DMDC

Information and Technology for Better Decision Making

Key & Card Management 101

Prepared for

Federal Agency Government Employees

Presented by

Winifrid Whaley, Senior Business Services Analyst

Jason Stenstrom, Senior Systems Engineer

Aug 2005

Overview

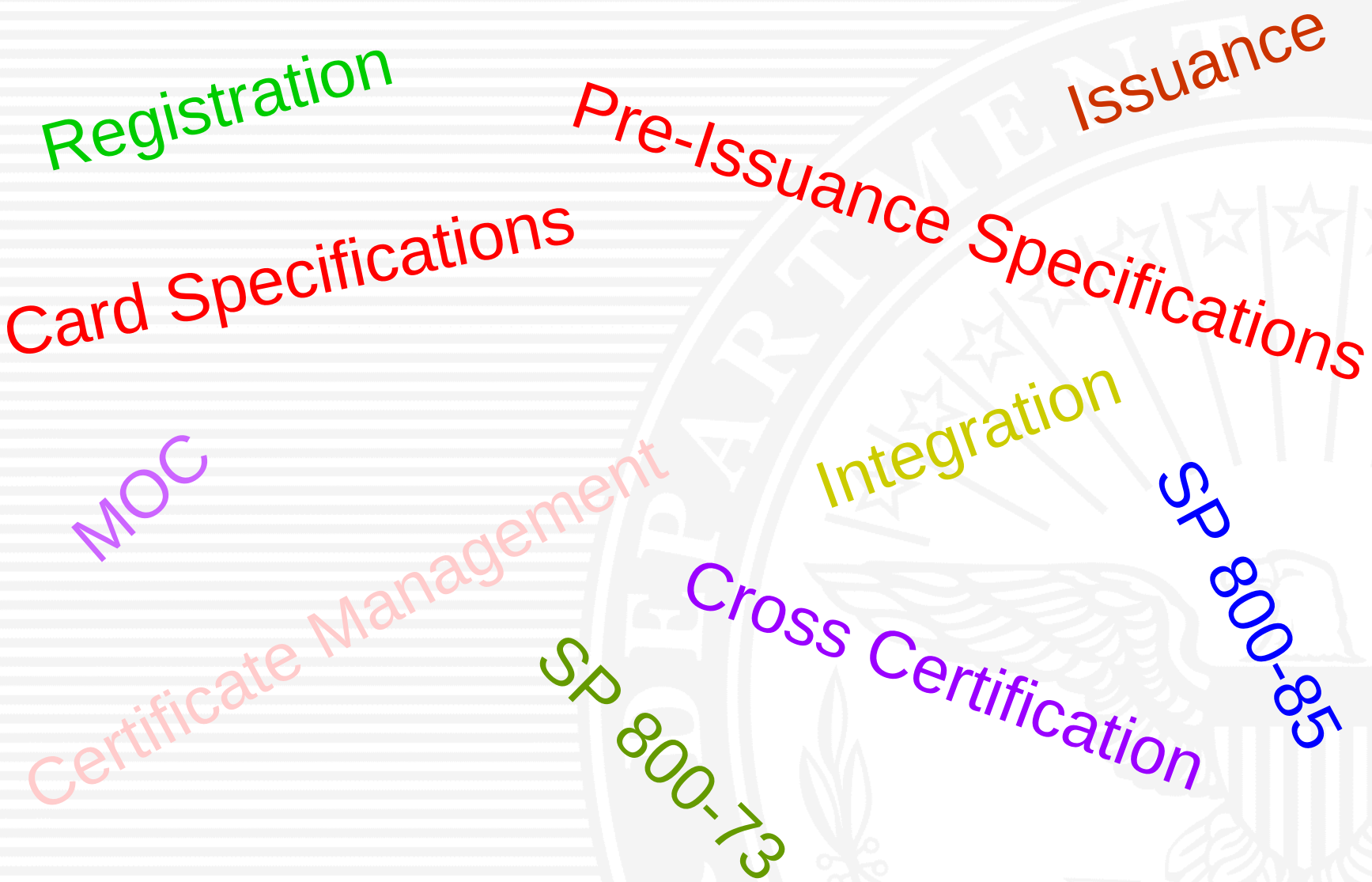
Key & Cardstock Management

- Federal Pre-Issuance Specification
- Key Management
- Cardstock Management

DoD's PIV Approach

- Architecture
- Lesson Learned

A focused discussion



Today's Goals

1. Identify the differences between the card specification and the Pre-Issuance Technical Requirements documents
2. Comprehend the basic requirements for implementing key management within your infrastructure
3. Identify the required pieces for drafting an organizational card issuance process flow

Not a "K-Mart" Process

- Advance planning and coordination is required for card platform and key management
  - Card products require Agency specific keys on each "batch" of cards
  - Agencies need to test cardstock and insure that it integrates within their infrastructure

Identity Management

- Not a building badge
- Nor an access badge
- Not just a personnel process - Security Process because of PKI

It is identity Management

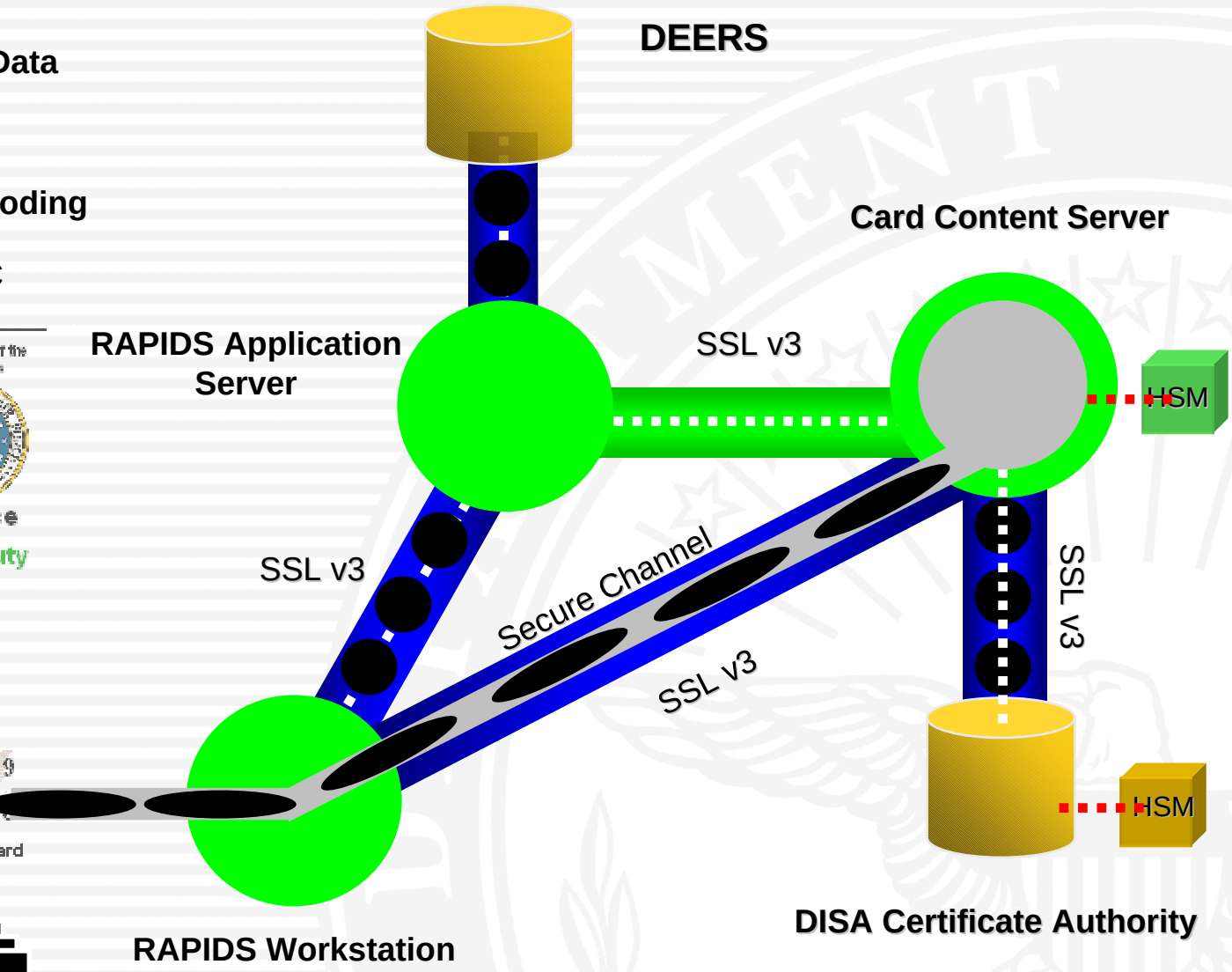
Create CAC

1) Request DEERS Data

2) Print CAC

3)Request CAC Encoding

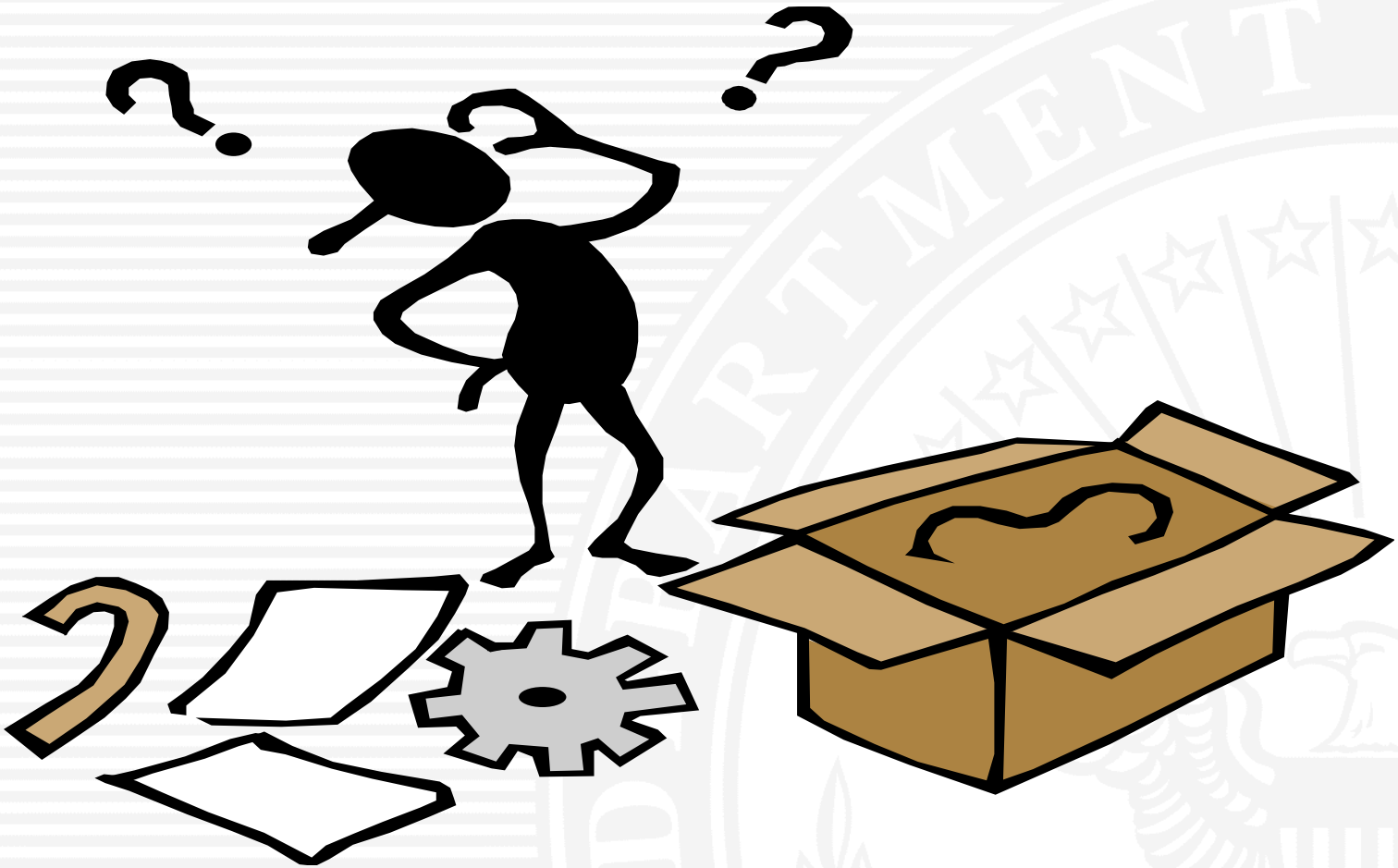
4) Synchronize CAC



House Analogy

- Card Specification is the blueprint for your home
- Pre-Issuance Specification contains the building codes and additional specs for the house
- Keys grant access to your house and the rooms of your house and Key Management is the lifecycle monitoring of those keys

Card and Pre-Issuance Specifications



What is the card specification?

- Identifies the card functionality and behaviors expected

- Outlines contractual requirements that must be fulfilled by the card
  - Industry/ISO standards
  - Physical attributes
  - Security
  - Card functionality

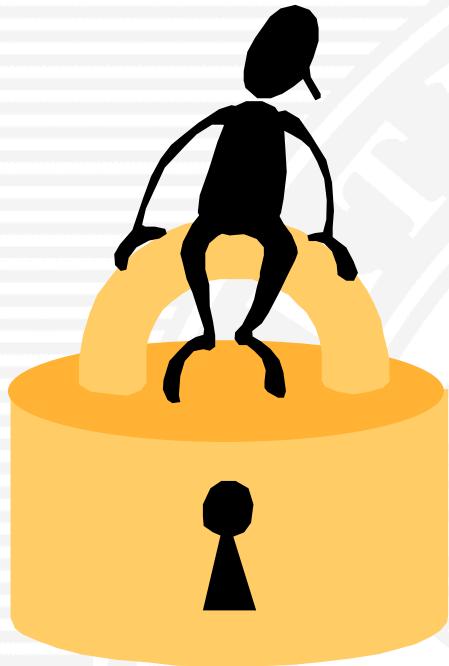
Why create a pre-issuance spec?

- **Documents requirements and expectations from Card Issuer to Card Manufacturer**
  - Key Management
  - Card Configuration Management
  - Cardstock Inventory Management
- **Provides consistent process across vendors, products, and agencies**
  - Outlines communication channels
  - Details shipping requirements
- **Outlines process for automated data transfer between Card Issuer and Card Manufacturer**

What criteria shapes the spec?

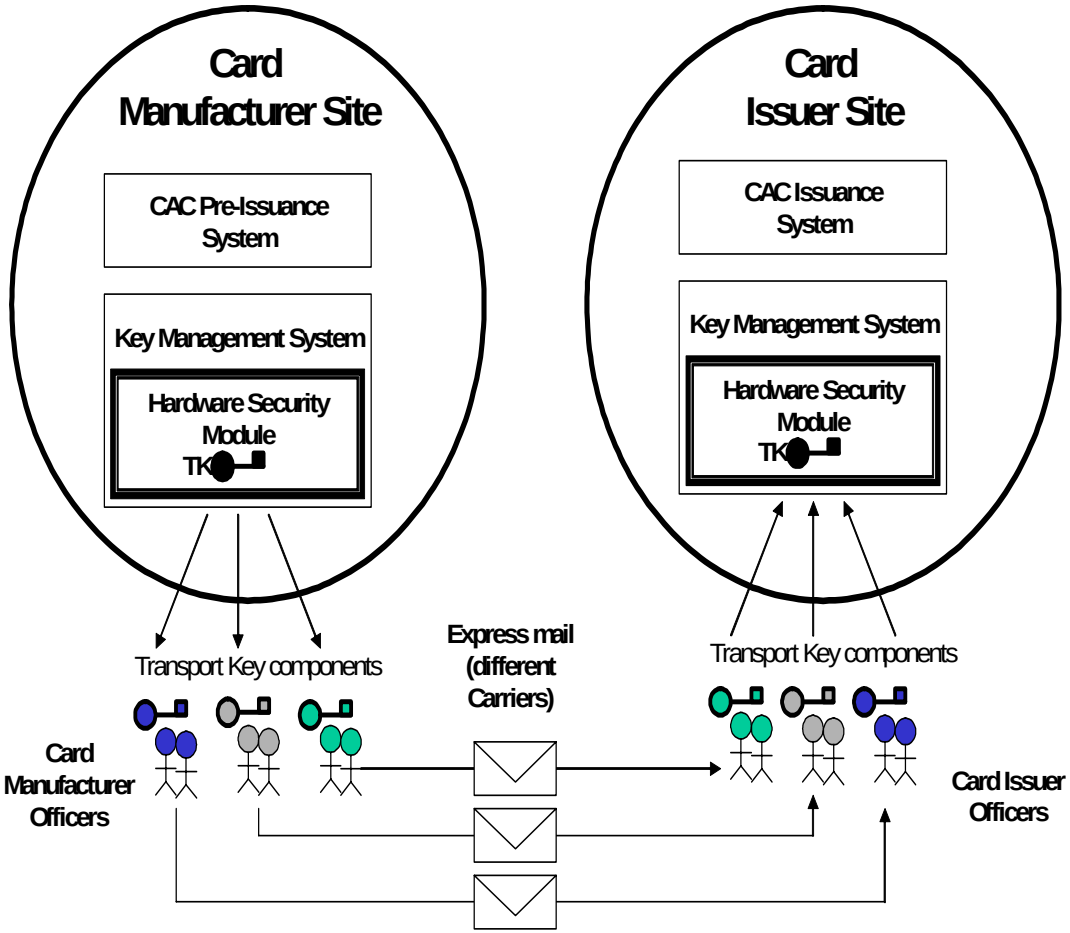
- **Card Usability**
  - Gather requirements from end users
  - Identify Long Range usage goals (both operational and technical)
- **Product Availability**
  - Verify availability of products that meet your end user requirements and mid-term usage goals
- **Card Management Process/System**
  - Spec outlines card issuer business and technical process
  - Spec clearly outlines process for sharing/storing card data between card issuer and card manufacturer

Key Management



What is Key Management ?

1. The process for transmitting non-PKI keys between card issuer and card manufacturer and
2. The internal administrative and security procedures used by the card issuer and card manufacturer to protect the keys and key components for the full lifecycle of those keys/key component



Why is Key Management important?

”__” cards compromised

- Each agency’s PIV cards will be used for asserting identity and for signing or encrypting data.
- If an agency’s keys are compromised those tokens may be compromised and the goals of HSPD-12 will not be met within that organization

How is Key Management accomplished?

- **Key Management Configuration**
  - Process for differentiating multiple keys across vendors, products, and customers
  - Required format and diversification algorithm for creation of keys
- **Key Exchange and Storage**
  - Security requirements (technical and operational) at card issuer and card manufacturer facilities
  - Process for administering key ceremonies

Key Management Configuration is…

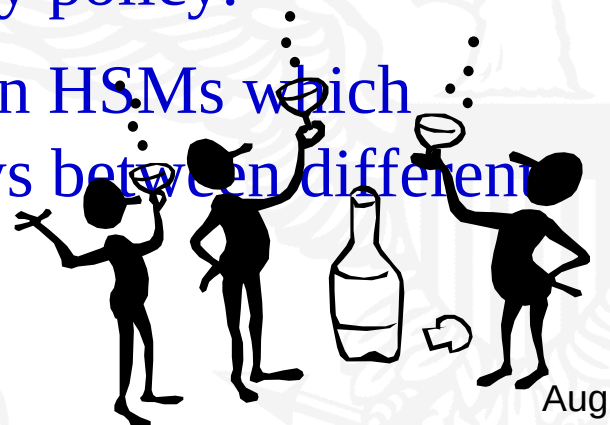
- Each organization defining the schema for each non-PKI key across their vendors and/or products
- Diversification
  - One master key plus the unique card data ensures that each card has a unique key to decrease the potential of card compromise. So if someone spends a lot of resource cracking the key on one card, they have only compromised one card and not all.

Key Exchange and Storage is…

- The basic security requirements (technical and operational) at card issuer and card manufacturer facilities
  - What physical security should be implemented at the card issuer and card manufacturer facilities
- Determining the personnel involved and the process procedures:
  - How keys are transmitted between card issuer and card manufacturer
  - Who is authorized to receive keys and participate in the key management process
  - What products are managed within the infrastructure
  - When new keys are introduced into the production environment
  - Where key management activities will occur

What is a Key Ceremony?

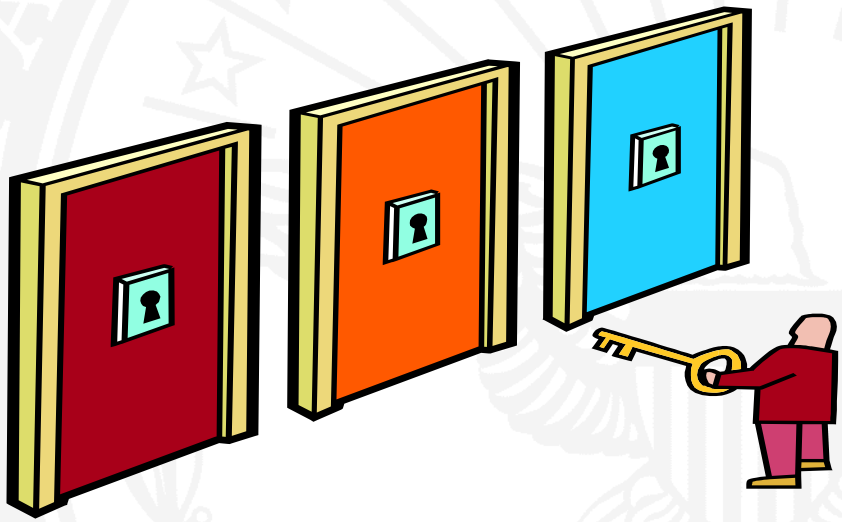
- Consists of the generation or import of a transport key composed of multiple key components (at least 3) in the Hardware Security Module (HSM) used to unwrap the Open Platform (OP) Master Keys.
  - Key is split into three components for separation of duty / shared control so that no one person has knowledge of the complete key.
- Each component is protected by one or two officers depending on the organization security policy.
- Allows for cloning of transport keys in HSMs which enables the transport of all master keys between different sites or HSMs.



House Analogy - Keys

Transport Keys grant access to your house

Master Keys grant access to various rooms within your house



Transport Keys

Transport keys are…..

- the unique key to transmit all “sub” keys between the card issuer and the card manufacturer
- 3DES-112 bit keys
- used to wrap/backup/export or unwrap/restore/import OP Master Keys
- are permanently defined in the HSMs

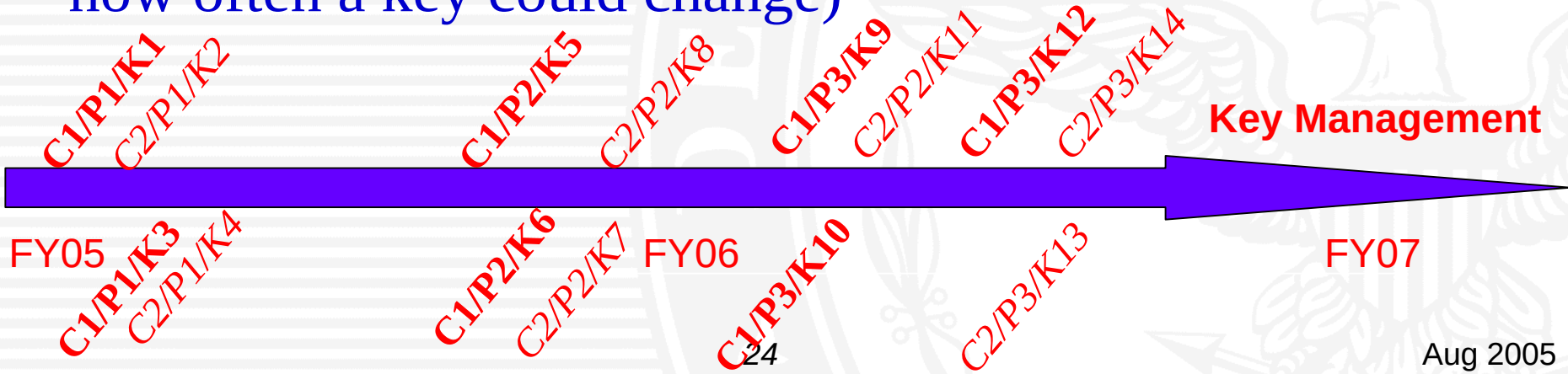
OP Master Keys

Master Keys are….

- "subkeys" transmitted by the card issuer and card manufacturer under the transport key and are used to "lock" specific batches of a card issuer's cardstock
- 3DES-112 bit keys
- groups of three master keys that correspond to the three CAC keys required to open a secure channel (MAC,ENC,KEK)
- permanently defined in the HSM

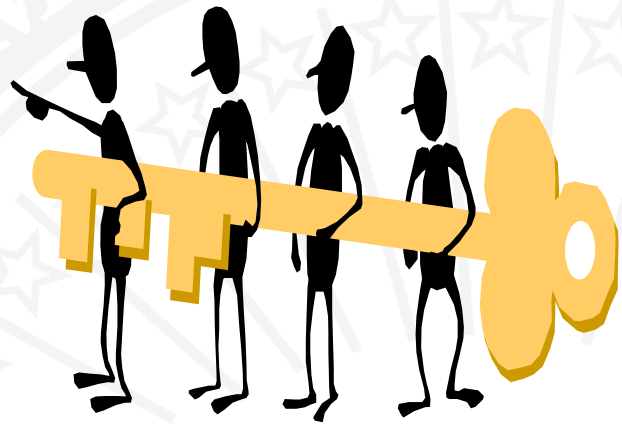
How is Key Management Implemented

- Multiple keys during program lifecycle
  - Lots of key (test, production, SDK, etc.)
  - Multiple vendors over program lifecycle
  - Annually changing keys (keeps exposure to compromise small)
  - New Vendor, Product end of life, etc.
- Example: Timeline (over the course of a few years how often a key could change)



Key Management Summary

- Key Management is a coordinated process between the internal and external teams at the card issuer and the card manufacturer
- Key Management Procedures and Policies are needed to ensure compliance is met and security is maintained
- Key Compromise leads to a broken trust chain and ends identity management



Cardstock Acceptance & Management

Why is acceptance testing important?

- Why you need to validate process - Products may have issues
  - Card product may not operate as advertised
  - Card provided may not meet original agreement – card body differences, physical printing, security devices,
- Acceptance testing is verification that products received meet the requirements

What is Cardstock Inventory Management?

- **Cradle to grave tracking of card products**
  - Requested by Agency and created by Card Manufacturer
  - Stored in vendor vaults
  - En route to Agency
  - Stored in Agency location (s)
  - Issued to Agency personnel
  - Lost, stolen, reissued, or damaged
  - Final destruction

What is Cardstock Inventory Management?

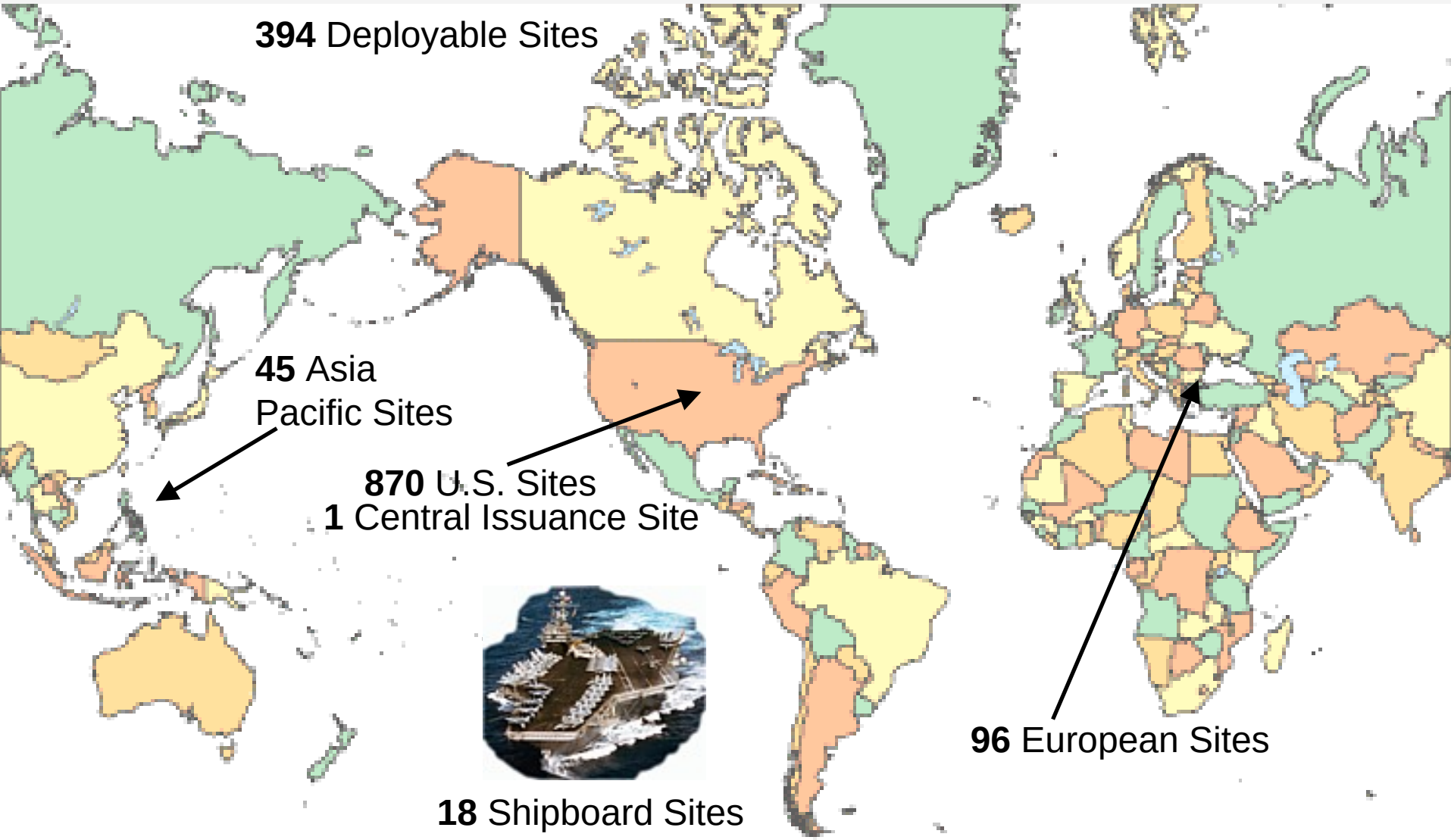
- **Process for requesting orders**
  - Personnel authorized to submit orders from Card Issuer to Card Manufacturer
  - Format and timeline for processing orders
- **Process for packaging of orders**
  - Labeling of individual stacks and cartons
  - US and International Shipping requirements
  - Preferred Carriers
- **Process for shipping of orders**
  - Authorized locations and personnel for order shipments
  - Format and timeline for processing Orders

What is the importance of Chip Management?

- Chips may change
- Chip space
- Applets

DoD's PIV Approach

DoD Distributed Issuance



1,425 Sites Deployed Worldwide as of June 2005

DoD's Identity Management

Nov. 1999	**Directed to implement smart card/PKI technology**
Oct. 2000	**First site issuing CACs**
Now	• **Issued over 8.5 million cards to DOD personnel/contractors** –3.2M of 3.5 M population have active CACs • **Over 2M readers/middleware deployed** • **Logical access – PKI** – Single sign on & PK-enabled websites growing • **Physical access – not so fast** –But with HSPD-12 – momentum growing • **Submitted on June 27, 2005, OMB mandated plan to become PIV compliant (plan approved)** –Deploying a dual-interface card utilizing V2 applets and new PIV applet at issuance or post issuance –Any new cards introduced must be backwards compatibility to cards previously fielded

	OCT 05 – PIV I	OCT 06 – PIV II
1. Identity Proofing	Breeder Documents	
	Investigations Completion and Reporting	
	Fingerprint Collection and Reporting	
	Training	Training
2. Topology		Policy Decisions
		Software Changes
		Advertisement – Internal and External
3. Authentication & Data Structure		Software/Hardware Changes
4. PKI		Two-way Federal Bridge cross certification
		Software/Hardware Changes
		Migration Strategy
5. Calls to Card		Software & Middleware Changes
		Card Platform changes
6. Biometrics		Fingerprints – collection, extraction, storage, and verification
		Facial image
7. Privacy	Assessment - Policy and Audit	Audit – incl. Contactless
8. Certification and Accreditation	System-wide C&A	Annual Verification

PIV Technical Changes

- Card Topology
  - Alter card topology and educate CAC Community (DoD end users, Customs/ Border Patrol, etc.)
- Card (Platform)
  - Pilot Dual Interface 64K contactless card in Q1/Q2 2006
- Card (Applets)
  - Develop, test, and FIPS certify New PIV compliant applets
- Document Capture/Proofing
  - Currently evaluating various vendor products
- Biometrics
  - Currently capture 2 fingerprints. Must upgrade equipment to include a 10 print capture device
- Camera
  - Seeking new equipment as DPI on current camera not PIV compliant.

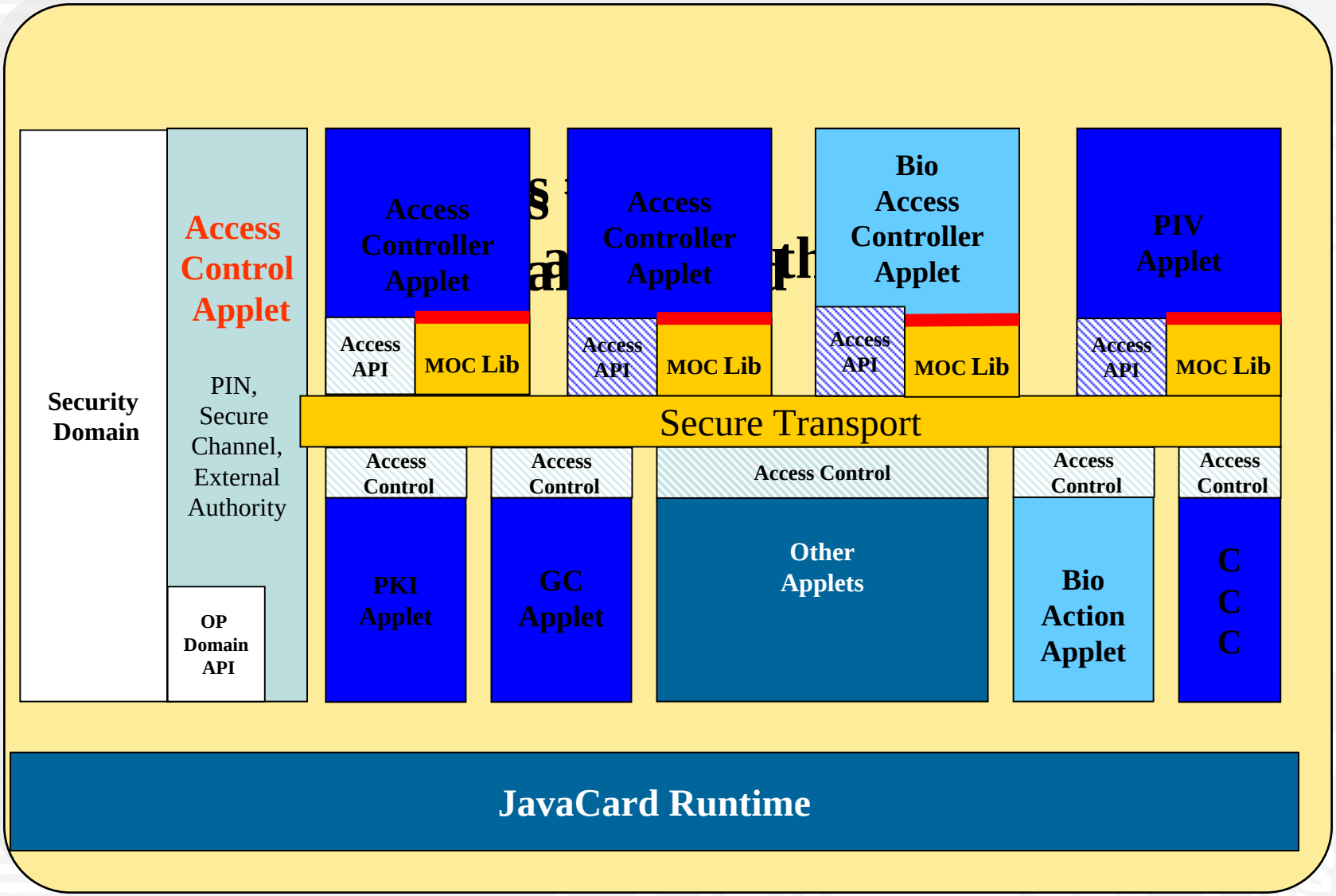
PIV Operational Changes

- Document Capture/Proofing
  - FIPS 201 requires breeder documents used to establish identity be captured, authenticated, and the images be available for retrieval at an issuance or physical access station. In addition, DoD has chosen to store the captured/authenticated images.
- NAC verification prior to issuance
  - Collection of 10 prints, storage of NAC results, and presenting results to Federal Partners.

Access Control Rule Changes

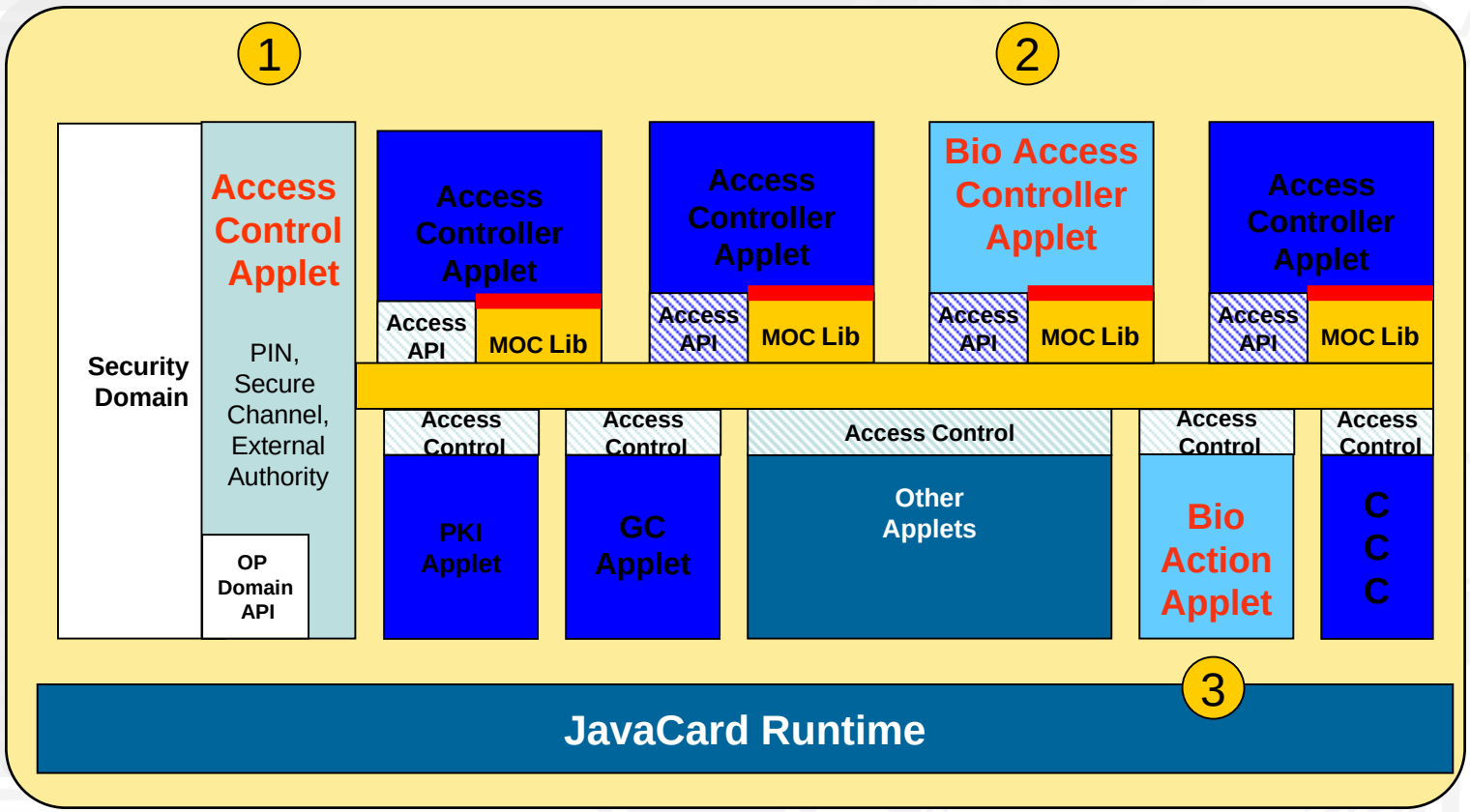
- Security enhanced by centralizing ACRs under issuer's control
- Biometrics used as an access control rule (ACR)for applets provides:
  - **Flexibility** to add much needed access control rules (ACR) to the current ones in use.
  - **Reuse** capability through the sharing of biometrics controllers and ACRs.

Architecture



Three Major Components

1. Access Control Applet
2. Biometrics Controller Applet
3. Biometrics Action Applet



Two Phase Process

Preparatory Steps

1. Load Access Control Applet
2. Load Bio Template
3. Load Bio Action Applet
4. Register Bio Action Applet Access Control Rules

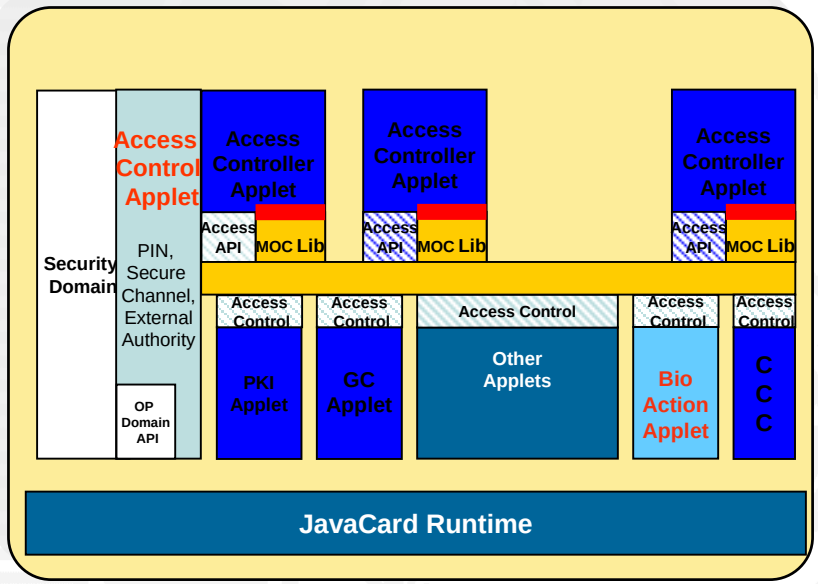
Action Steps (Bio Unlocks Door)

1. Card inserted in Bio Lock
2. Bio Lock signals for Bio Capture and transmits to Access Control Applet (ACA)
3. Access Control Applet compares captured bio to stored bio on card and set the access control state for bio controller
4. Bio Lock calls Bio Action Applet on Card
5. Bio Action Applet checks access control rule in ACA.
6. ACA state is determined to Yes and tell Bio Action Applet.
7. Bio Action Applet release Bio Lock “Unlock Command”
8. Door opens

Phase One: Preparation

Preparatory Steps

1. Load Access Control Applet
2. Load Bio Template



Phase One: Preparation

Preparatory Steps

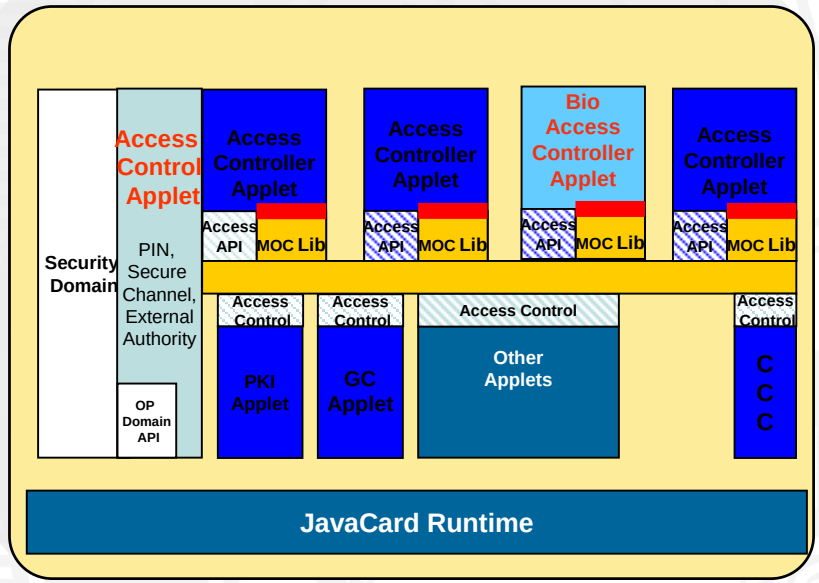
3. Load Bio Action Applet

4. Register Bio Action Applet Access Control Rules

The Applet

The Rule

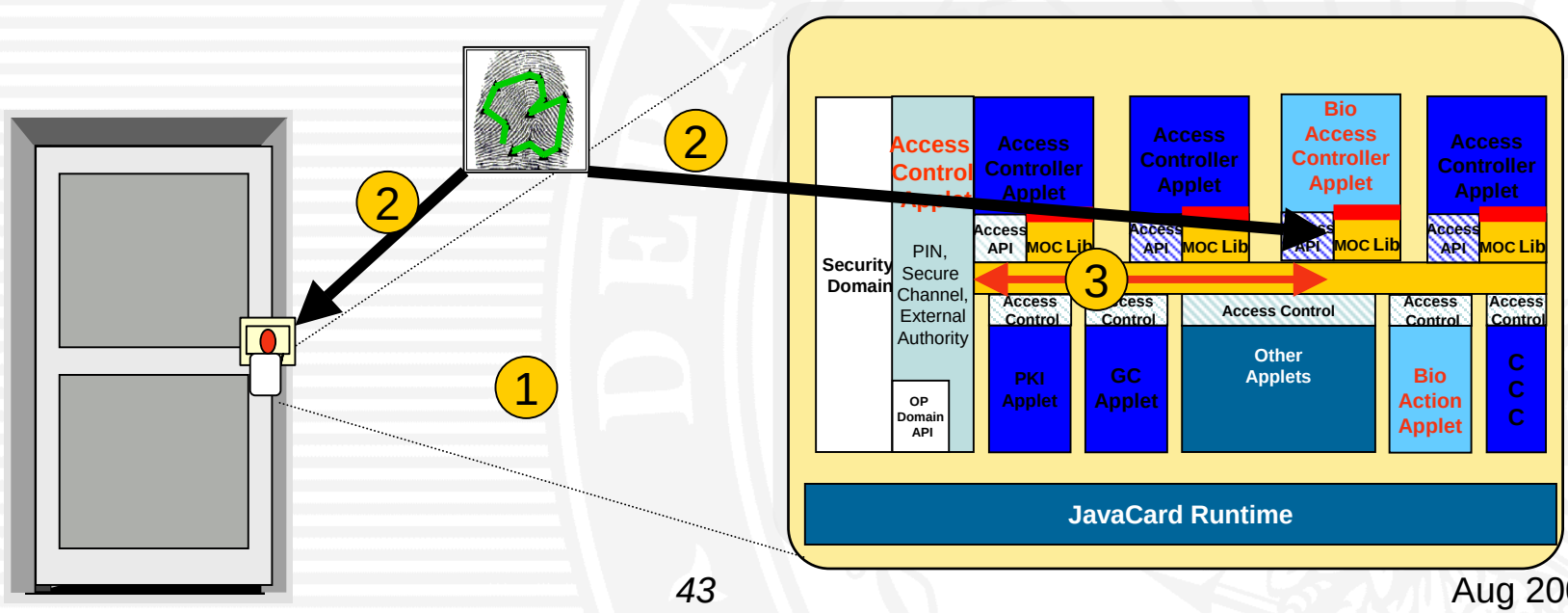
Bio 1 only



Phase Two: Usage

Action Steps (Bio Unlocks Door)

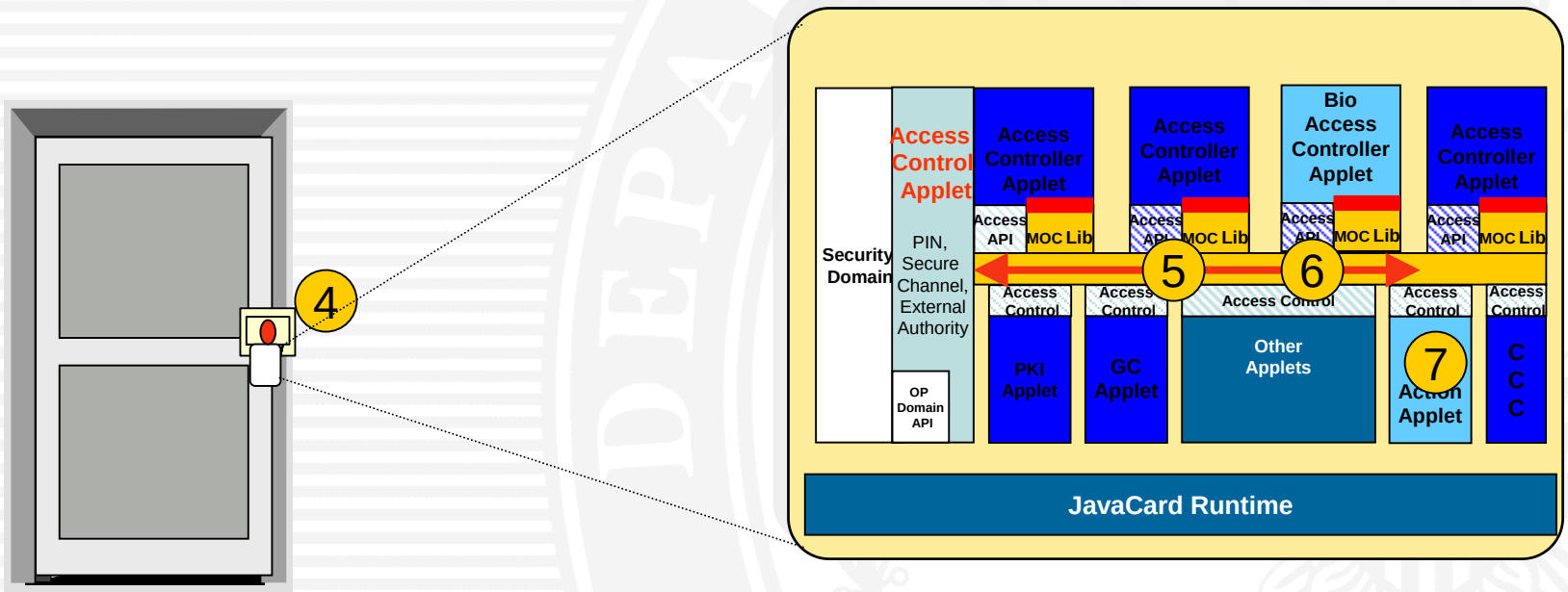
1. Card inserted in Bio Lock
2. Bio Lock signals for Bio Capture and transmits to Access Controller Applet (ACA)
3. Access Control Applet compares captured bio to stored bio on card and set the access control state for bio controller



Phase Two: Usage

Action Steps (Bio Unlocks Door)

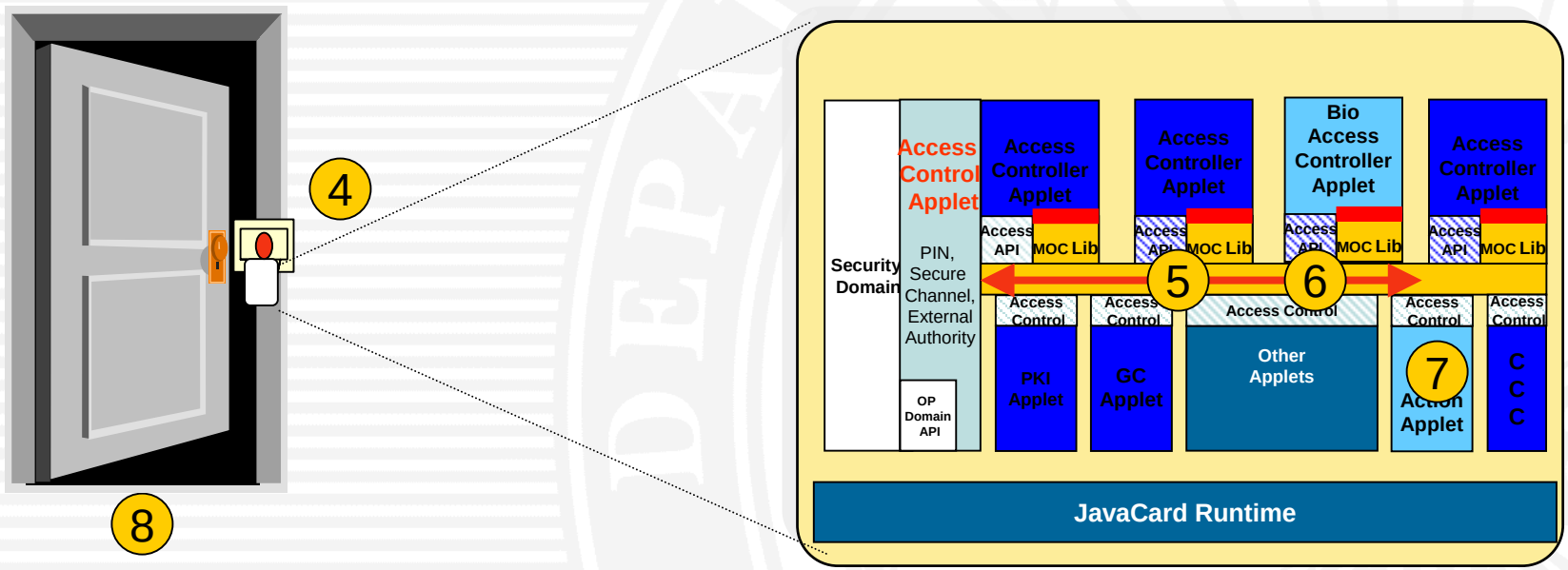
4. Bio Lock calls Bio Action Applet on Card
5. Bio Action Applet checks access control rule in ACA.
6. ACA state is determined to Yes and tells Bio Action Applet.



Phase Two: Usage

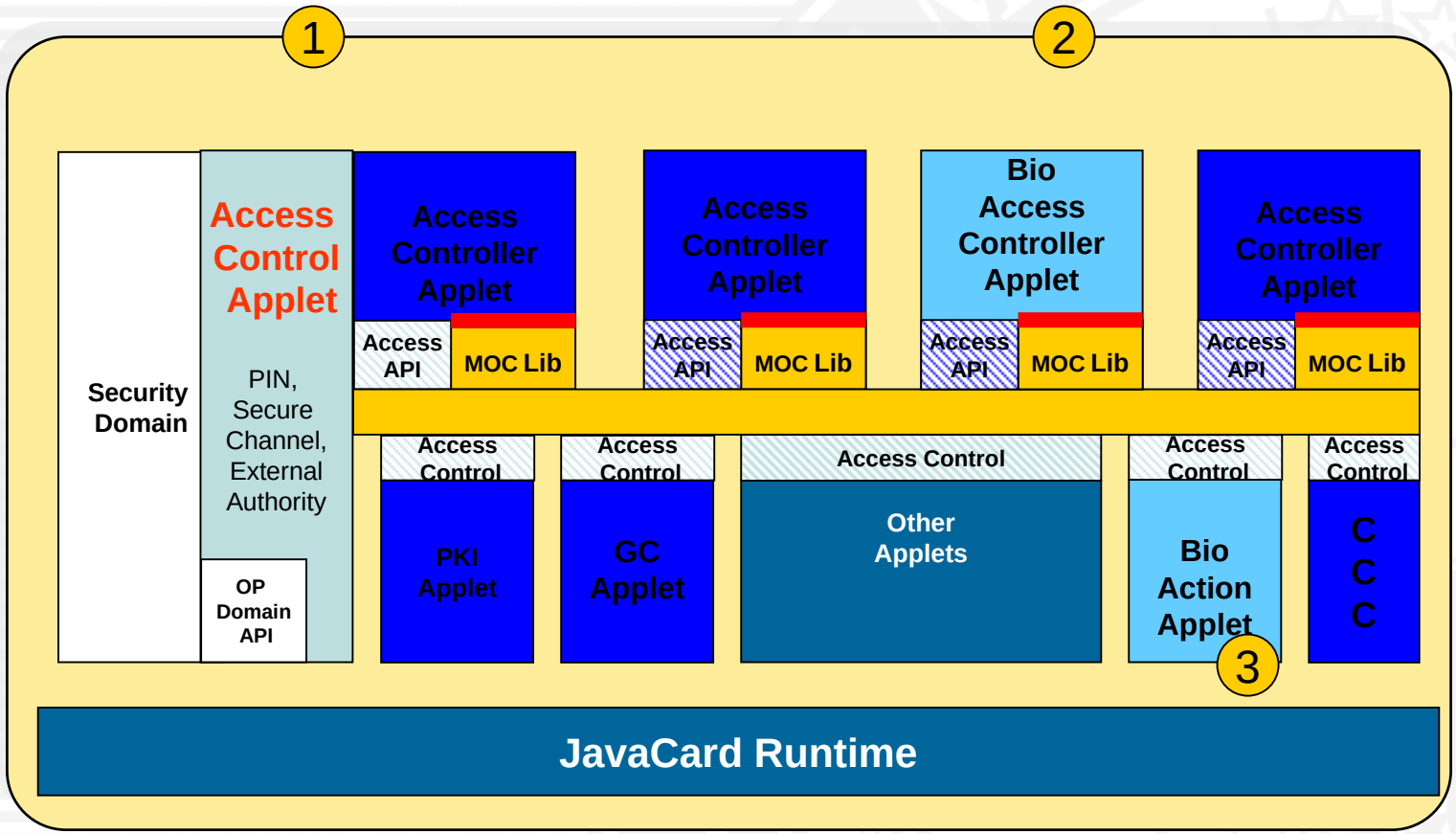
Action Steps (Bio Unlocks Door)

7. Bio Action Applet release Bio Lock “Unlock Command”
8. Door opens



Summary

Flexibility to add much needed access control rules (ACR).
Reuse capability through the sharing of biometrics controllers and ACRs.

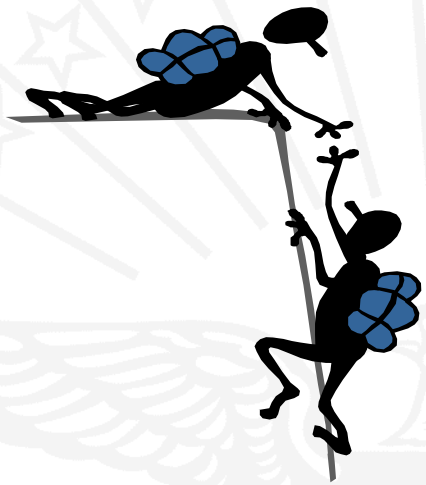


Summary

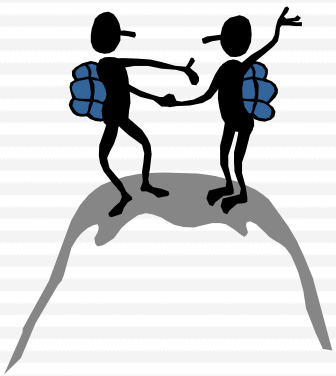
- **Pre-Issuance Specification is the building block for both key and cardstock management**
  - **Provides guidance to the card manufacturer on what will be ordered and the accepted format for processing the order**
  - **Provides guidance to the card issuer implementation team and the card manufacturer team on what the key management procedures are**
- **Key Management is critical as a compromised token weakens an organization's identity management architecture**

Summary

- **Meeting the requirements of HSPD-12/PIV will be a strenuous process for all involved**



- **Let's leverage past lessons learned and implement specifications together**

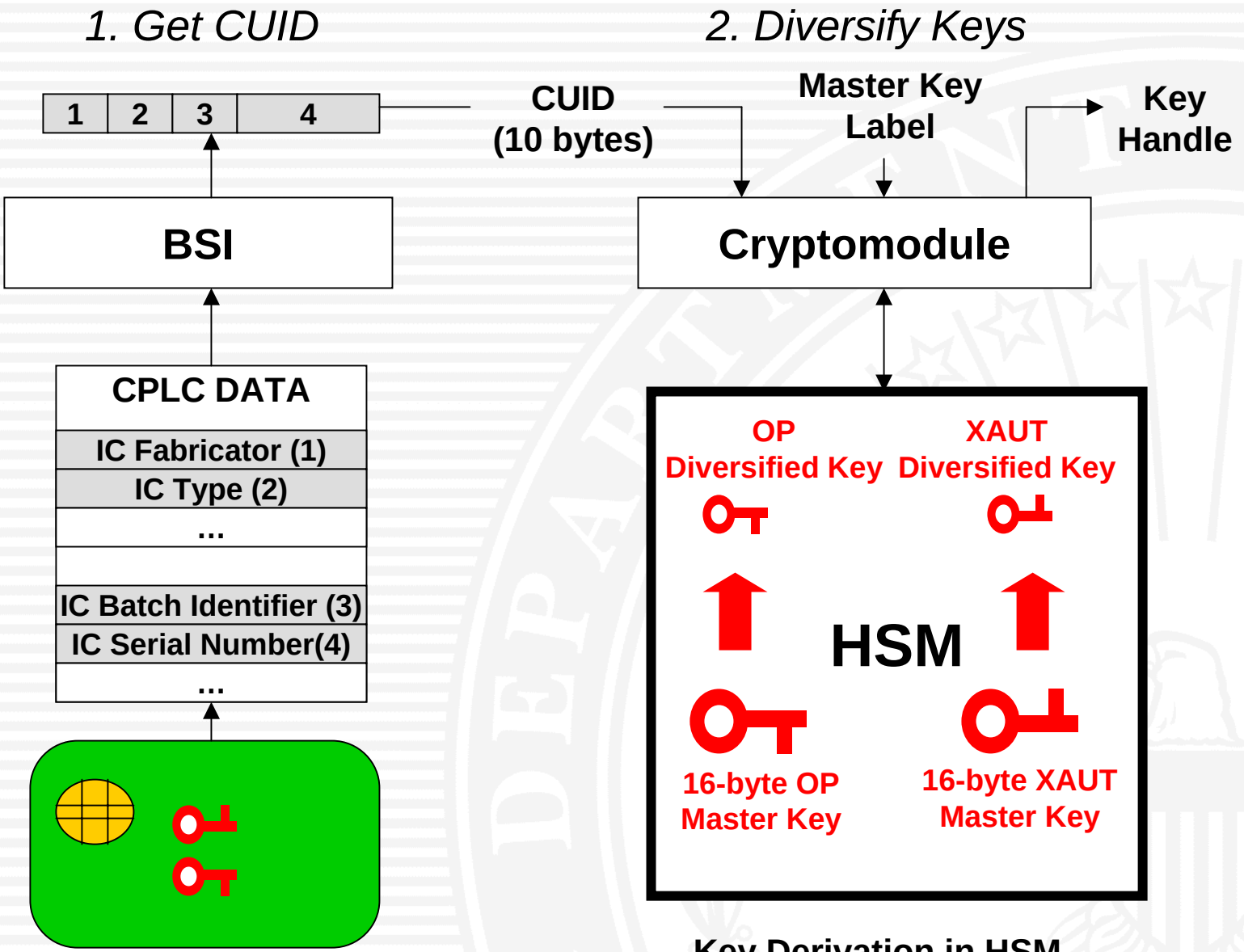


- **So we can all experience success together**

Questions?

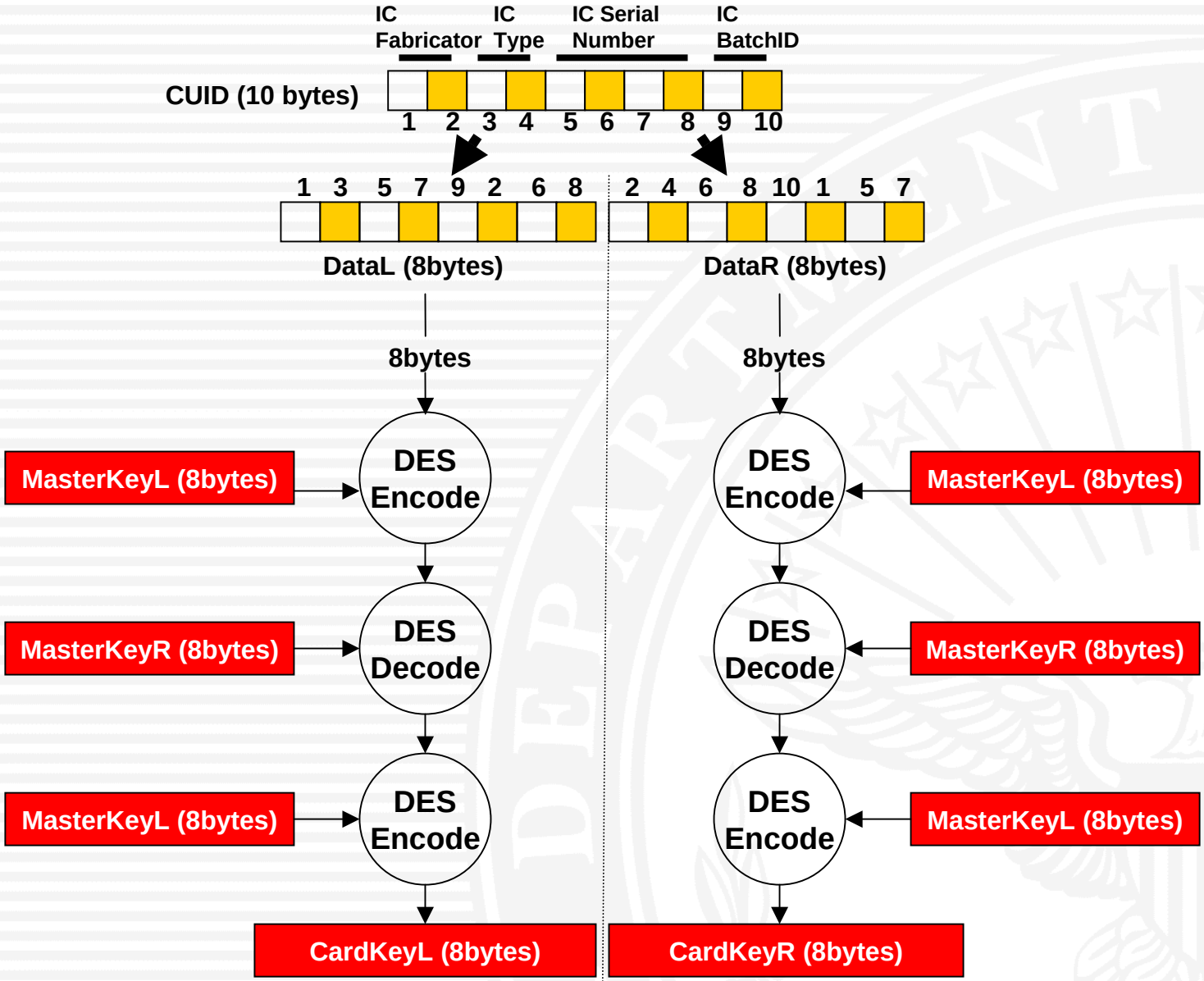
Backup slides

CAC Key Diversification (1)



Key Derivation in HSM

CAC Key Diversification (2)



Key Management System