

PKI in Large Scale Environments

A Look at DMS



George Hoover
Jayne Schaefer
PKI/KMI
(480) 441-0898
jayne.schaefer@motorola.com

Information Assurance: Voice, Data, Network, PKI



How Great is the Threat?

2000 CSI/FBI Computer Crime and Security Survey

- 90% of Survey Respondents Detected Cyber Attacks
- 70% Reported Serious Computer Security Breaches
 - Theft of Proprietary Information
 - Financial Fraud
 - System Penetration From Outsiders, etc.
- 74% Acknowledged Financial Losses Due to Computer Breaches
- 273 Organizations (42%) Report \$265,589,940 in Financial Losses
 - Average Annual Total Over the Last Three Years Was \$120,240,180
- Price Waterhouse Reported that U.S. Businesses Lost \$45 Billion in Thefts in 1998, the Majority Through Computer Crime

Public Key Infrastructure Considerations

- Level of Trust
- Scalability
- Manageability
- Flexibility
- Topography
- Policy
- Interoperability
- Applications
- Support
- Key Management

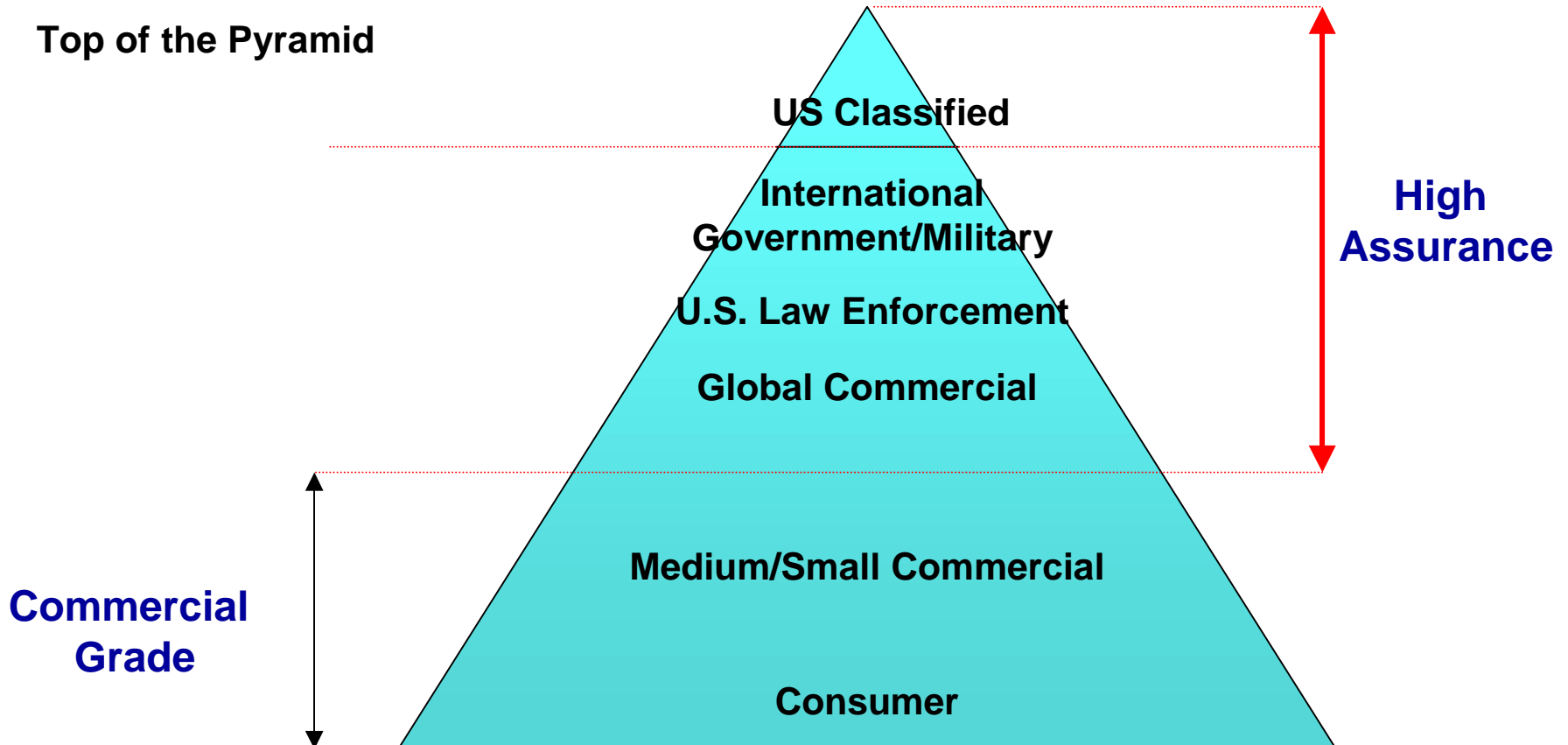
Security Level

- What is the Threat?
- From Whom?
- What is at Risk?
- What is the Potential Loss?
- How Sophisticated is the Adversary?
- How Strong is Our Existing Security?
- Platform
 - Trusted/Versus Non-Trusted Operating Systems for CA

High Assurance Security

Complete World Class Security **Architecture and Implementation**. Provides **Substantial** Protection Against a **Well Funded** and **Sophisticated** Adversary.

Top of the Pyramid



Applications and Considerations

- Commercially Available vs. Home Grown
- Multiple Applications
- Multi-Use (Computer Access, Web Access, Physical Access)
- Electronic Commerce
- Financial Services
- Corporate Data
- Healthcare
- Subscriptions
- Legal Information
- Proof of Document Transmission
- Document Archive and Retrieval
- E-Mail
- Web Access
- Digital Content Distribution
- Proof of Authorization

Sample Applications

- E-Business
 - Vendors, Suppliers, Partners
 - Procurement Process/Workflow
 - On-Line Product Access/Digital Content Distribution
 - Technical Support
 - Publications/Manuals
 - Software
- Internal Operations
 - Access Privileges
 - Financial
 - HR
 - R&D
 - Workflow

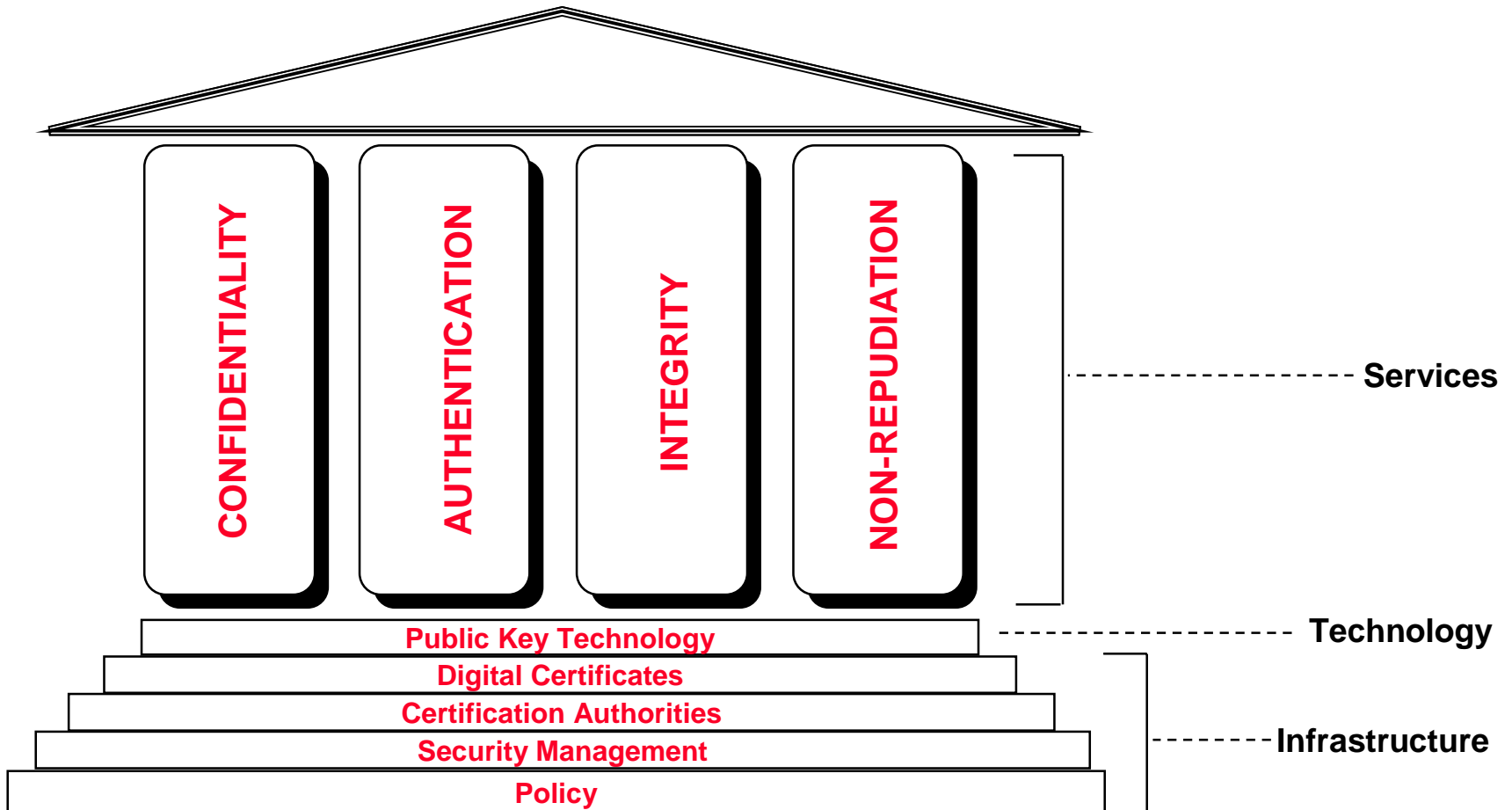
Policy

- Who Will be Issued Certificates?
- What Will They Have Access To?
- How Many Certificates Will be Issued?
- What will be the Certificate Lifetime?
- What will be the Certificate Turnover?
- Will there be Multiple Levels of Security?
- How will Users Register?
- How will Users Obtain their Certificate?
- Will there be a Need for Individual, Identity and Role Certificates?
- What Type of Token(s) Will Used?
- Will Outside Partners Require Access To/From Your Systems?
- Will Certificate Management be Outsourced or Handled In-House?

Interoperability

- Cross Certification
 - Other Certificates
 - Other Formats
- With Whom
- How Often
- Level of Trust
- What Applications
- Access Rights
- Media/Platforms
 - Wireless (Cellular, Radio, Satellite, PDF, Other RF)
 - Wireline (Phone, Fax, Desktop, Laptop)

Security is Only as Strong as the Weakest Link . . .

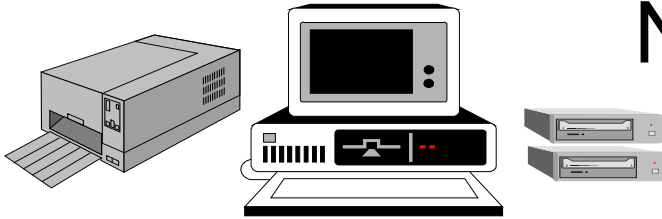


Defense Message System - Network Security Managers

- High Assurance Public Key Infrastructure (Class 4)
- Organizations and Individuals
- Utilizing A Gobble Directory
- Providing Security Services
- Management Services
- Installations
 - 251 NIPRNET (98% Complete)
 - 190 SIPRNET (94% Complete)
 - Total 441 Installations
 - 350,000 Users
 - *Largest PKI Implementation in the World !*



NSM Deliverables



Certification Authority
Workstation



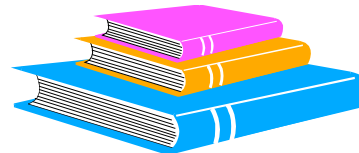
Registrar

The NSM Program develops and supports the higher assurance public key infrastructure.

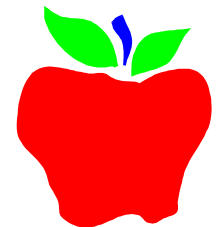
This infrastructure includes the personnel, policy, procedures, components and facilities to bind user identities to key and privilege information so that applications can provide the desired security service.



Product Support



Policy, Procedures and
Documentation

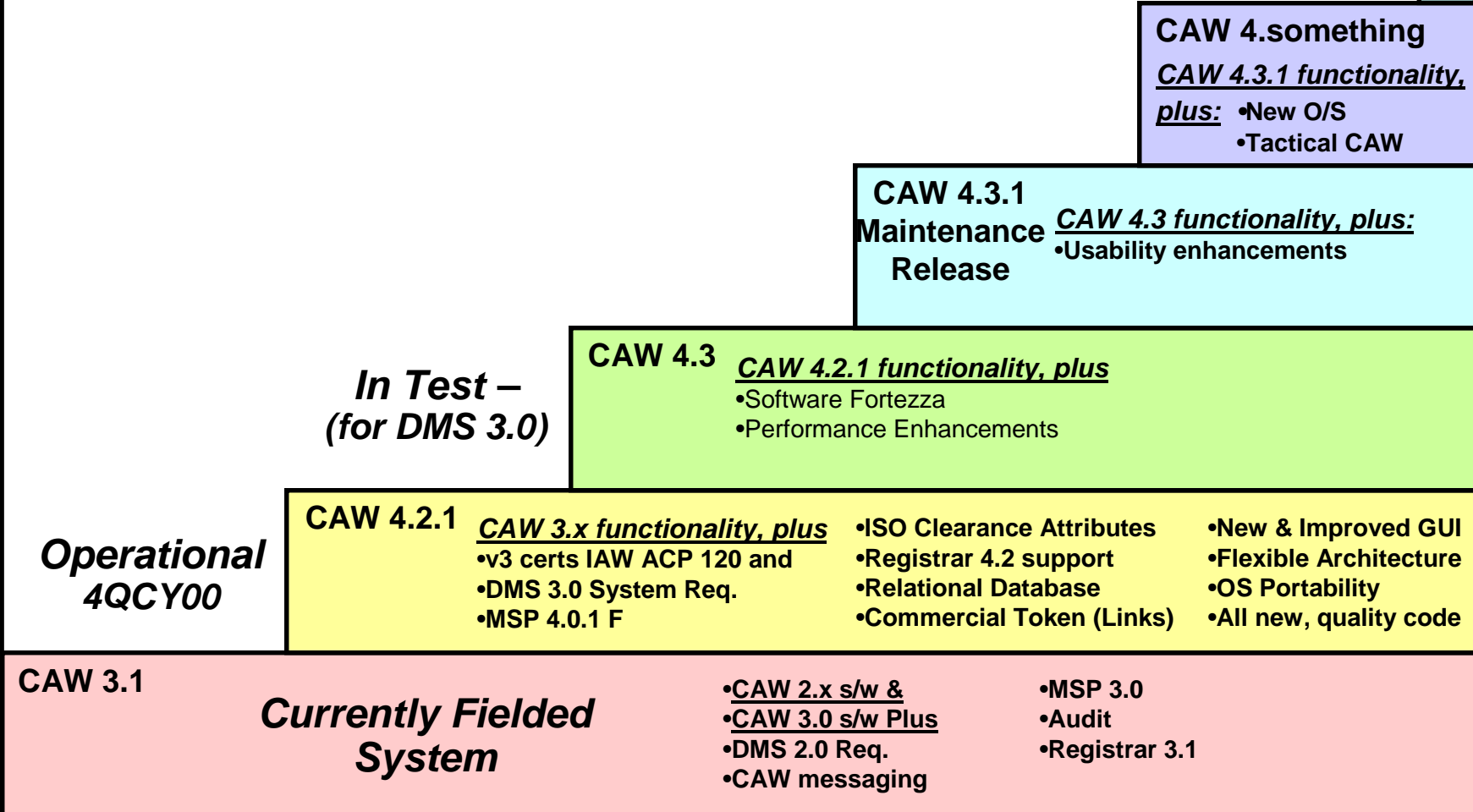


Training
Material

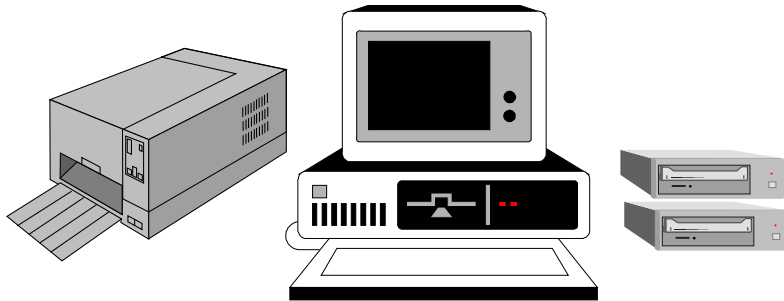
CAW History and Evolution

Increasing Functionality > DMS 2.X > DMS 3.0 > DMS 4.0 > Target Class 4 PKI

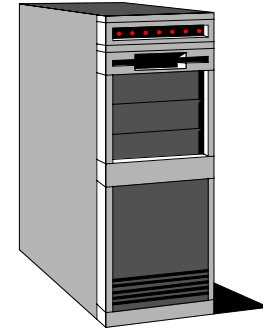
?



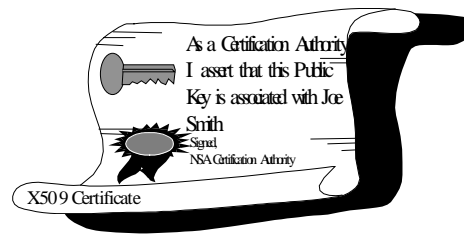
Primary Infrastructure Components



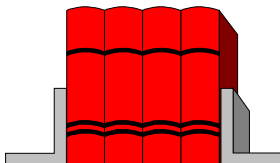
Certification Authority
Workstation



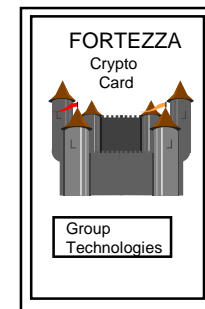
X.500 Directory
System



Certificate



Documentation



FORTEZZA
Crypto Card

CAW 4.2.1 Key Features

- TSDM-Based Development & SEI Process
- High Assurance Security Architecture
 - Software Architecture Separates Trusted & Untrusted Process
 - Software Uses Trusted OS Access Control & Roll Separation Features
 - Design Incorporated Feedback From Penetration Testing of Earlier MISSI Caws
 - Robust, Profiling & Penetration Testing by NSA
- FORTEZZA Card Supported

Capabilities

- Enables Real-time and Store-and-Forward Security Applications Using Public Key Cryptography
- Binds Subject's Public Key and Privileges to Their Identity Via Certificates
 - X.509 Signature Certificates
 - X.509 Key Management Certificates
 - Attribute Certificates
- Enables Application Security Services Including
 - Source Authentication: Verification of Identity [Signature]
 - Data Integrity: Verification of No Unauthorized Modification [Signature or Encryption]
 - Non-Repudiation: Undeniable Proof of Participation (Sender and Receiver Can Be Verified by a Third Party) [Signature]
 - Confidentiality: Data Privacy [Encryption]
 - Access Control: Authorization of Users to Access Data
 - Audit: Individual Accountability for Actions

Archive

- Store, Manage, and Preserve Electronic Records for Historical Reference
 - Maintain Integrity and Authenticity of Archived Records
 - Consolidate CMI Archives
- Enable Historical Non-Repudiation
 - Maintain Continuity of Non-repudiation Services
- Provide Means to Validate Signatures Using a Public Key Contained in an Expired Certificate
 - Provide Defense Against Claims of False Certifications
 - Provide Defense Against Claims of False Revocations

Access Control

- Identity Based Access Control (IBAC)
 - Subject Name in Certificate can be used for IBAC
- Rule Based Access Control (RBAC)
 - Based on a set of user authorizations, object sensitivities, and rules as to which user authorizations grant access to which object sensitivities
- Partition Rule Based Access Control (PRBAC)
 - Widely understood
 - Example: classification level (U, C, S, TS)
- Local Rule Based Access Control (LRBAC)
 - Limited to smaller enclave
 - Example: security categories (compartments) within an organization such as NSA or CIA
 - Existence of security category or possession of security category authorization may be classified

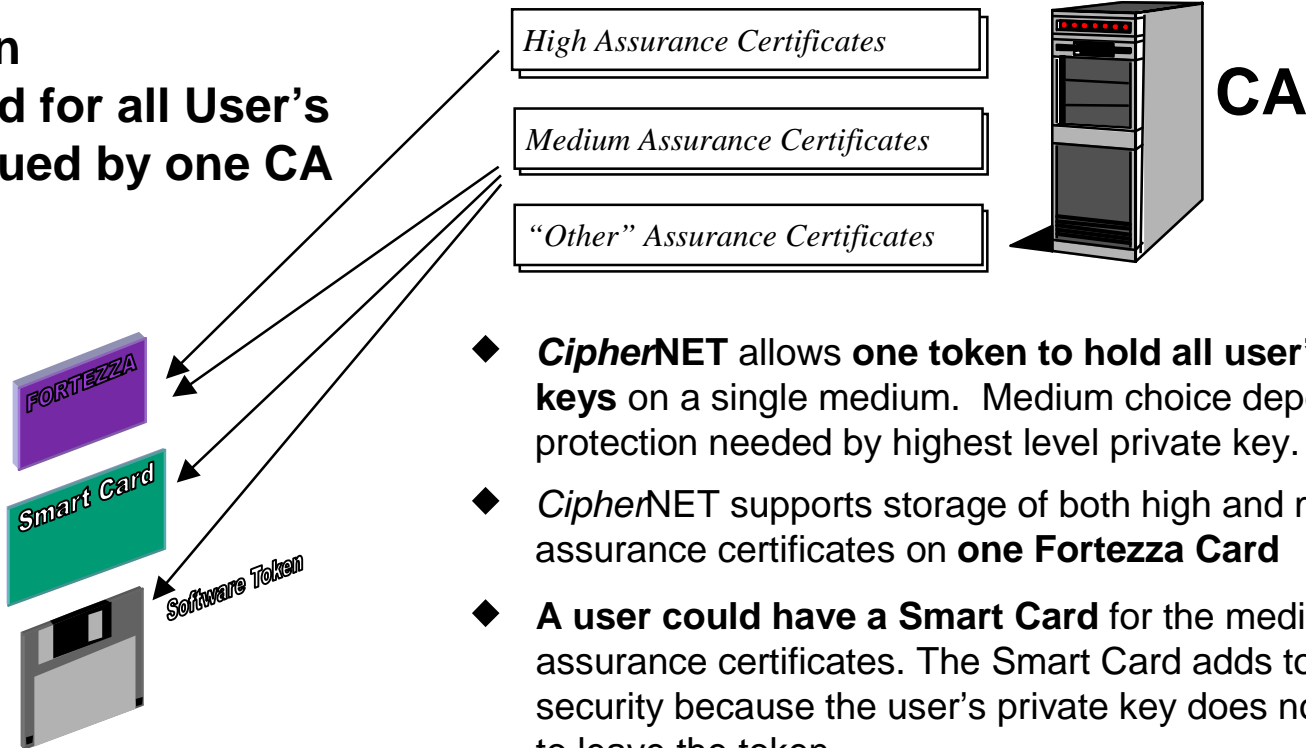
FORTEZZA PCMCIA Card

- Personal Security Token
 - Encryption/Decryption Engine
 - Digital Identity Storage
- Security Services
 - Confidentiality
 - Authentication
 - Data Integrity
 - Non-Repudiation



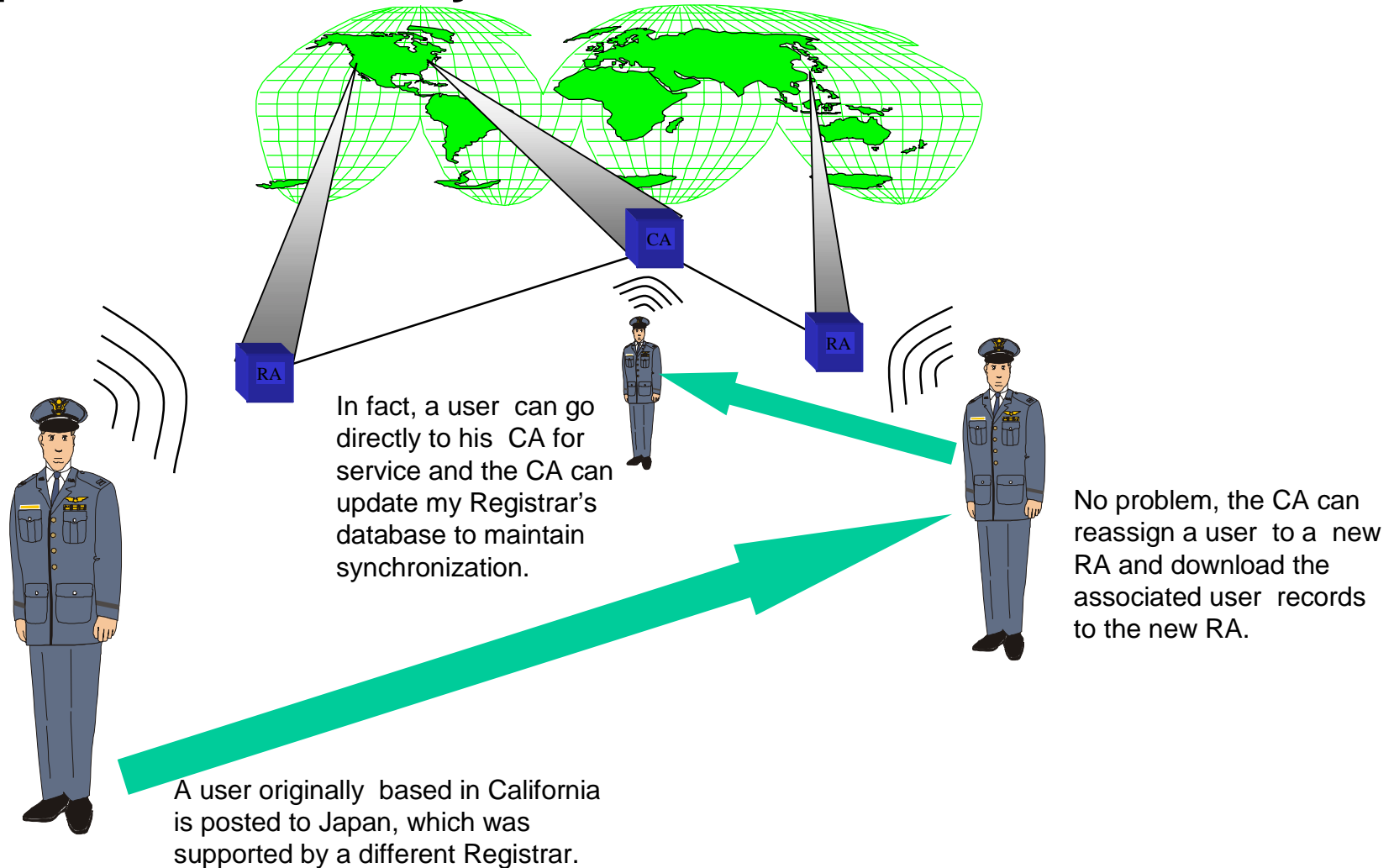
SKIPJACK Encryption
Key Exchange Algorithm (KEA)
Digital Signature Algorithm (DSA)
Secure Hash Algorithm (SHA-1)

One Token to be used for all User's Needs Issued by one CA

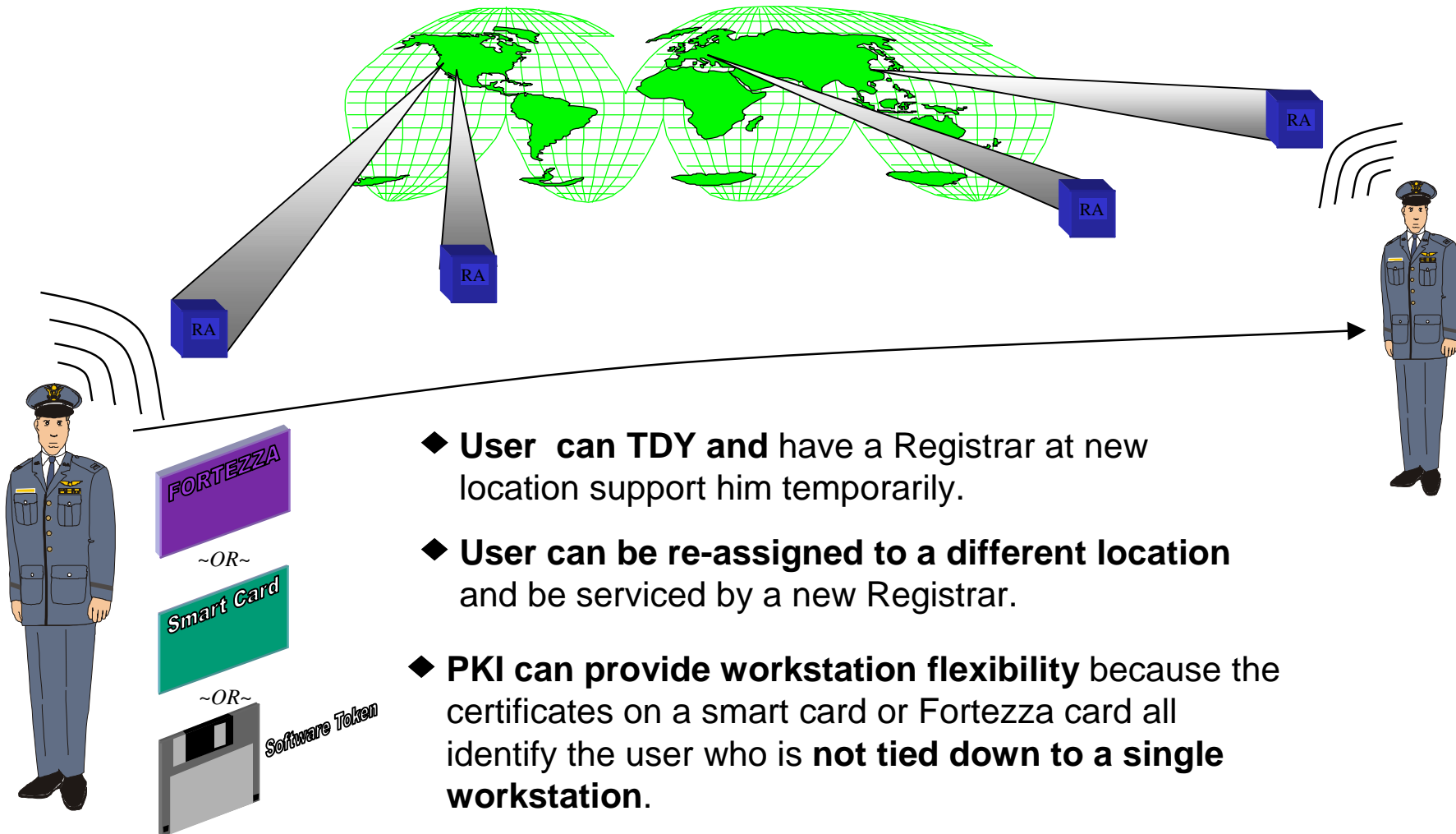


- ◆ **CipherNET** allows **one token to hold all user's private keys** on a single medium. Medium choice depends on protection needed by highest level private key.
- ◆ **CipherNET** supports storage of both high and medium assurance certificates on **one Fortezza Card**
- ◆ **A user could have a Smart Card** for the medium assurance certificates. The Smart Card adds to system security because the user's private key does not have to leave the token.
- ◆ **CipherNET** allows users to have a **floppy token** to hold their medium assurance certificates.
- ◆ **The PKI supports traveling user** with different token (possibly different medium) for use when outside of protected enclave

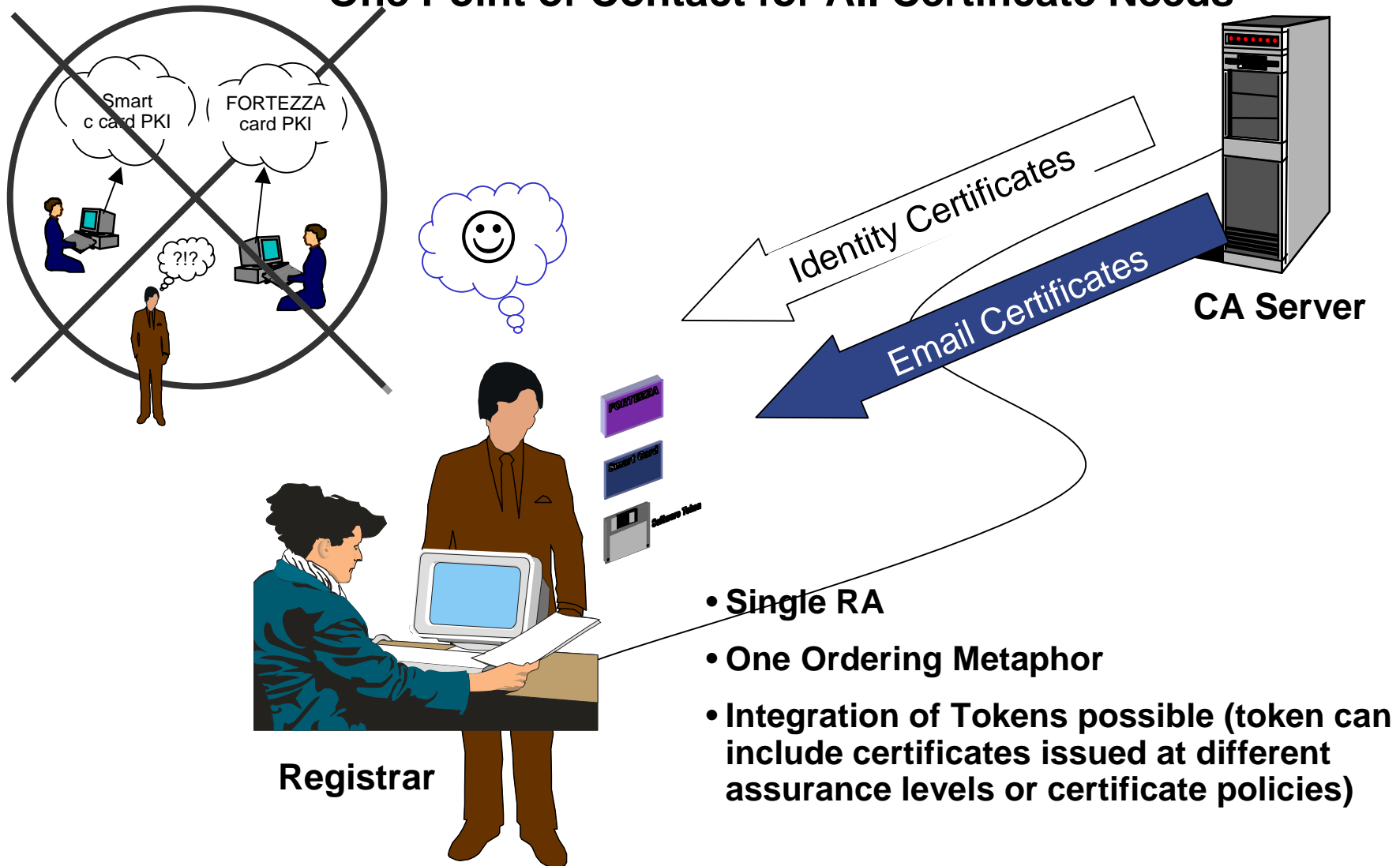
Supports User Mobility



Full Service for Mobile Users

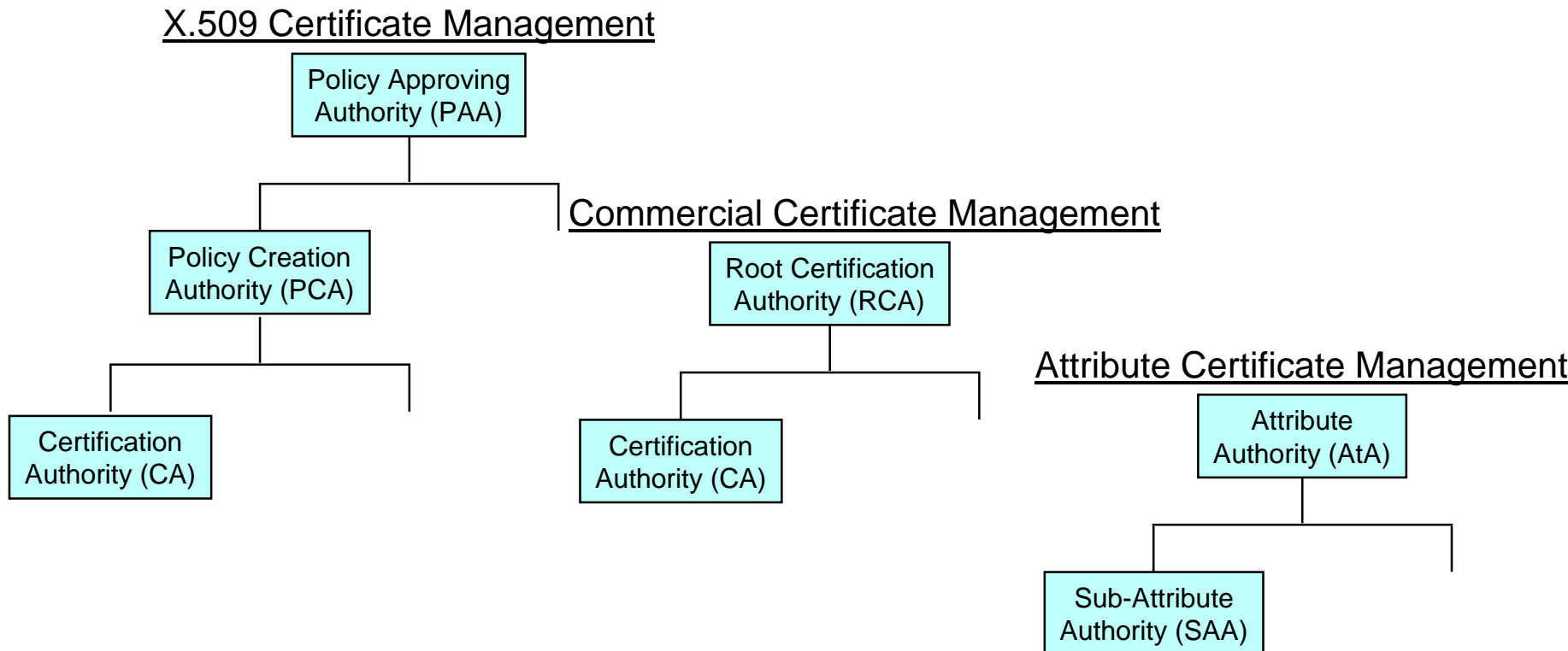


One Point of Contact for All Certificate Needs

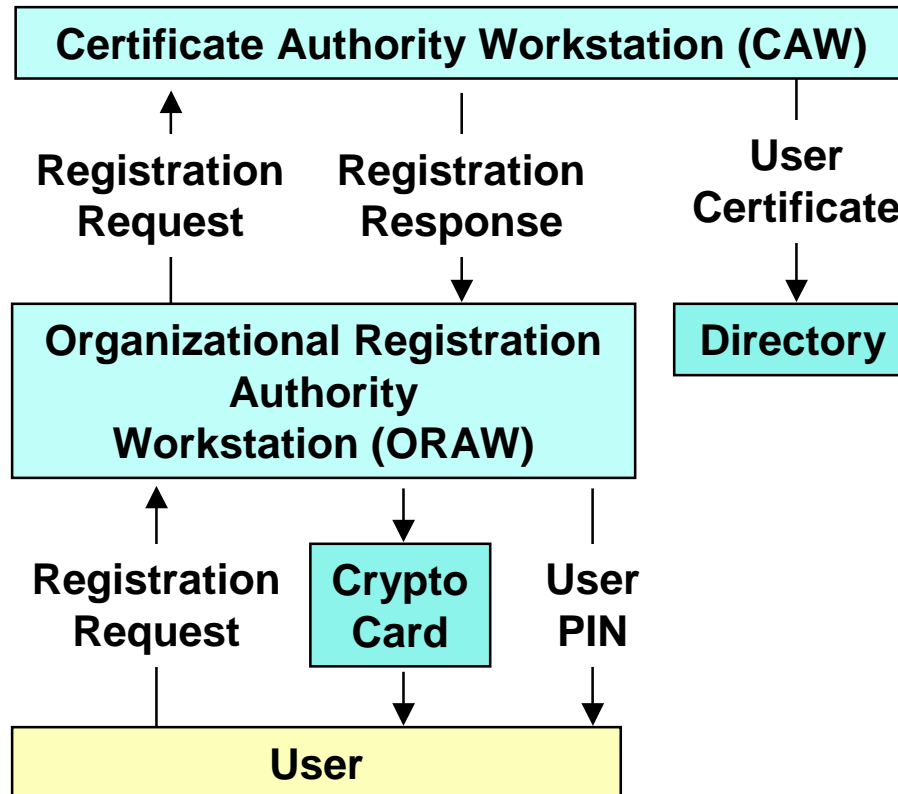


Certification Hierarchy

NSM Provides Hierarchical Certificate Management

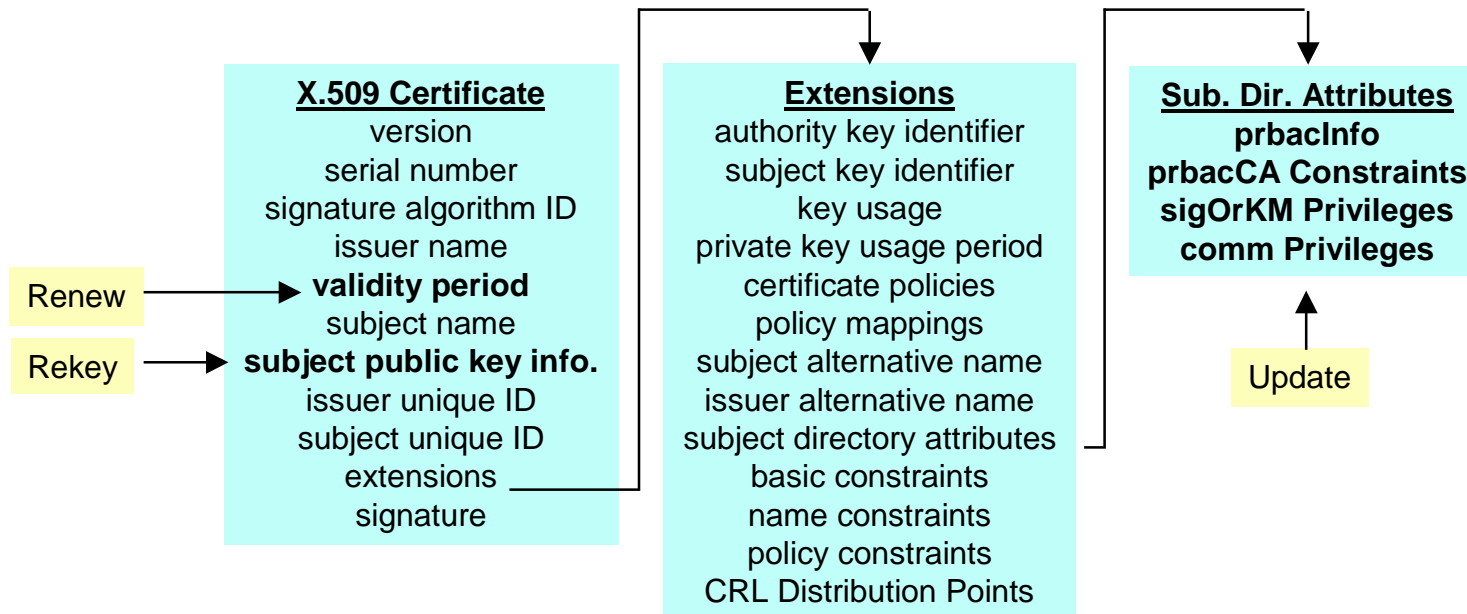


User Registration



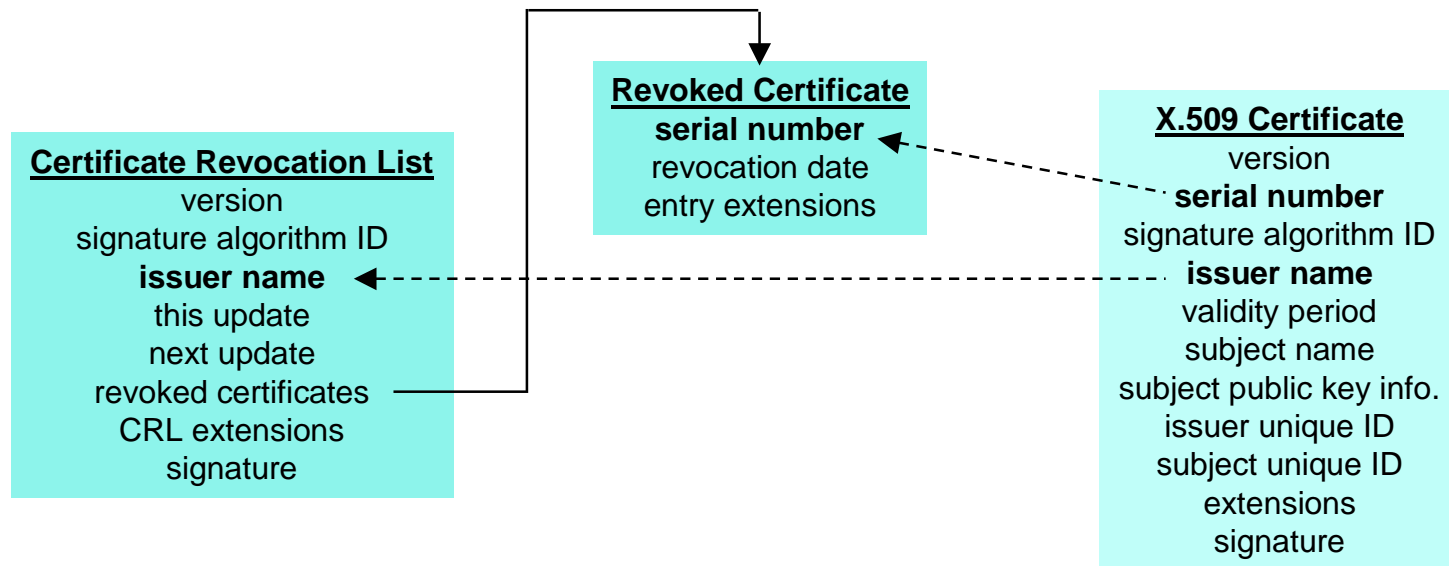
Certificate Renewal/Rekey/Update

Certificate Maintenance Functions



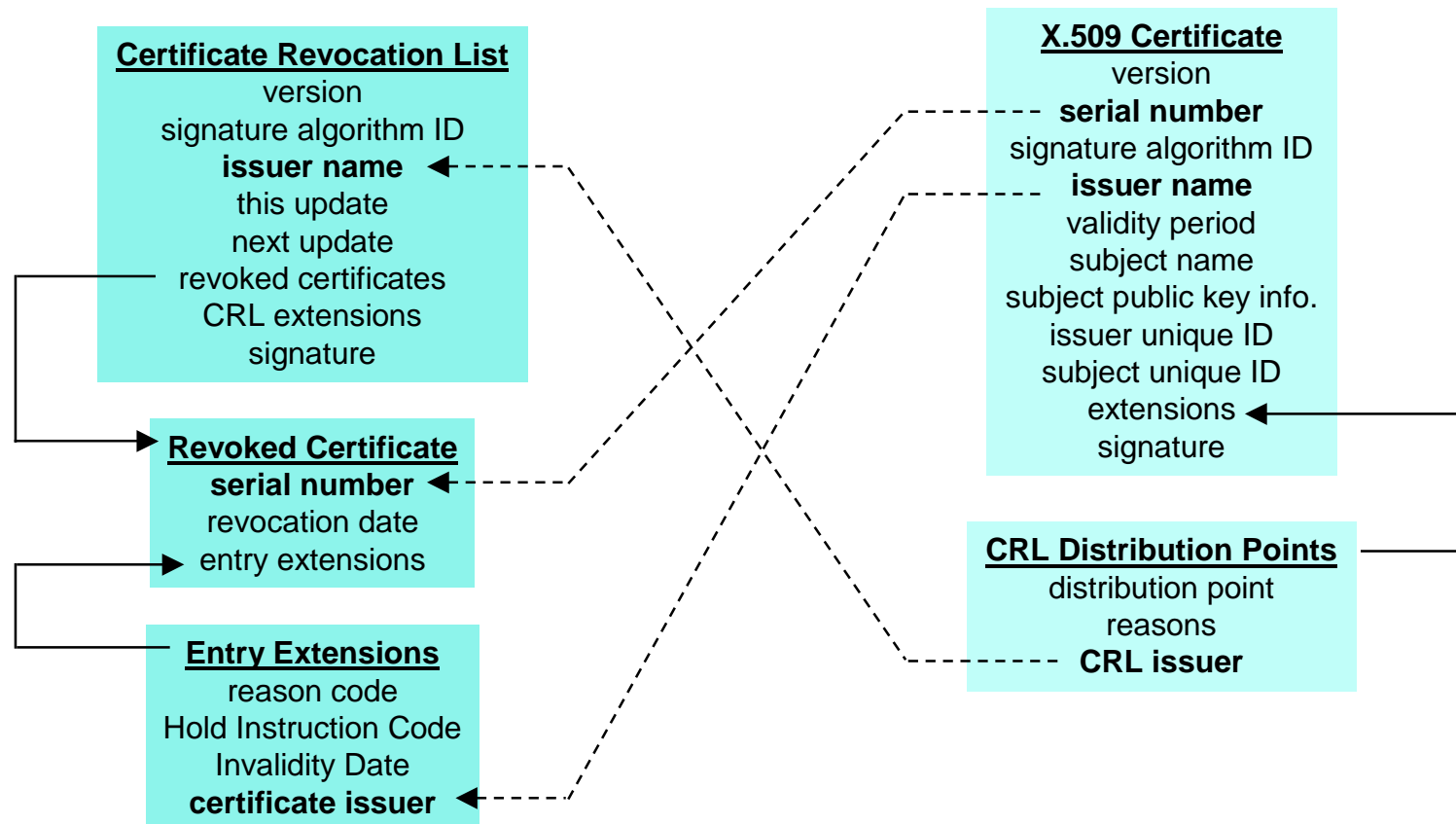
Certificate Revocation

- Certificates May Need to be Revoked Due to an Individual Leaving an Organization or a Change in an Individual's Privileges
- Certificates are Revoked Via Certificate Revocation Lists (CRLs), Which Are Posted to the Directory



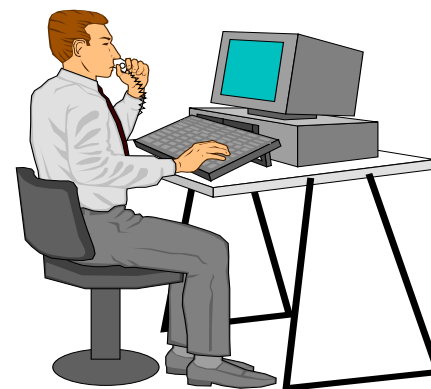
Compromise Recovery

Indirect Certificate Revocation Lists (ICRLs) Provide Recovery in the Event of the Compromise of an Individual's Private Key



Product Support

- Training
 - Classroom
 - Onsite
- Tech Support and Help Desk
- Web Site
 - General Information
 - Tech Support
 - SW Maintenance/upgrades
 - Training Scheduling
 - Sales and Marketing



CAW 4.2.1 Training

- Formal Classroom Training Initially Required
- Follow-On Training Can Be Done With CBT
 - Includes Assistant CA and SA/ISSO Training
- Training Available from Service Schools
 - Ft. Gordon, GA Seoul, Korea
 - Ft. Huachuca, AZ Mannheim, Germany
 - Keesler AFB, MI Wahiawa, Hawaii
- And Vendor (Motorola)
 - Linthicum, MD Scottsdale, AZ

CAW 4.2.1 Installation Strategy

- Army/Navy Using Install Teams
 - Teams Received Training From Motorola
 - Schedule Tied to Delivery of DMS 2.2
- Air Force Debating Use of Install Teams
 - Current Plan Is to Let Site Do Install With Phone Help From Motorola
- Motorola Provides Install Support

CAW 4.2.1

- *CipherNET*[®] 3000, Based on CAW 4.2.1, Is Culmination of Years of Work by Industry Experts:
 - NSA X, Y and C Organizations
 - DMS Leaders at DISA and Lockheed Martin
 - V3 Application Providers
- *CipherNET* 3000 Has Benefited by Extensive Scrutiny by the DoD Community
- Design Responded to Feedback From User Community Learned Via Operational Activities
- *CipherNET*'s Trusted Architecture Has Been Designed to Be Easily Extensible

QUESTIONS & DISCUSSION