Deloitte.

FIPS 201 and Physical Access Control

ASIS International
National Capital Chapter
Government and Industry Technology Seminar

Michael Kelley
ERS Specialist Manager
November 11, 2009

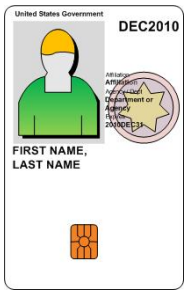
"…require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities…"

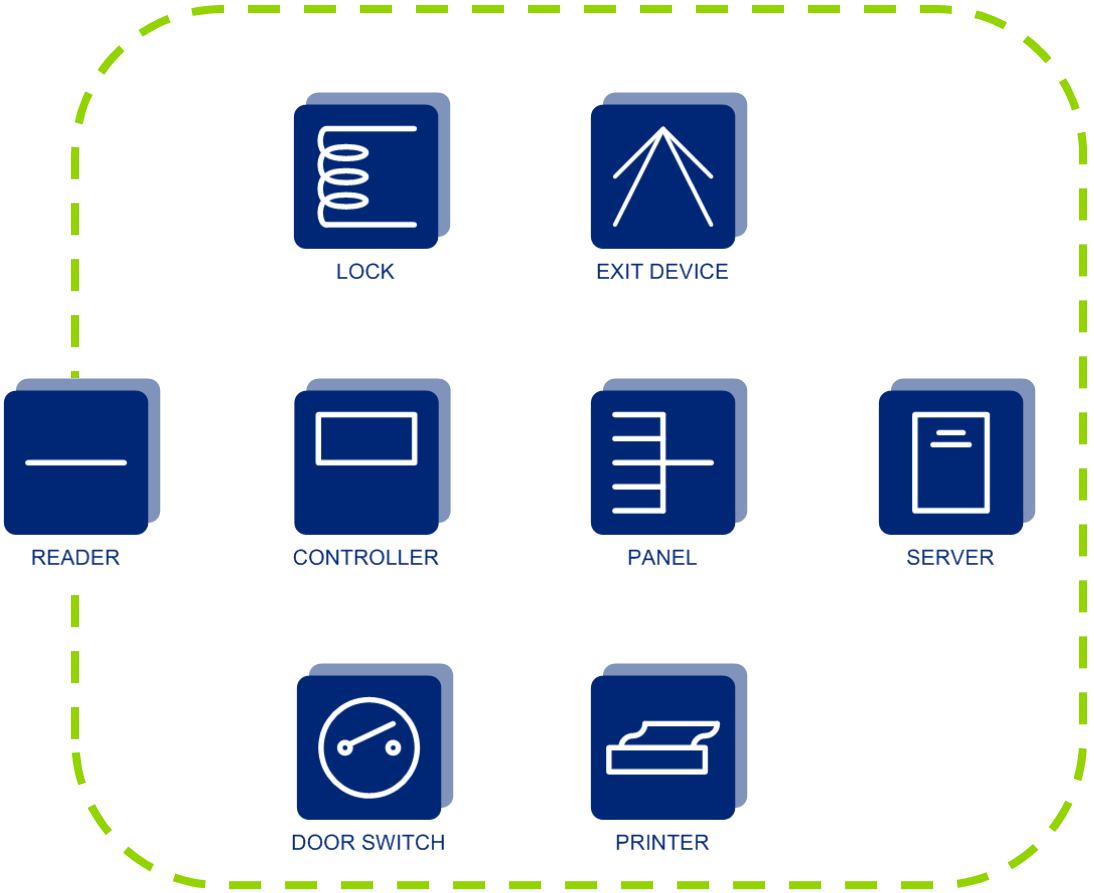
- HSPD 12, August 2004

"In physical access control systems where the readers are not connected to general purpose desktop computing systems, the reader-to-host system interface is not specified in this standard."

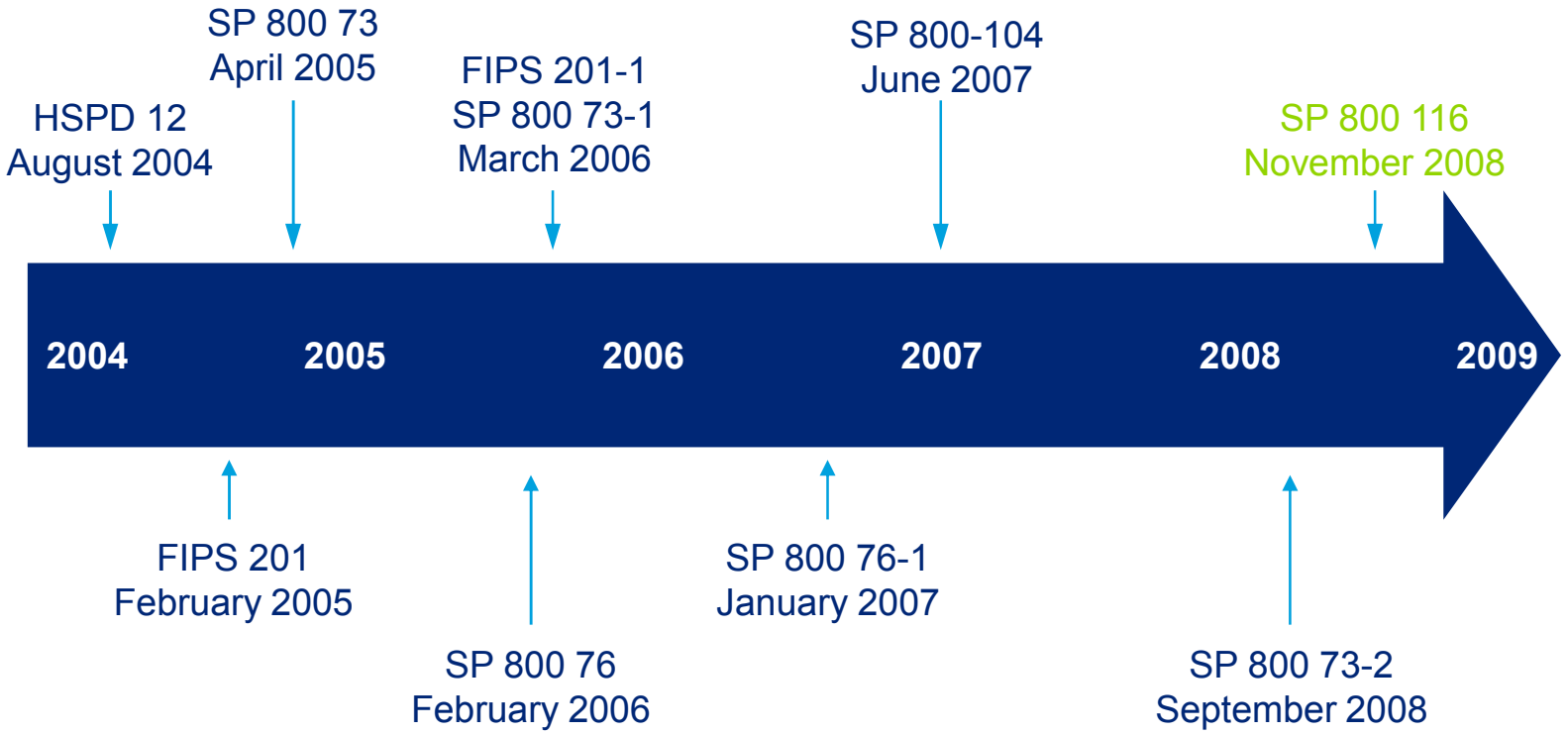
- FIPS 201, February 2005

FIPS 201 PACS Requirements



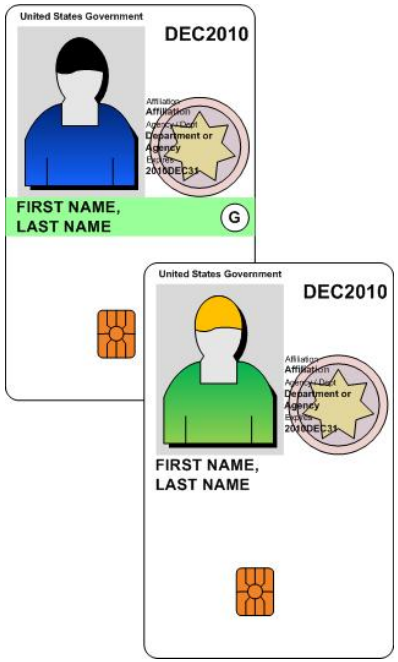


HSPD-12 Related Standards



Card Changes

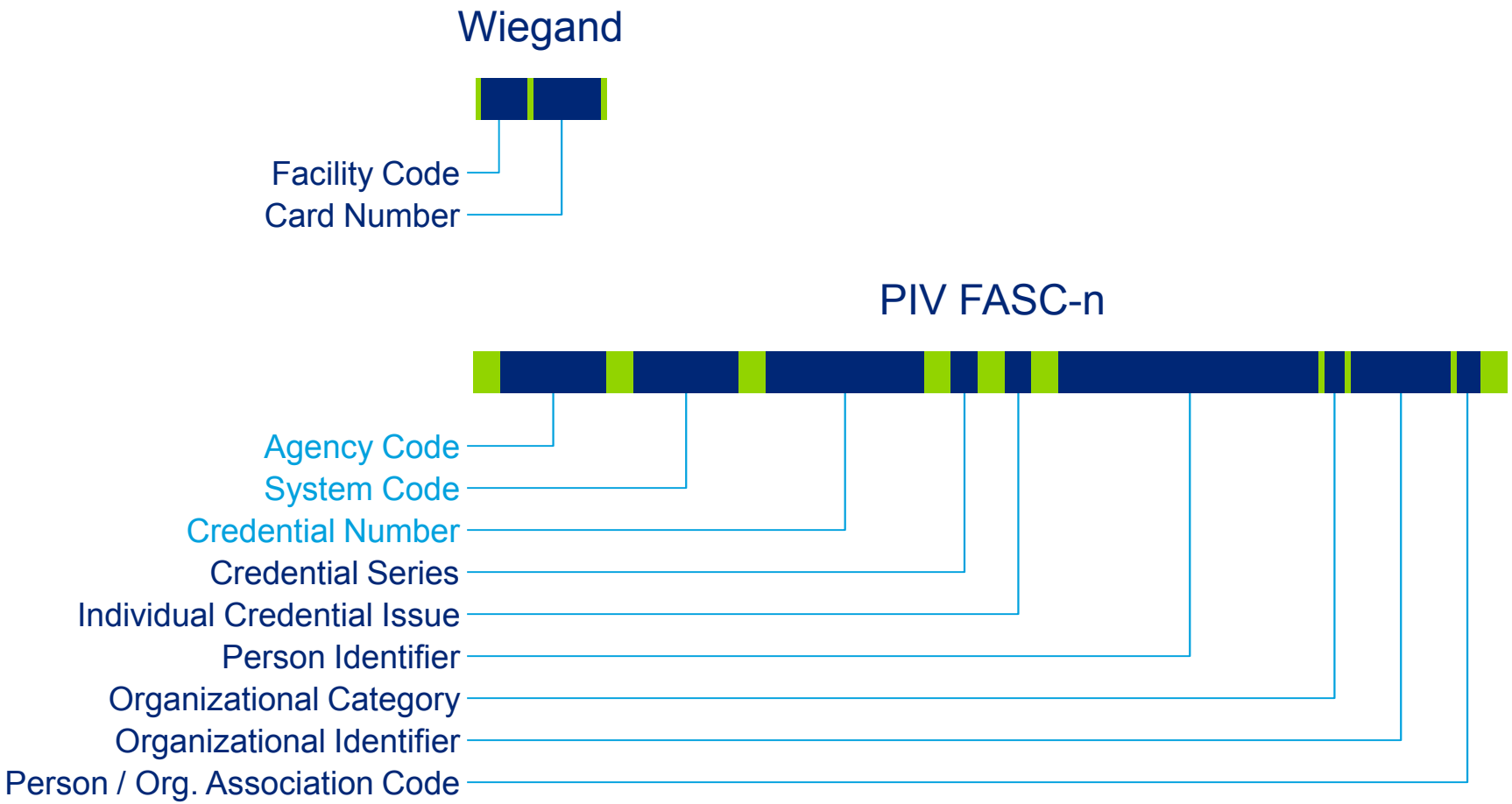
- Legacy
  - Visual topology was not standard
  - Multiple technologies and formats
  - No direct support for biometrics
  - Cards are read only
  - No support for cryptographic functions
    - No protection from unauthorized disclosure or modification
    - Card is not bound to the cardholder
- PIV
  - Seven standard items; five on front, two on back
  - Standard technology and format
  - Biometric templates on the card
  - Bi-directional communication between cards and readers
  - Supports cryptographic functions
    - Access rules and digital signatures
    - Card is bound to card holder



PIV Data Model

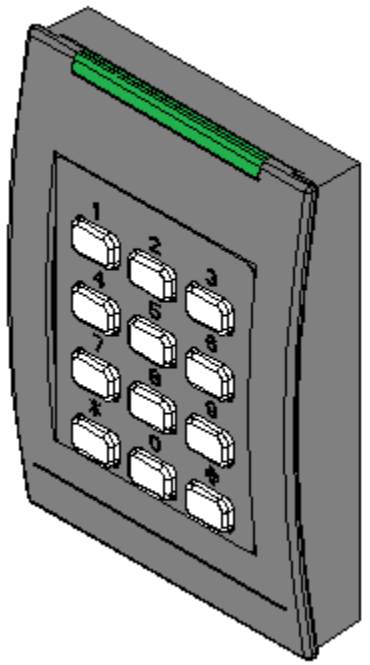
	Access Rule	Contact / Contactless	Mandatory / Optional
Card Capability Container	Always	Contact Only	Mandatory
Cardholder Unique Identifier	Always	Both	Mandatory
PIV Authentication Certificate	Always	Contact Only	Mandatory
Cardholder Fingerprints	PIN	Contact Only	Mandatory
Security Object	Always	Contact Only	Mandatory
Cardholder Facial Image	PIN	Contact Only	Optional
Printed Information	PIN	Contact Only	Optional
Digital Signature Certificate	Always	Contact Only	Optional
Key Management Certificate	Always	Contact Only	Optional
Card Authentication Certificate	Always	Both	Optional
Discovery Object	Always	Both	Optional

Card Numbers



Reader Changes

- Legacy
  - One reader supports one technology / format
  - Configured by manufacturers
  - Longer read ranges
  - Fast card reads
- PIV
  - Multi technology readers
  - Flashable firmware
  - Shorter read ranges
  - Slower read times



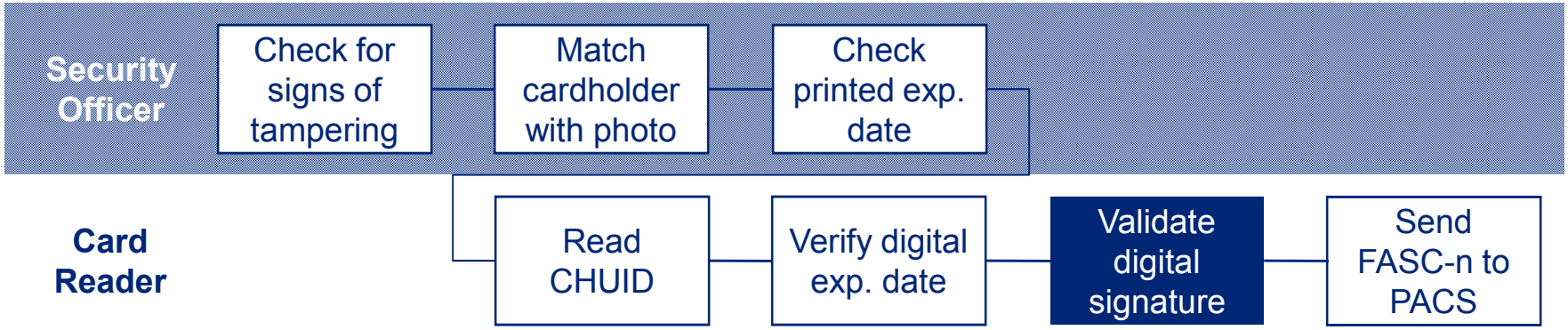
Authentication Mechanisms

Legacy	FIPS 201-1	NIST SP 800-116	
• Visual	• Visual	• Visual & CHUID	• PKI
• Card number	• CHUID	• CAK	• BIO-A
• PIN	• Biometric	• BIO	• CAK + BIO(-A)
• Biometric	• PKI		

Objectives:

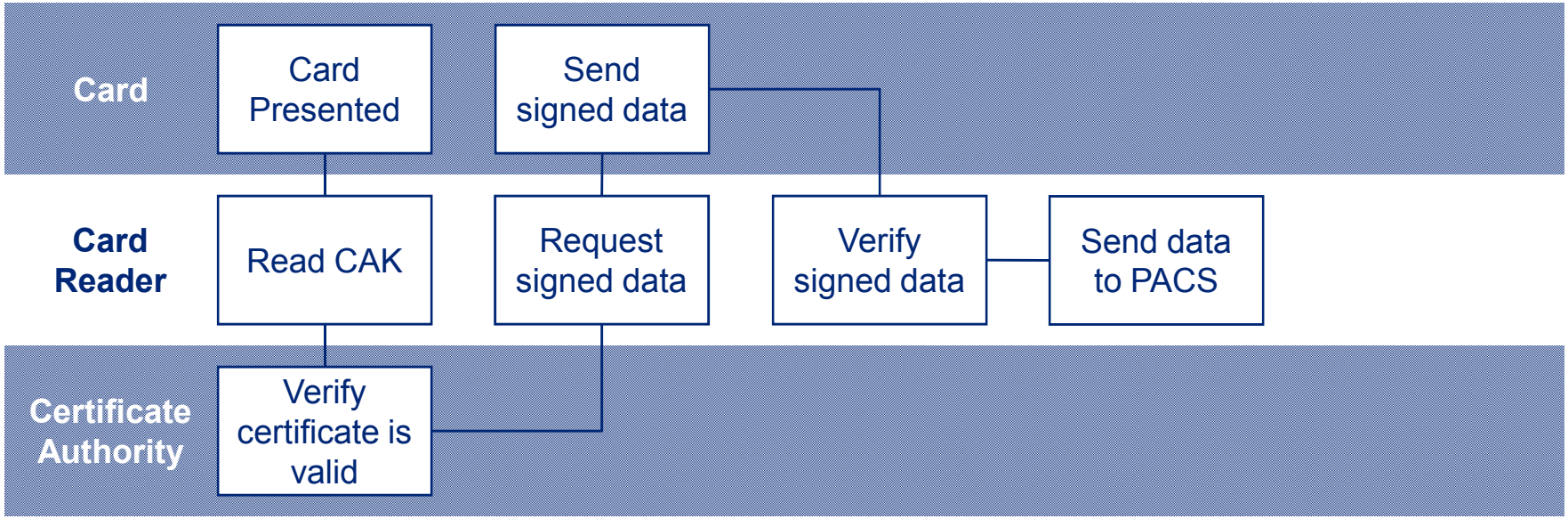
- Cardholder Validation
  - Establish person presenting the card is the person it was issued to
- Card Validation
  - Verify that the PIV card is authentic
- Credential Validation
  - Verify one or more credentials on the PIV card are authentic

CHUID and Visual Mechanism



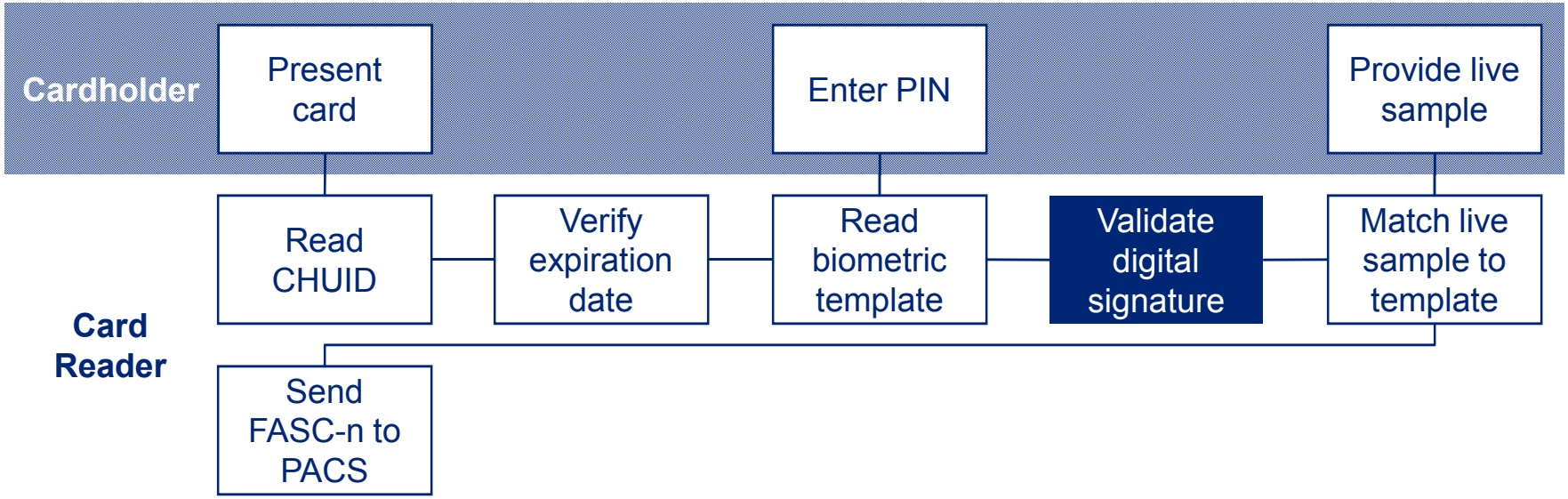
- Single factor authentication
  - Something you have
- Used to pass from Unrestricted to Controlled areas
- Digital signature validation is optional
  - Data could be electrically cloned if signature is not checked
  - Security Officer performance becomes more important

Card Authentication Key Mechanism



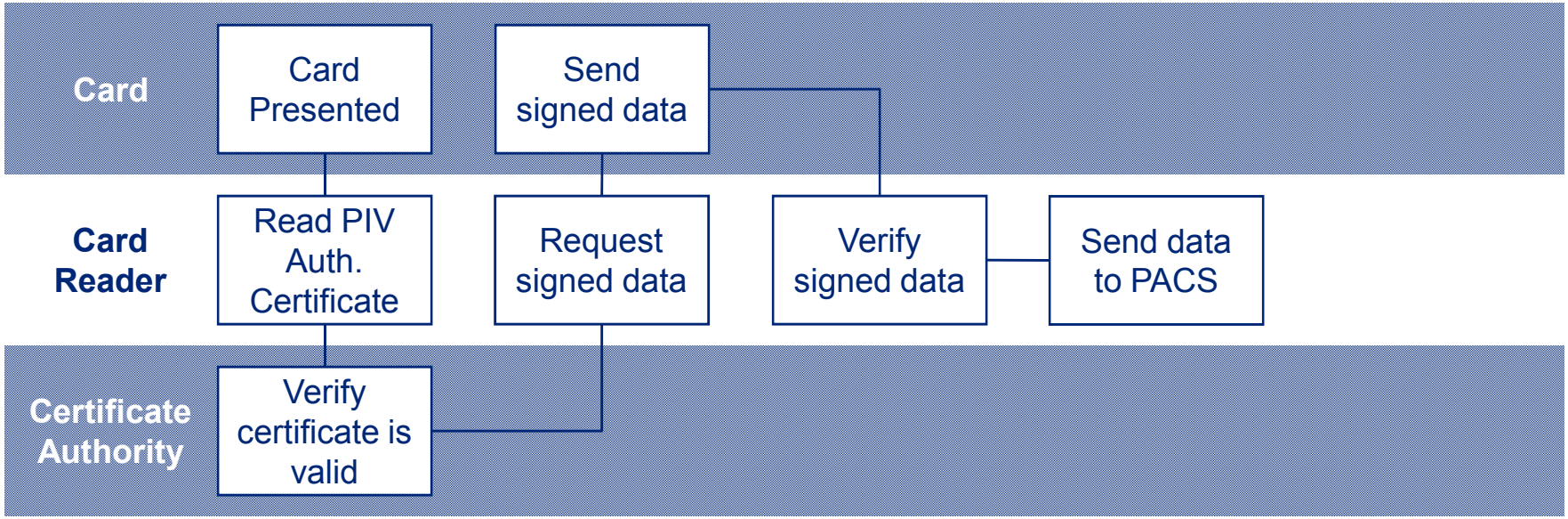
- Single factor authentication
  - Something you have
- Used to pass from Unrestricted to Controlled areas
- Presence and format not standardized
  - Not interoperable
  - Asymmetric implementation shown

Biometric Mechanism



- Two factor authentication
  - Something you are, something you know
- Used to pass from Controlled to Limited areas
- Digital signature is optional
  - Data could be electrically cloned if signature is not checked

PIV Authentication Key Mechanism

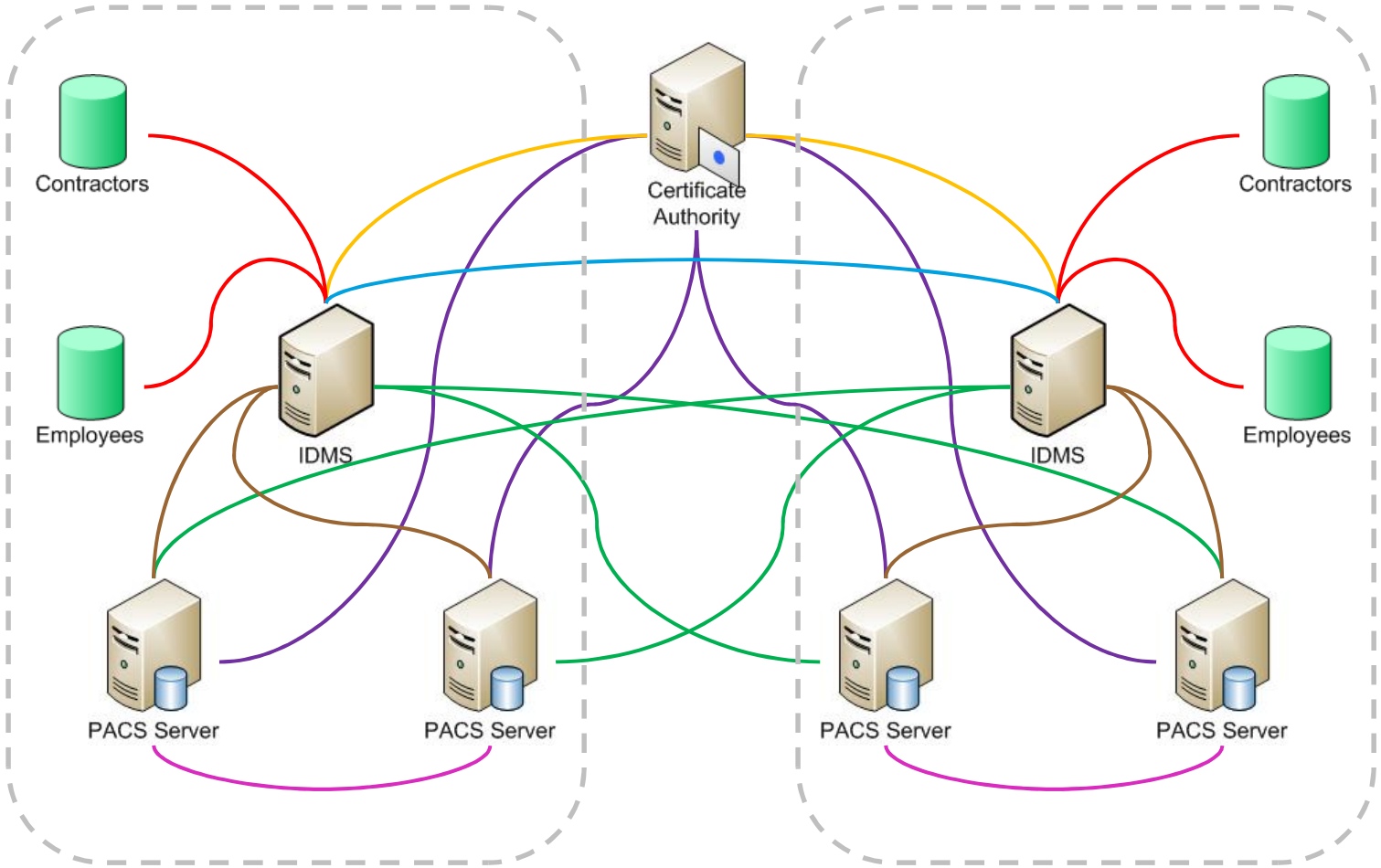


- Two factor authentication
  - Something you have, something you know
- Used to pass from Controlled to Limited areas

Changes to Systems, Products, Procedures and Policies

- Accommodate larger card numbers
- Move devices to the edge
- Increased data capacity at the reader
- Move towards enterprise systems
- Multi-technology readers
- Workflow management
- Card issuance
- Privilege management
- Identity management
- Trust Models
- Information security
- Lifecycle management

FIPS 201 Enterprise



- Identity attributes fm authoritative sources
- Certificate information for lifecycle management
- Back end attributes between issuing authorities
- Agency cardholder and card attributes to PACS
- OGA cardholder and card attributes to PACS
- Certificate status to PACS
- PACS information between agency facilities

Summary

- HSPD-12 standards for PACS are still developing
  - Special Publication 800-73-3 scheduled late 2009 / early 2010
  - FIPS 201-2 scheduled for 2010
- PACS systems and components will continue to evolve in response
  - Support for additional authentication mechanisms
- Information is no longer restricted to the PACS stovepipe
  - PACS will be gradually integrated into the enterprise
  - Increased focus on information security, integrity and availability
- New policies and procedures
  - Use cases
  - Trust models