


# Network Security Manager

## PKI For DoD

## Defense Messaging System

**The Open Group**

**September 25, 1997**

**Bob Frith**

**Motorola**

# NSM Objectives

MOTOROLA

*Information Security Division*

- **Provide a flexible and evolving Security Management Infrastructure (SMI) solution for the Multilevel Information System Security Initiative (MISSI).**
  - **CMI, Audit, Archive, Key Management**
- **Provide Security enablement of User Applications**
  - **"Messaging" Applications**
    - **Email, File Transfer, Remote Login, WWW Access, etc.**
  - **Data Storage Applications**
- **Meet DMS 2.0 SMI requirements**
- **Provide interoperable security solutions for DoD, Allies, Civil Government, Trading Partners and Public Domain**

# High Level Components of SMI



| Components | Elements |
| --- | --- |
| Certificate Management | Technology |
| Audit Management | Doctrine |
| Archive Management | Policies |
| Privilege/Access Management | Procedures |
| Key Management | |

*?*

*?*

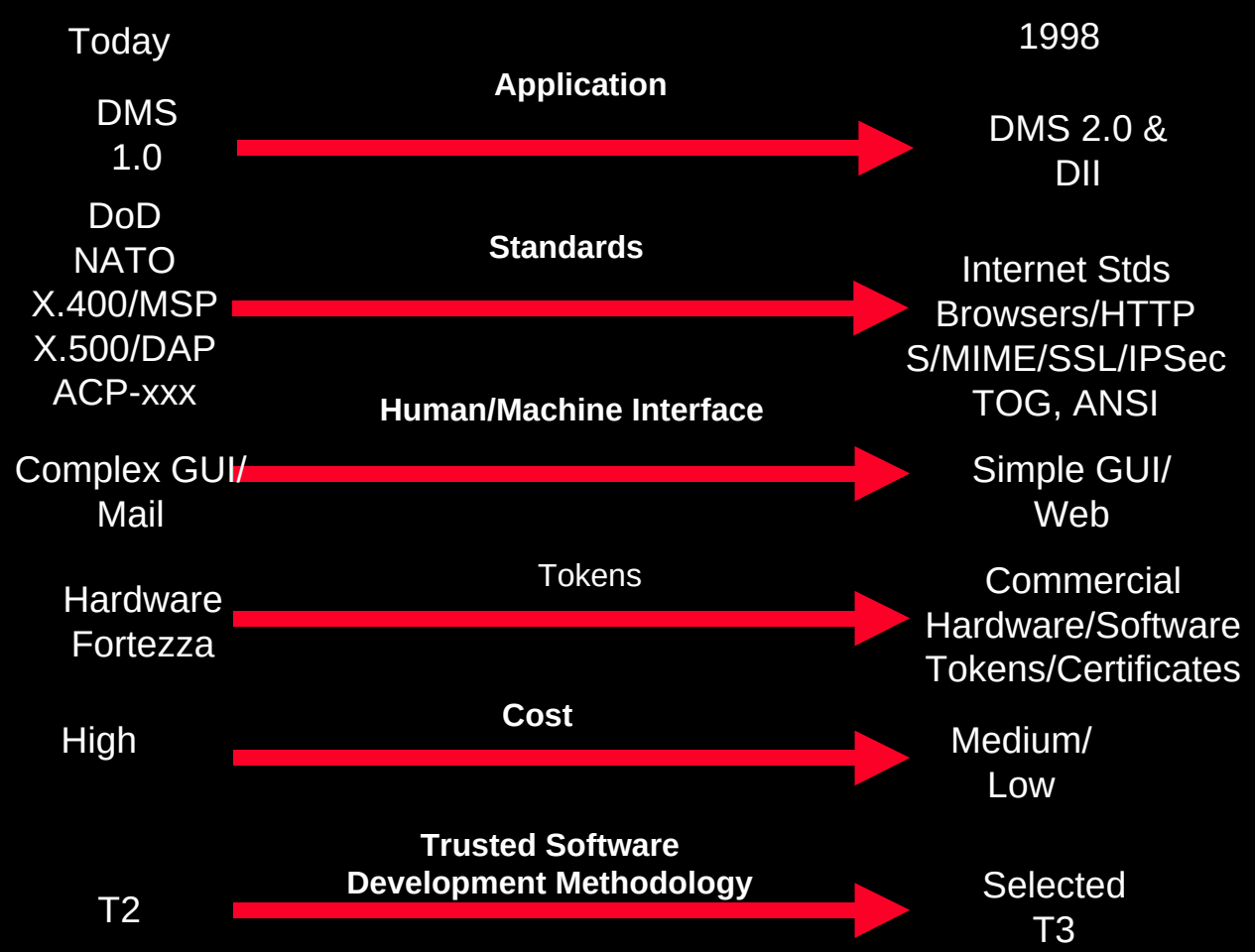
# Challenges



- Incremental system architecture
  - Serves immediate needs and grows to meet future requirements
- Robust system architecture
  - Open and responds rapidly to change
- Compatible with other security solutions and applications
  - Interoperable, graded security, value
- Meet Defense Information Infrastructure (DII) needs
  - Low to high

# NSM Growth and Evolution

*Information Security Division*



# NSM Release Features

*Information Security Division*

**Rel. 3.0 - Rel. 3.1**

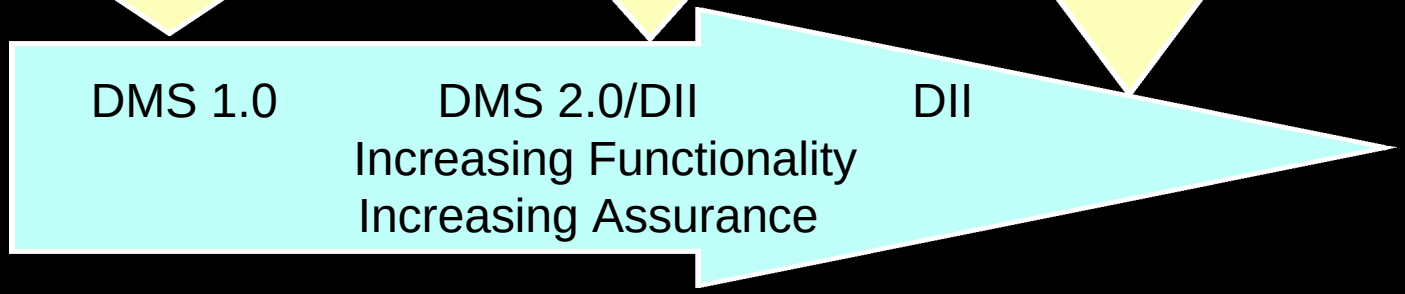
MISSI V1 Certs
MISSI V1 CRL/CKL
MISSI VI PRBAC
MSP 3.0
Fortezza
Med. Assurance

**Rel. 4.1 - Rel. 4.2**

Additional Capabilities:
V3 Certs
V2 CRL//ICRL
MISSI V3 PRBAC
MSP 4.0
Commercial Tokens
Med. High Assurance
Audit Manager
Audit Agents

**Rel. 5.X Option**

Additional Capabilities:
FLEX V3 Certs
Flex V2 CRL
Type 1 Token
High Assurance
Auto Intrusion Detect
LRBAC



# Overview of Program Plan Major Planned Milestones

MOTOROLA

*Information Security Division*

| | CY 96 | | CY 97 | | | | | CY 98 | |
|---|---|---|---|---|---|---|---|---|---|
| **Event** | **4th Qtr** | **1st Qtr** | **2nd Qtr** | **3rd Qtr** | **4th Qtr** | **1st Qtr** | **2nd Qtr** | **3rd Qtr** | **4th Qtr** |
| **3.1 Release Operationally Supportable** | | | ▲ | | | | | | |
| **4.1 Release Interim/Fieldable** | | | ▲ | | ▲ | | | | |
| **4.2 Release Fieldable** | | | | | | | | ▲ | |

# Contract Deliverables

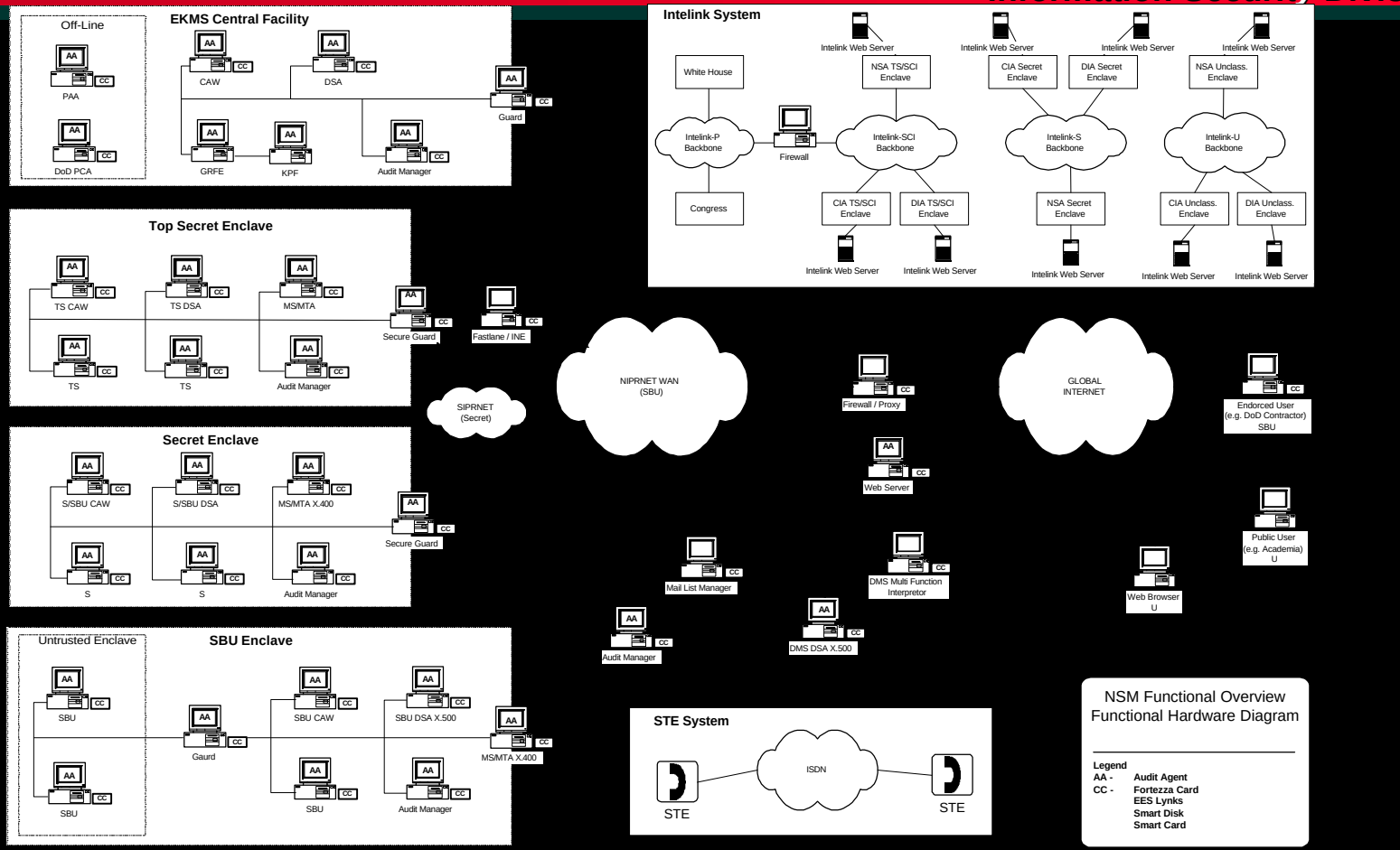


- Turnkey Systems
  - COTS Platforms with NSM application Software
    - SCO CMW+, HP CMW, Trusted Solaris, Win NT
- Documentation
  - NSM Specifications
  - Engineering Studies
  - Design Documents
  - Training Documents
  - Operations Documents

# Security Management Infrastructure (SMI) System Environment

MOTOROLA

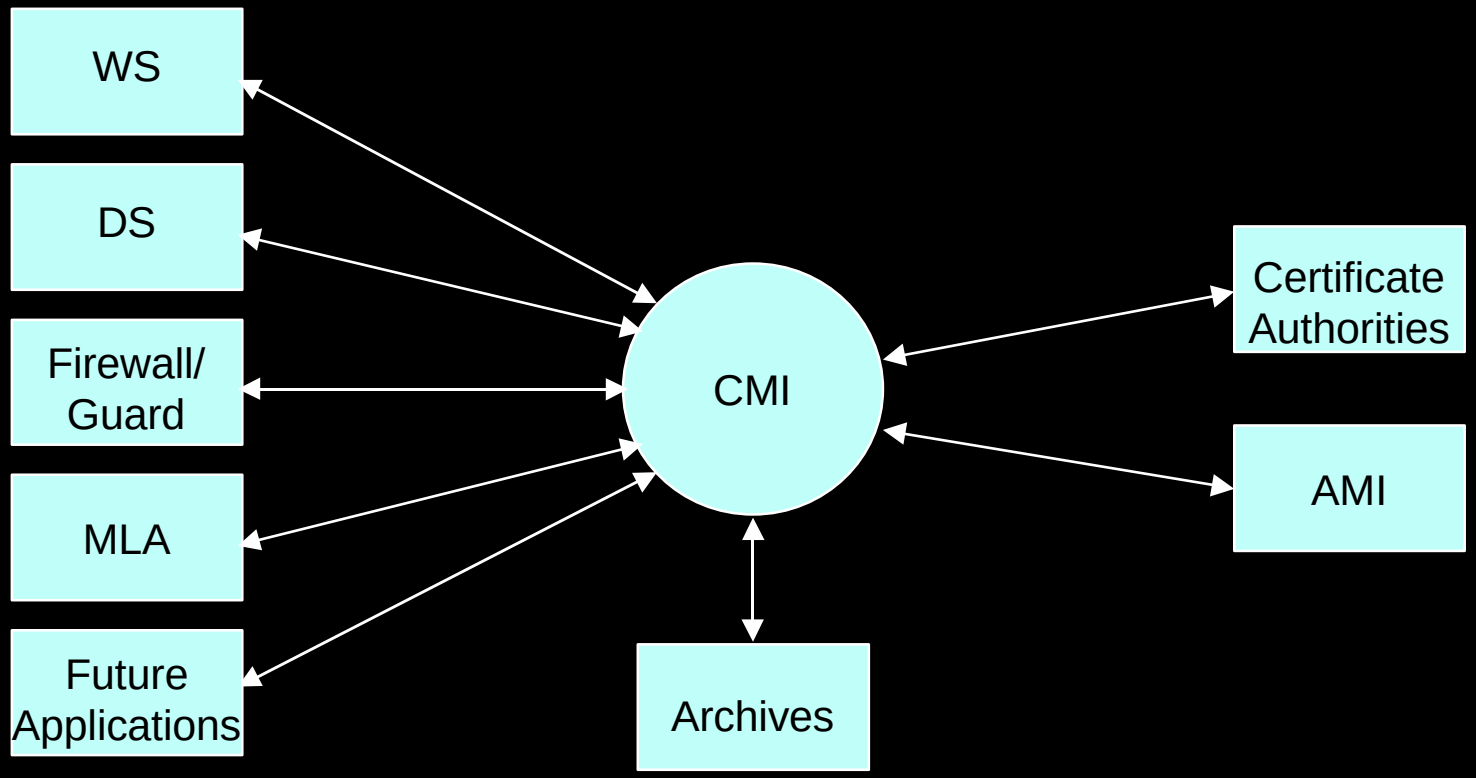
*Information Security Division*



# Certificate Management Infrastructure (CMI) System Context

MOTOROLA

*Information Security Division*




# Certificate Management Functions



- User Registration
- Public/Private Key Generation
- Certificate Creation & Validation
- Certificate Issuance, Delivery, and Token Management
- Directory Interface
- Certificate Revocation & Key Compromise Recovery Services
- Support to Audit, Archiving, and Data Recovery Processes

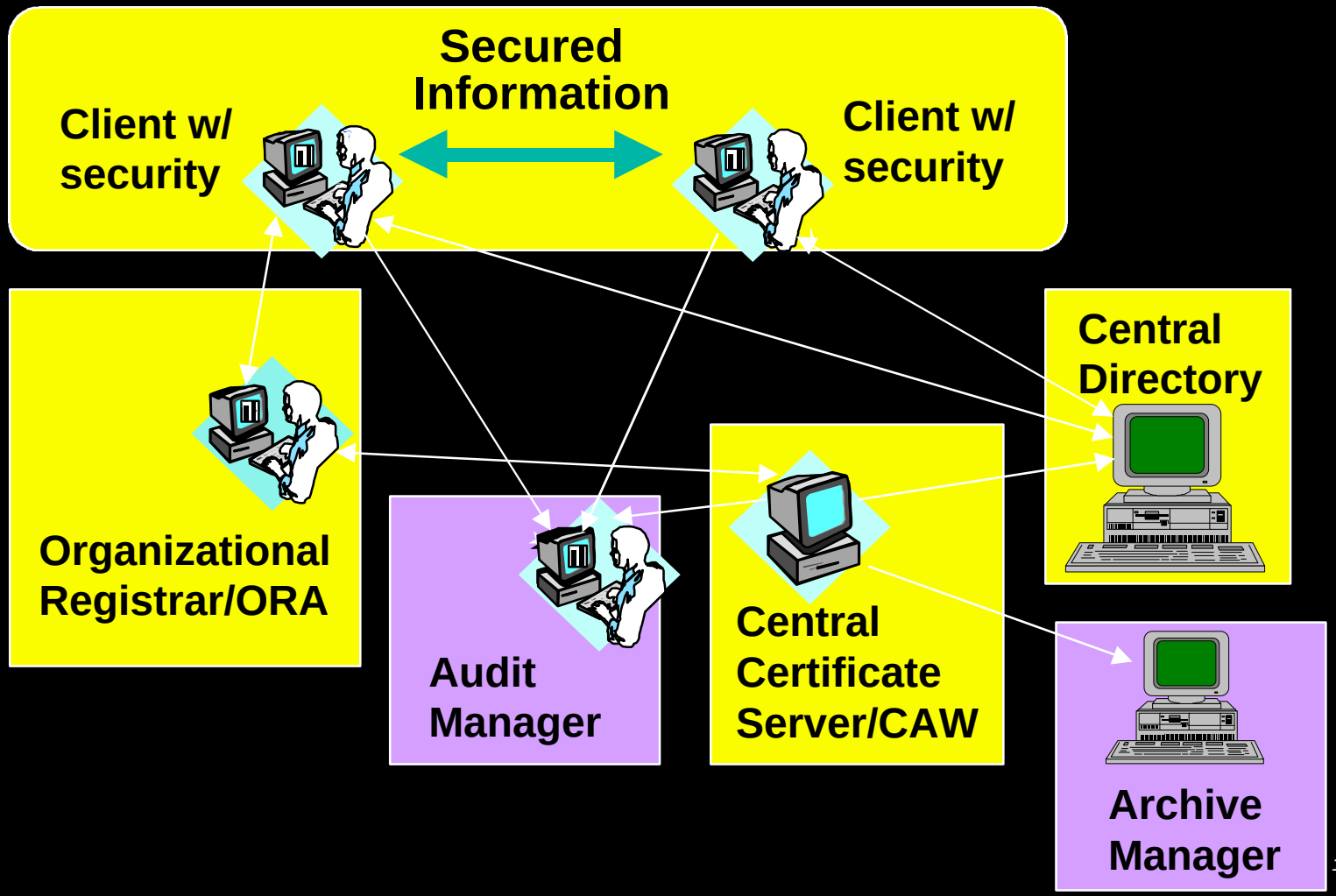
# Certificate Management Infrastructure



- 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

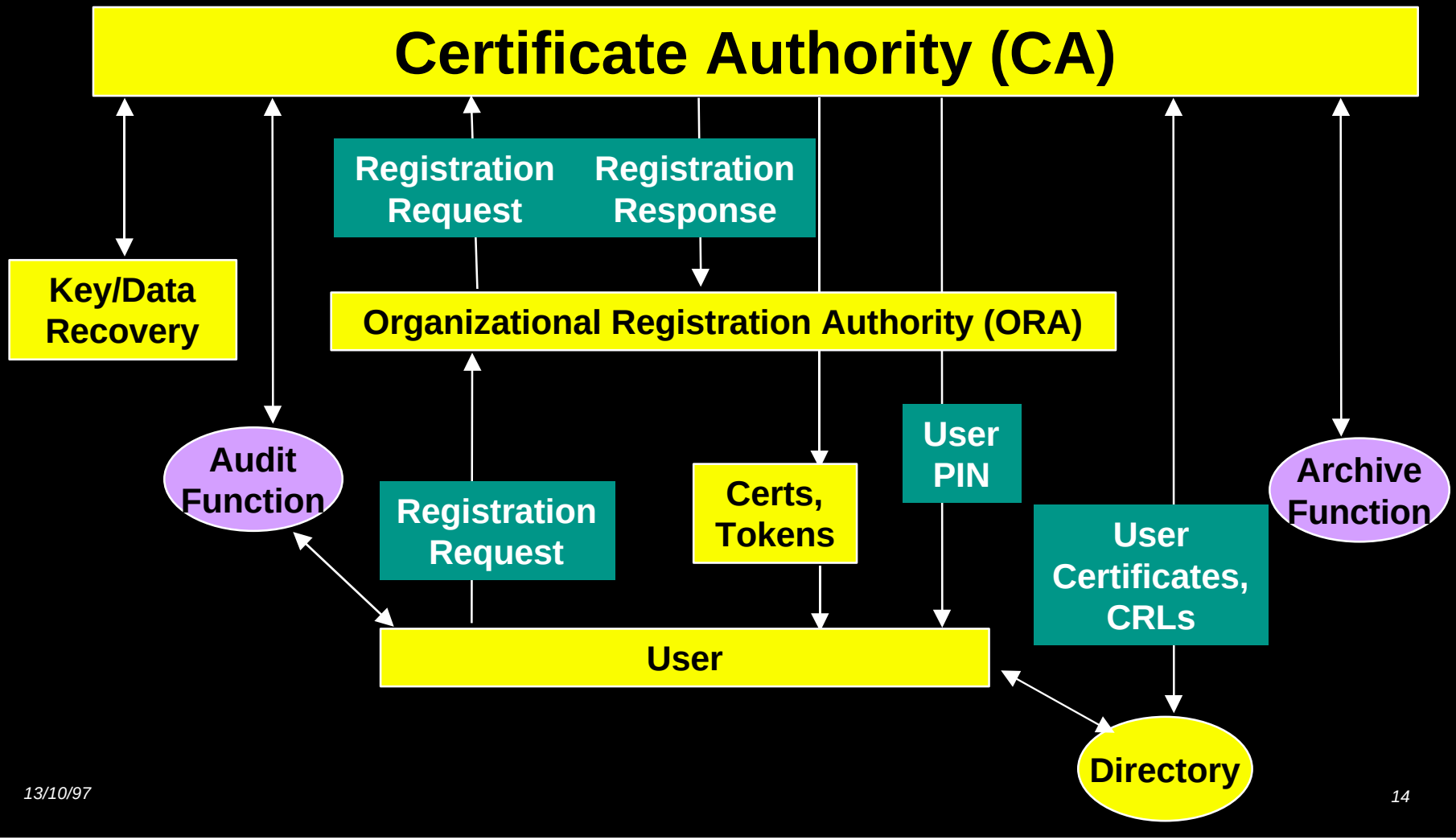
# CMI System Environment

*Information Security Division*



# The CMI Data Flow






# Certificate-Based Access Control Alternatives

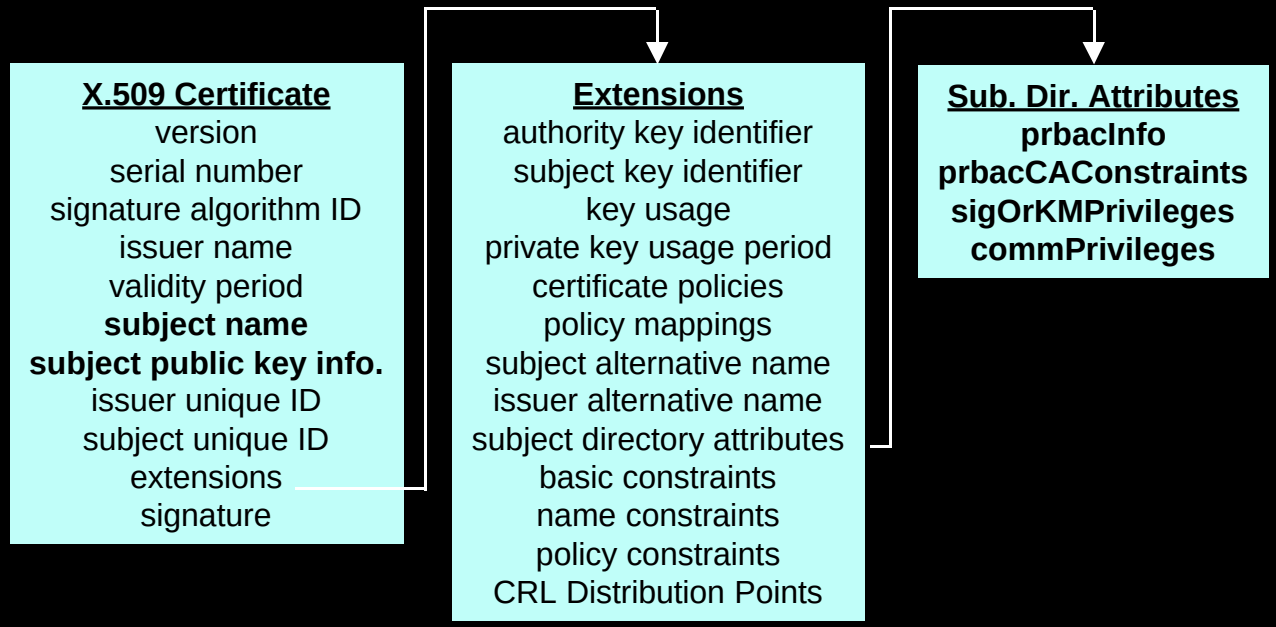


- Identity Based Access Control (IBAC)
  - Access based on user identity
  - Subject Name in certificate can be used for IBAC
- Rule Based Access Control (RBAC)
  - Based on a set of user authorizations, object sensitivities, and rules as to which user authorizations grant access to which object sensitivities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

# X.509 Certificates



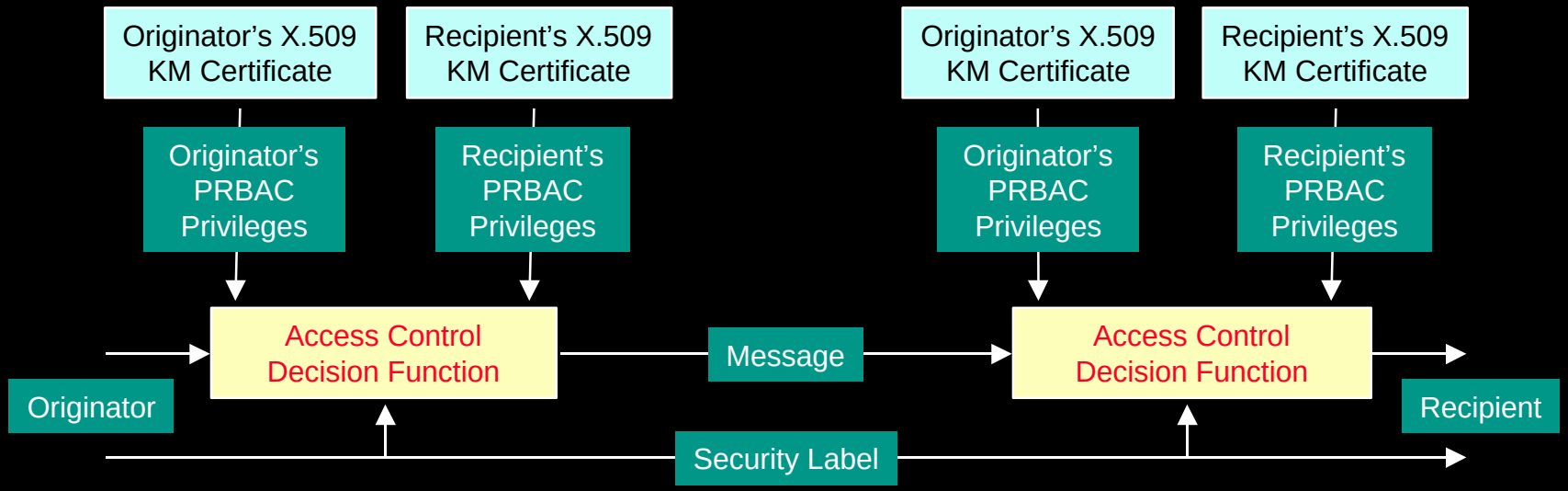
- X.509 certificates may contain public signature keys or public key management (KM) keys
- Also provide privileges for Partition Rule Based Access Control (PRBAC)



# X.509 Key Management Certificates

*Information Security Division*

## Certificates Provide Privileges for Partitioned Rule Based Access Control




# Attribute Certificates



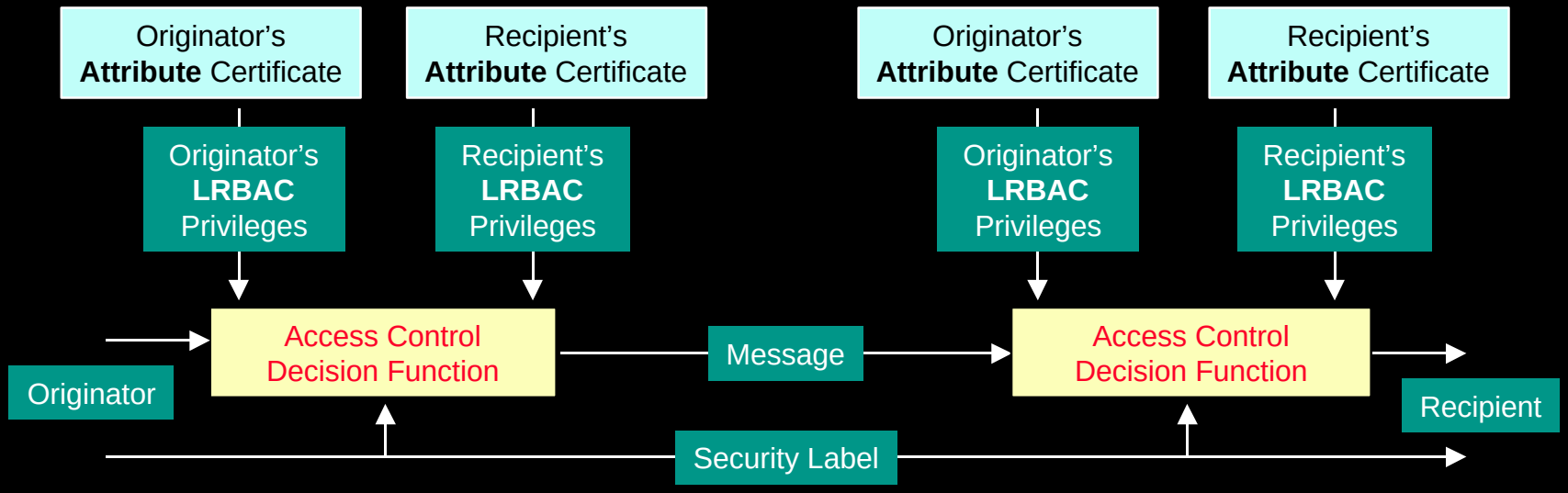
## Attribute Certificates Provide Privileges for Local Rule Based Access Control

**Attribute Certificate**
version
**subject name**
issuer name
signature algorithm ID
serial number
validity period
**attributes**
issuer unique ID
extensions
signature

# Attribute Certificates



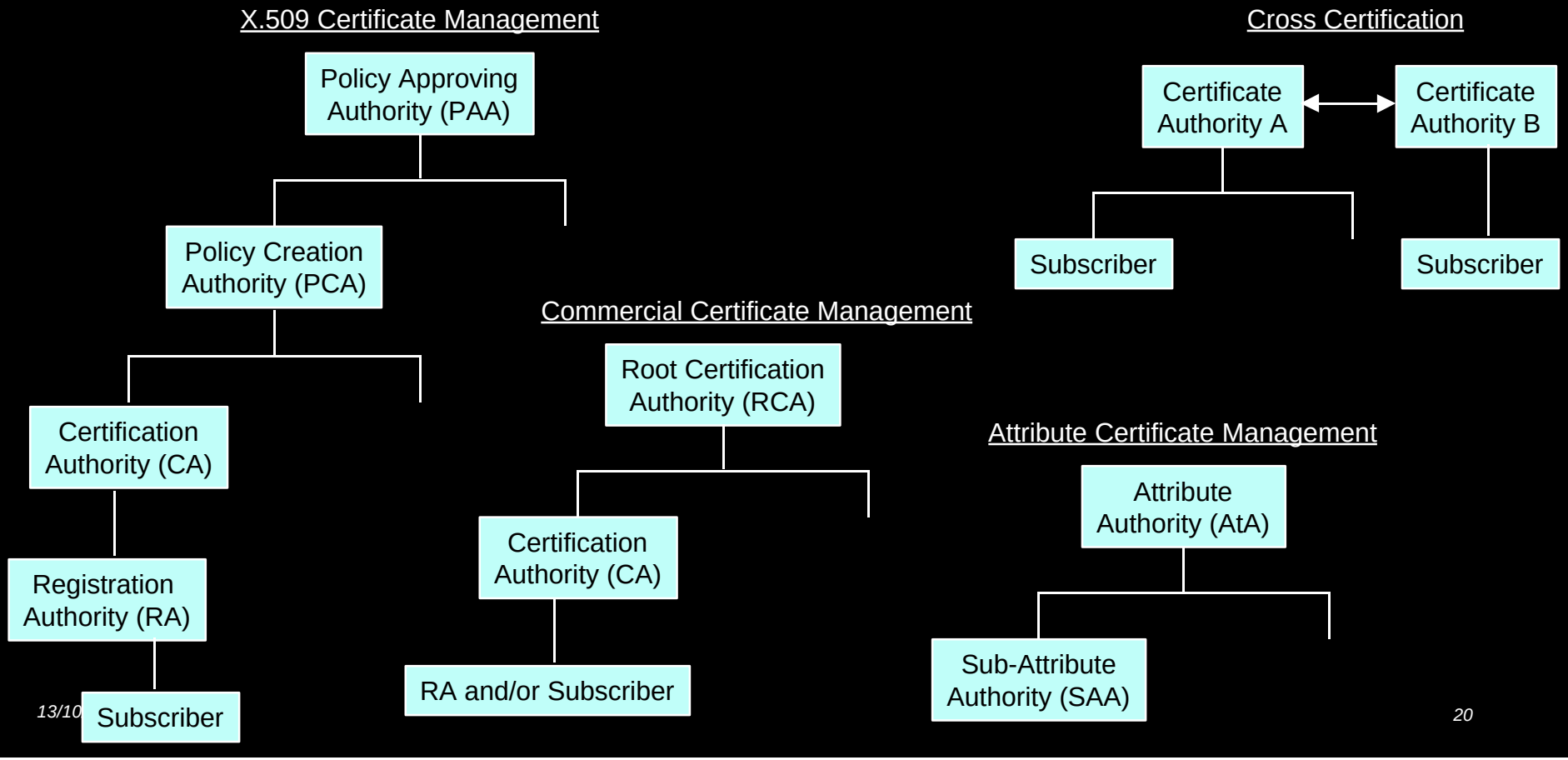
## Provide Privileges for Local Rule Based Access Control



# Certification Hierarchy

*Information Security Division*

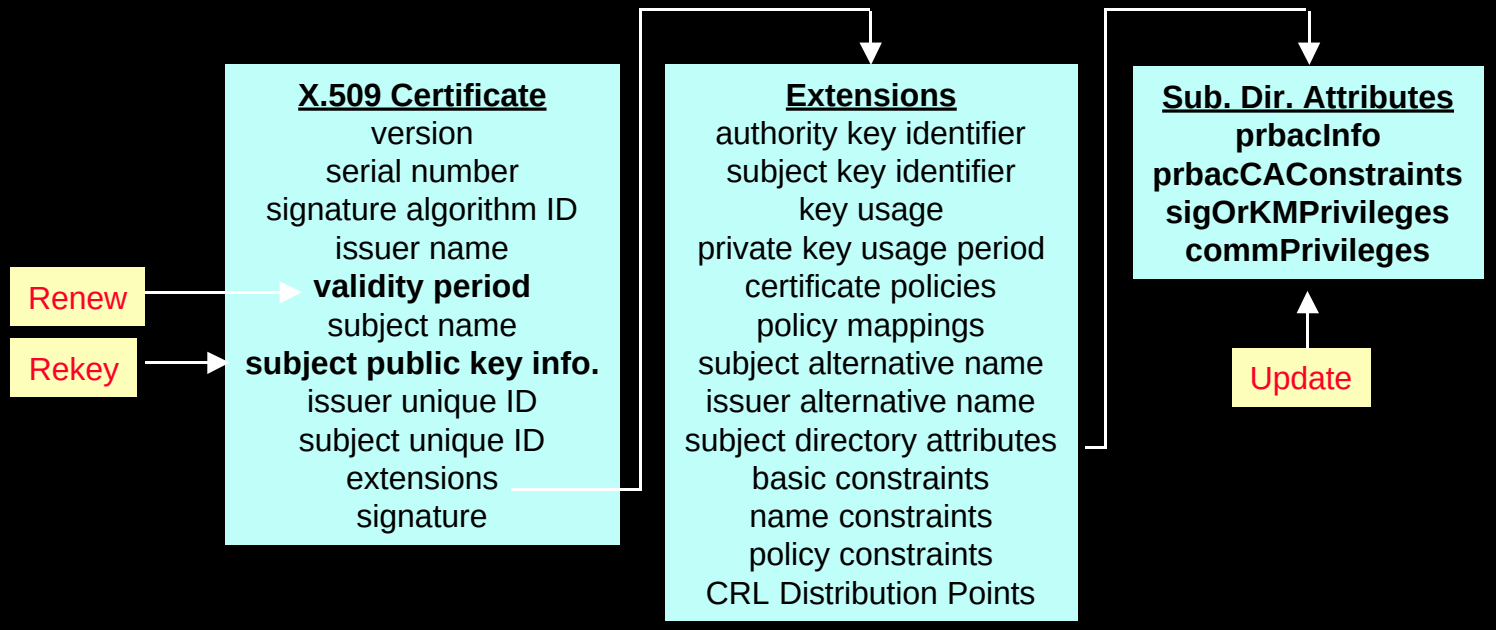
## NSM Provides Hierarchical & Flat Certificate Management



# Certificate Renewal/Rekey/Update

*Information Security Division*

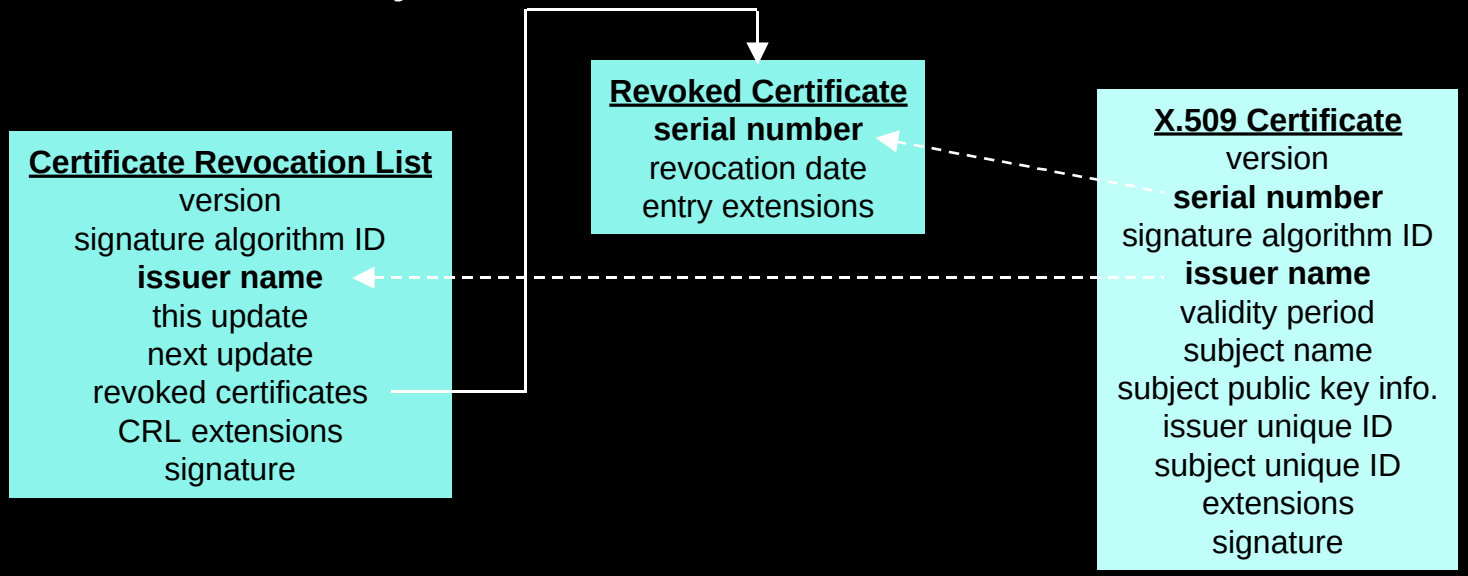
## CMI provides Certificate Maintenance Functions



# Certificate Revocation



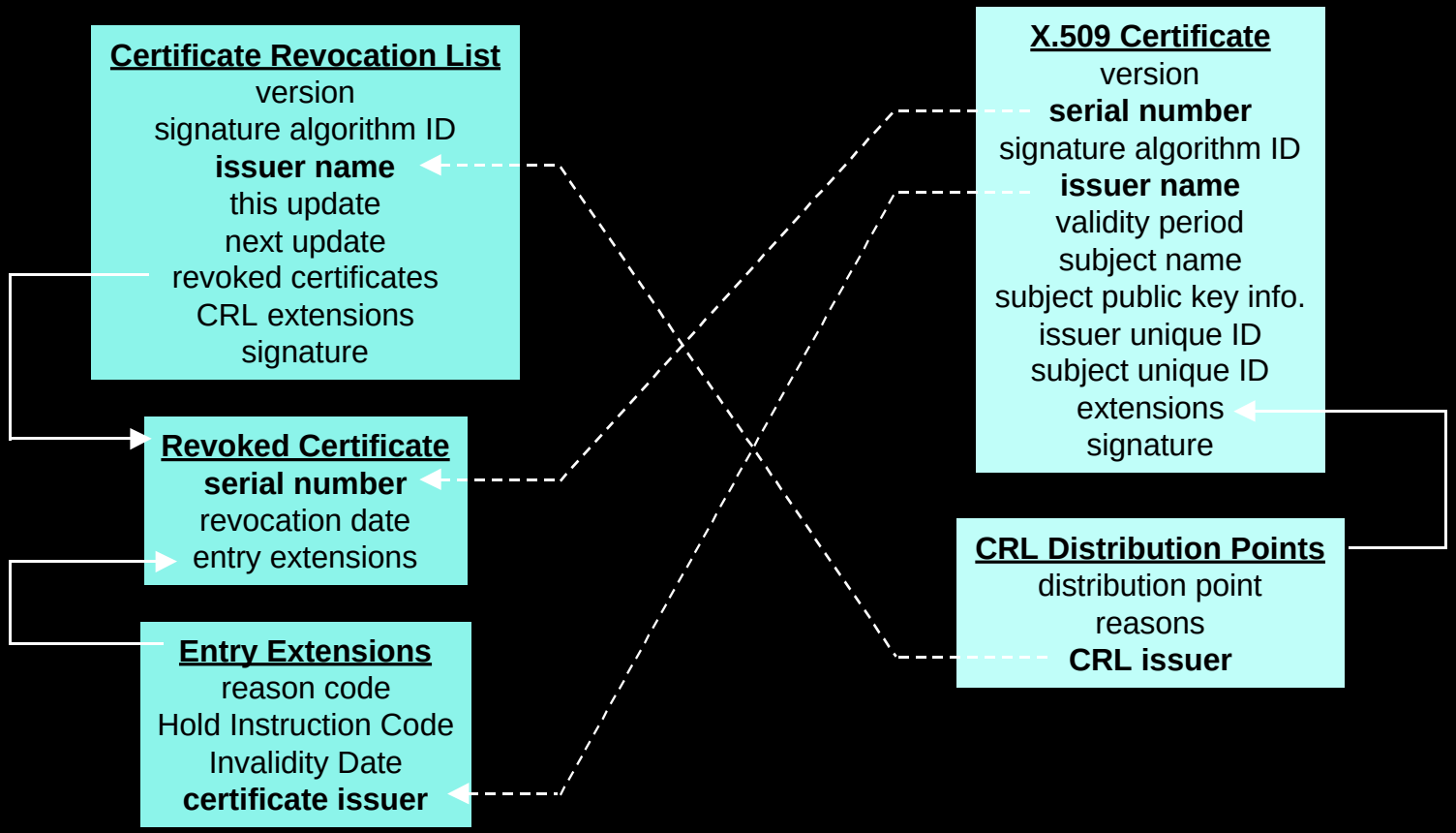
- Certificates may need to be revoked due to an individual leaving an organization or a change in an individual's privileges
- Certificates are revoked via Certificate Revocation Lists (CRLs), which are posted to the Directory



# Compromise Recovery



**Indirect Certificate Revocation Lists (ICRLs) provide recovery in the event of the compromise of an individual's private key**



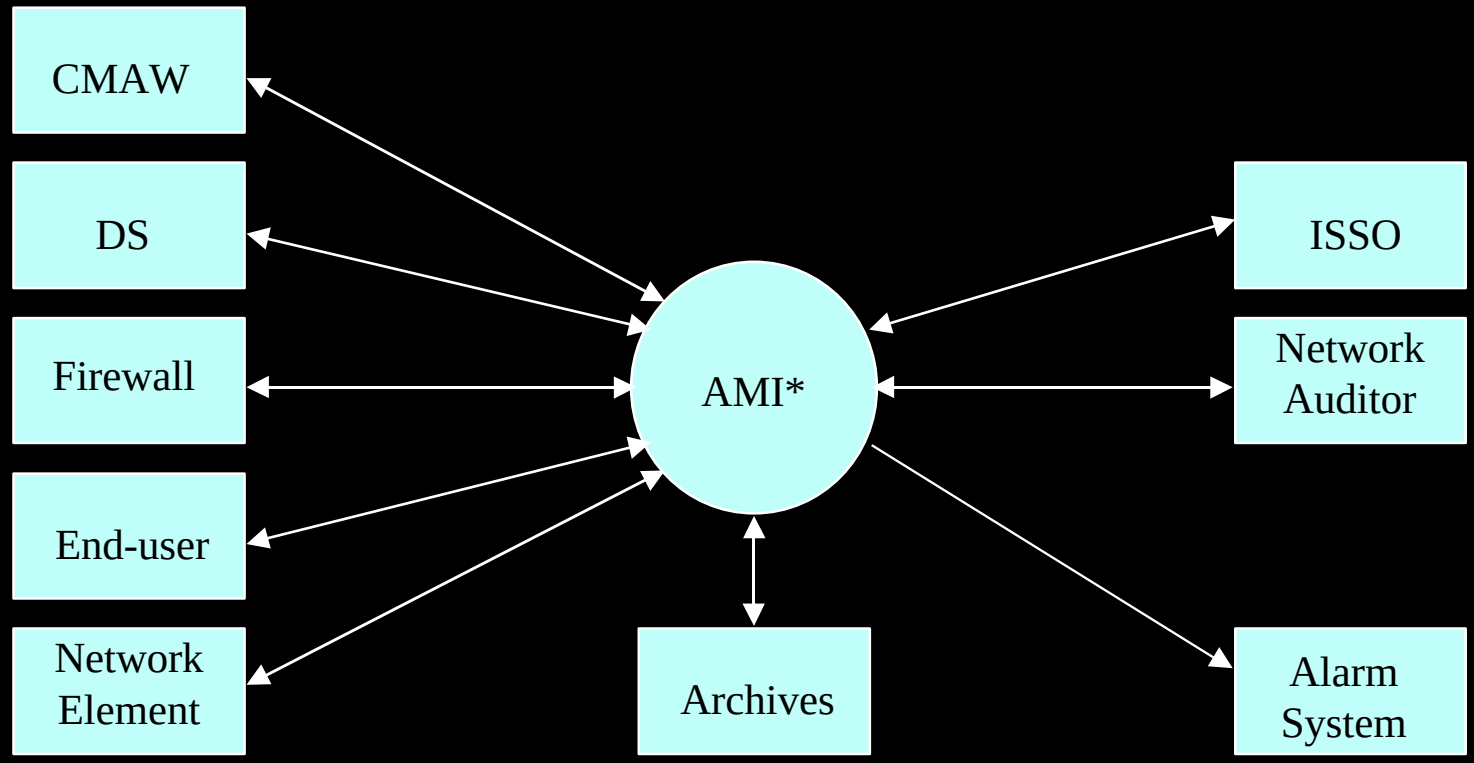

# Archive Management



- Stores, manages, and preserves electronic records for historical reference
  - Maintains integrity and authenticity of archived records
  - Maintains the means of authentication
  - Consolidates CMI archives
- Enables historical non-repudiation
  - Maintain continuity of non-repudiation services
- Provides means to validate signatures using a public key contained in an expired certificate
  - Provides defense against claims of false certifications and false revocations

# Audit Management Infrastructure (AMI) System Context






*Primarily Integration


# Audit Management Infrastructure

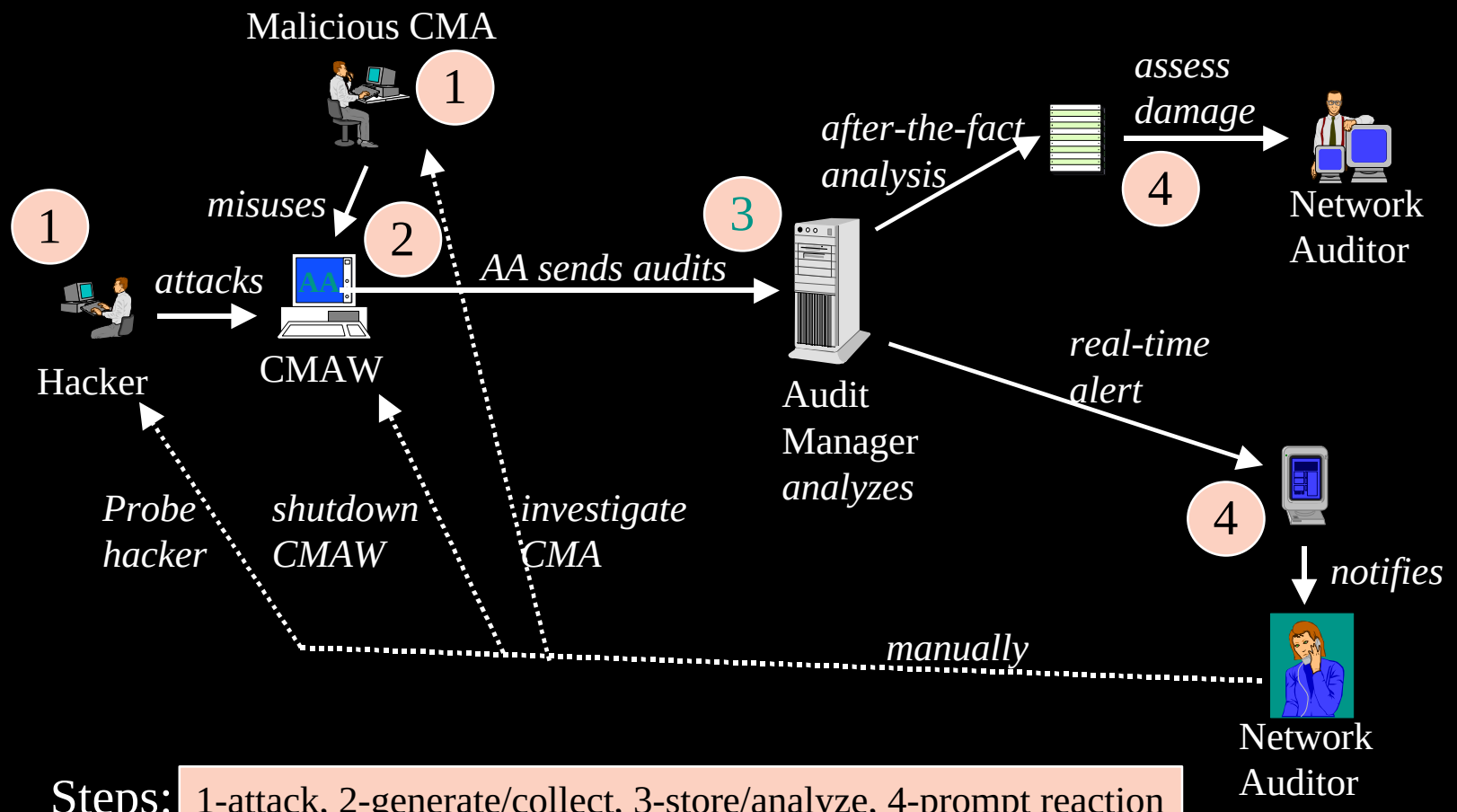


- Provides monitoring to aid in the detection of incorrect behavior of the system due to design errors, system failures, human errors, and malicious actions
  - Aids in detection of unauthorized use of the system and aids in assessment of damage when unauthorized use has occurred.
- Also aids in monitoring of system performance and preservation of system availability
- Provides real time alerts to prompt immediate reaction upon detection of anomalies in system behavior
- Provides long term record of system activities for later analysis

# Manual Anomaly Analysis

MOTOROLA

Information Security Division

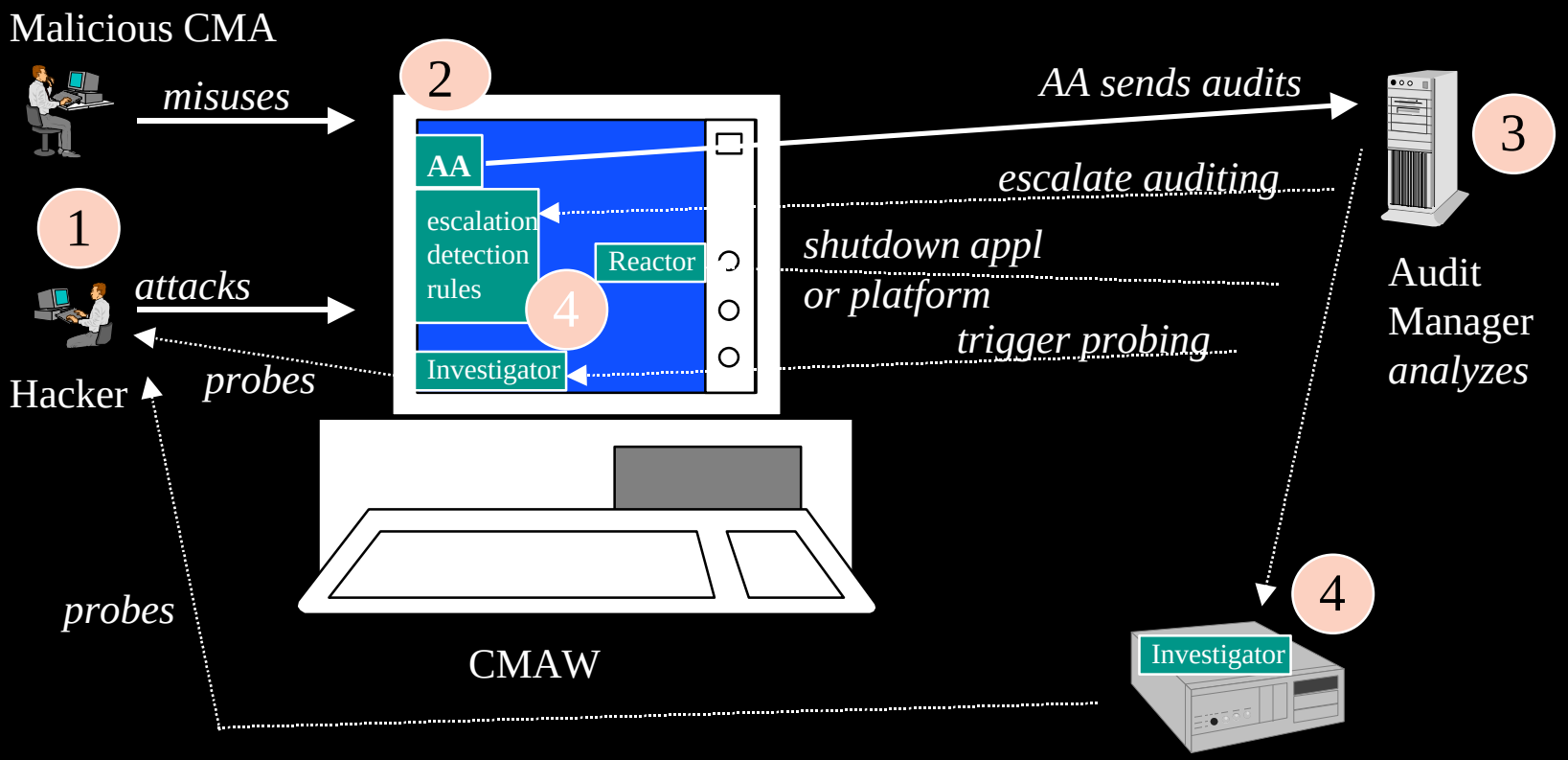



Steps: 1-attack, 2-generate/collect, 3-store/analyze, 4-prompt reaction

# Automated Anomaly Reaction

MOTOROLA

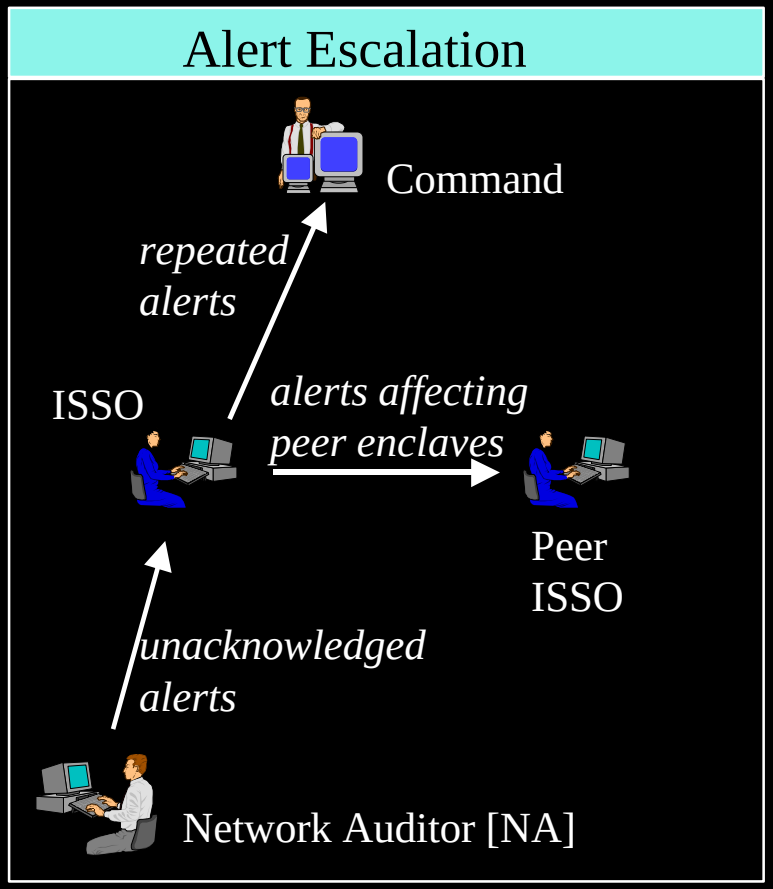
Information Security Division

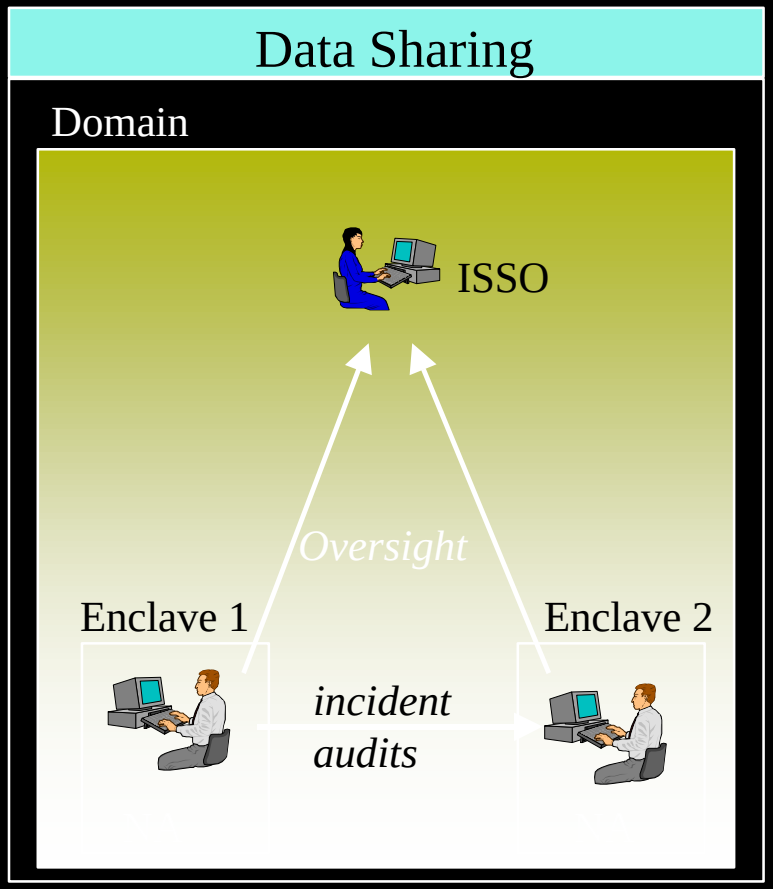



Steps: 1-attack, 2-generate/collect, 3-store/analyze, 4-prompt reaction

# AMI Hierarchies and Peers

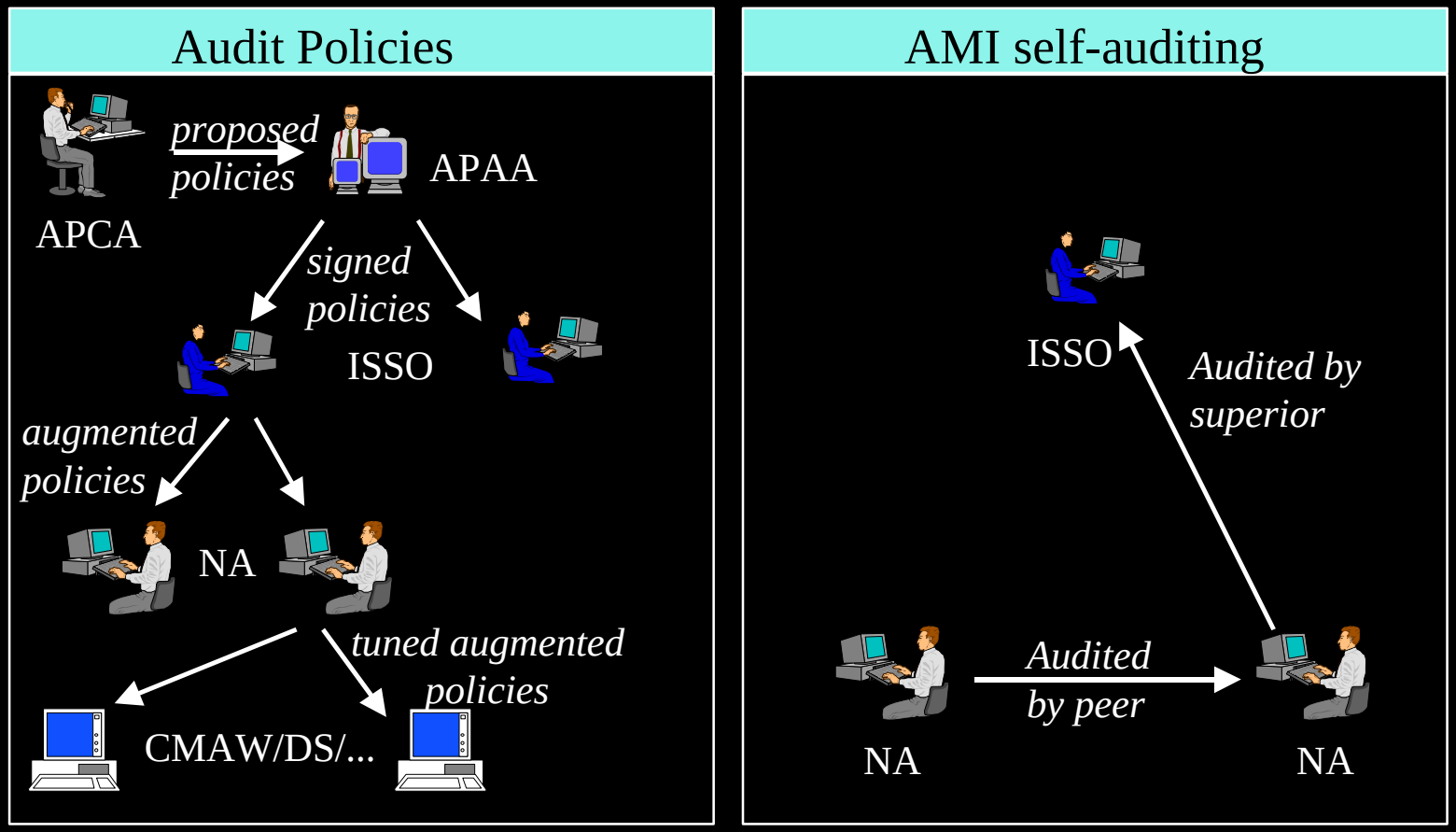




# AMI Hierarchies and Peers (continued)






# Audit Management Infrastructure Elements

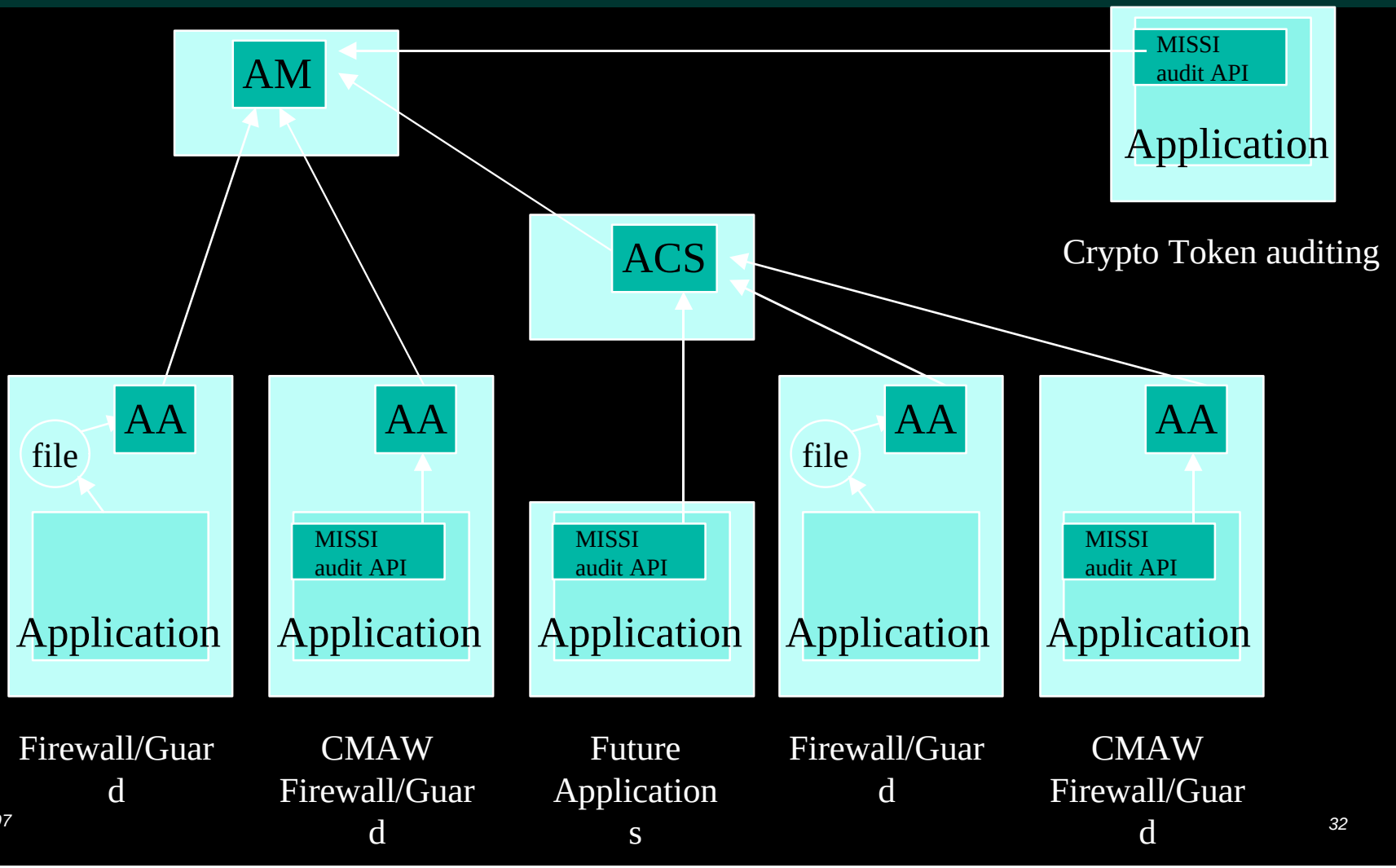


- Audit Detectors - in the application, OS, or AMI to detect an auditable situation and generate an audit (either by writing to a file, via the OS's native auditing subsystem API, or via the MISSI Audit API).
- MISSI Audit API - accepts audits directly from an application or OS, and sends them to an Audit Agent, Collection Sserver, or Manager.
- Audit Agent [AA] - a local audit collector [from files and applications], temporary buffer, and rule-based intrusion/misuse detector. Internally uses the same subroutines as the MISSI Audit API. Has NO user interface.
- Audit Collection Server [ACS] - an AA that can also collect audits from remote platforms. The audits can be stored in remote files, or sent via the network from an AA or MISSI Audit API. Has NO user interface.
- Audit Manager [AM] - centrally stores audit events received, performs analysis on those audits, provides results of the analysis to the Network Auditor, alerts Network Auditor to problems, and remotely controls the configuration of the AAs and the ACSs it receives audits from.

# Audit Event Network Data Flow Possibilities

MOTOROLA

*Information Security Division*




# Summary



- NSM provides the Security Management Infrastructure (SMI) to enable and monitor network security applications
- The Certificate Management Infrastructure (CMI) provides certificates which enable public key based network security applications to provide source authentication, integrity, non-repudiation, confidentiality, and access control security services
- The Audit Management Infrastructure provides network security monitoring to aid in the detection of anomalies in system behavior and provide a record of system activities