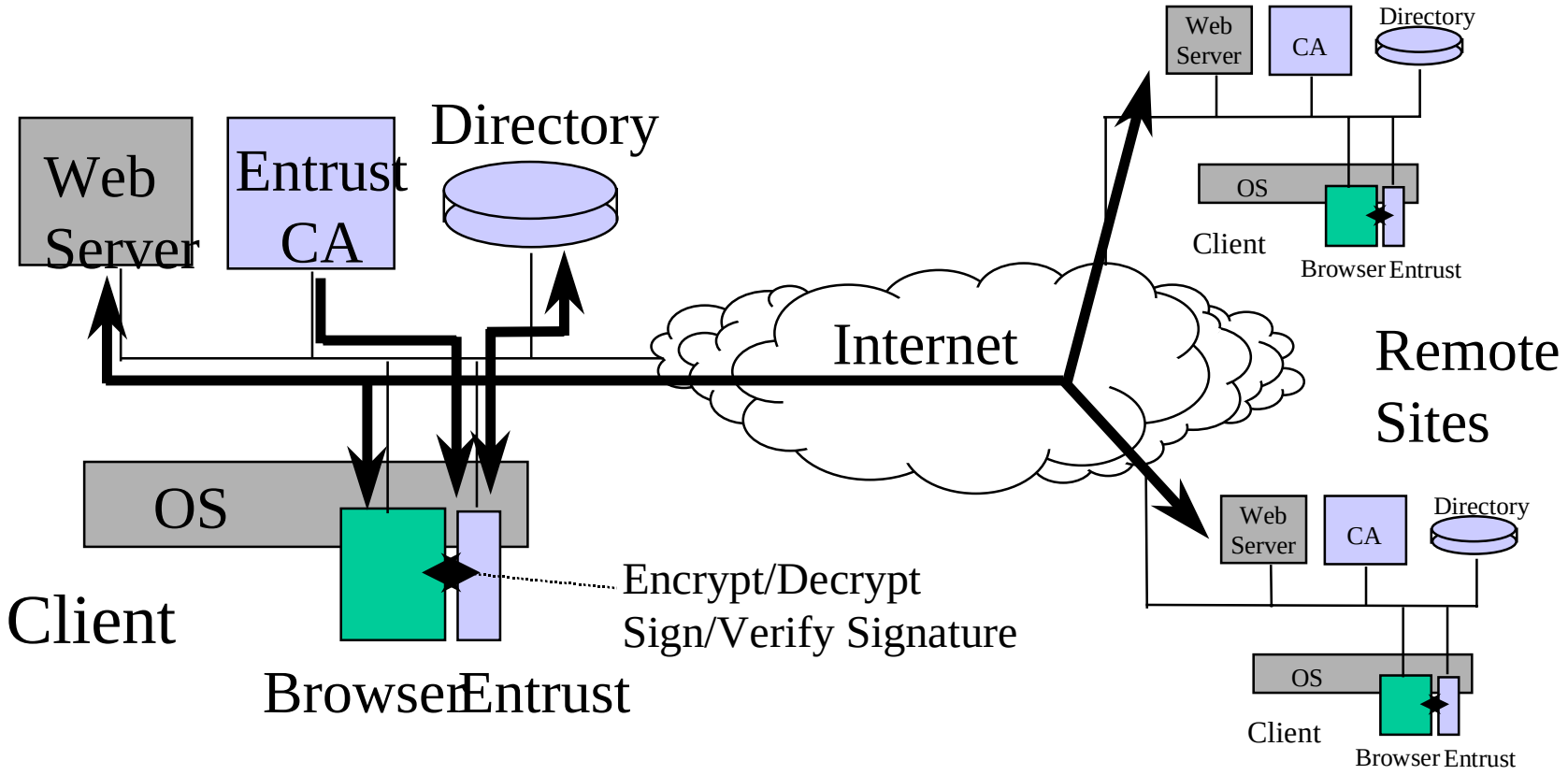
SPOCK CONTACTS

- **SPOCK Chairman**
  Louis Giles, Chief V2
  (410) 859-6281
- **SPOCK Program Manager**
  Terry Losonsky **terryus@aol.com**
  (410) 859-6318 **FAX: (410) 859-6897**
- **SPOCK Deputy Program Manager**
  MAJ Michael Davis **mdavis@gibraltar.ncsc.mil**
  (410) 859-6318 **FAX: (410) 859-6897**
  http://spock.v.nsa:12080/
- **SPOCK Contract Support**
  Larry McGinness **spock@coact.com**
  (301) 498-0150 **FAX: (301) 498-0855**
  www.coact.com/spock.html

SECURE E-MAIL



SECURE WEB BROWZER



MAJ Michael W. Davis, 410-859-6318
mdavis@gibraltar.ncsc.mil