

Use of Smart Cards in Physical Access Control Systems

Ron Martin, CPP



The presenter gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this presentation. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the government, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.



Security System Gateway

*“The implementation of HSPD-12 will be facilitated via the Physical Access Control System, (PACS). The **PACS must be the gateway to the backend cyber requirements** of an agency’s implementation. PACS will be a fully integrated and tightly coupled physical and logical access control system. These systems will provide federal agencies and their support contractors with a robust set of security safeguards and countermeasures. These environments must be capable of protecting federal information systems, the information stored, processed and transmitted by these systems and the facilities in which the systems reside. These systems will be deployed on Local as well as Wide area networks. **The PACS will have the capability to operate in harmony with a centralized physical security information management system.**”*



Advancing Security Worldwide™

Components of an Identity Management Process

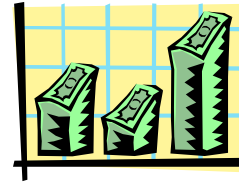
Policy,
Planning,
Politics and
Management



Defining
functional/business
requirements



Defining
Business Architecture



Determining budget
requirements



Reviewing
policies



Determining laws,
regulations, mandates
to be followed



**Identity Management is a broad capability
and requires an integrated solution**



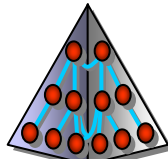
Creating new
policies where
needed

↑
80%

↓
20%
Technology



Hardware/
Software



Storage



Entity
Management



Credentialing



Access
Management



Application
Integration

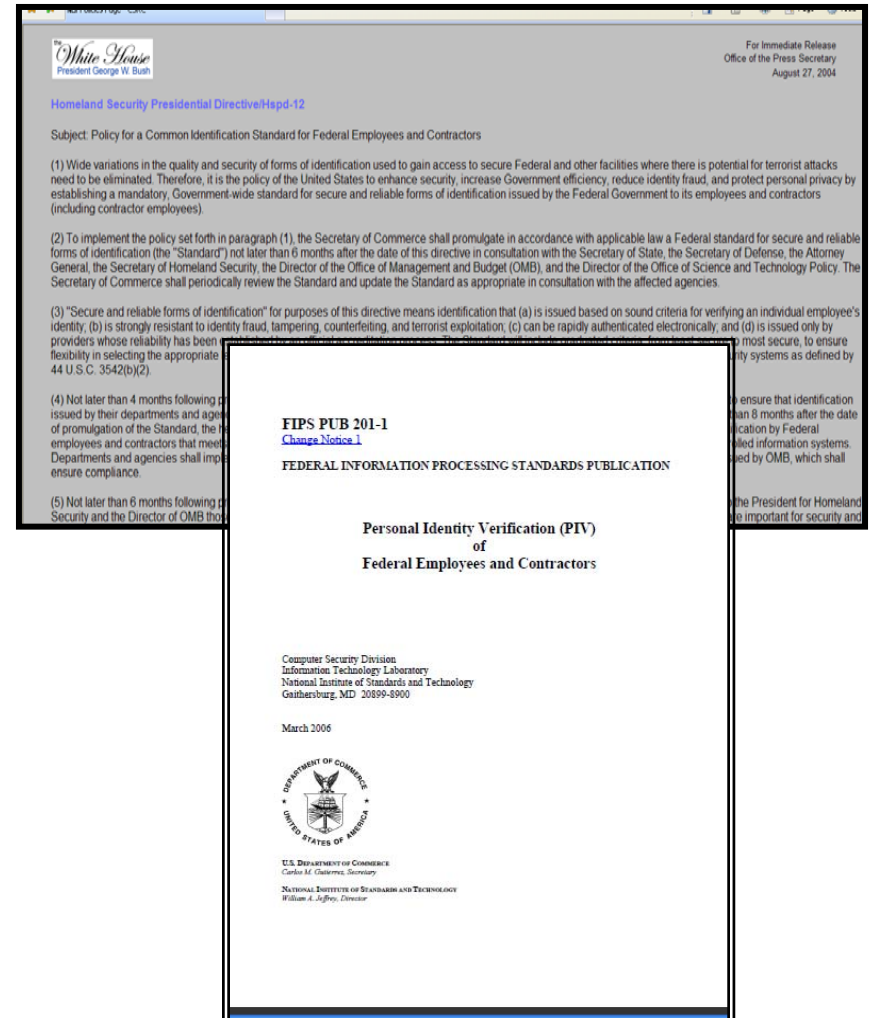


Facilities

IDMS Services

HSPD-12 and FIPS 201 Background

- Homeland Security Presidential Directive 12, issued *08/2004*:
 - Requires secure and reliable identification (for Federal employees & contractors) that:
 - Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
 - Can be rapidly authenticated electronically
- FIPS 201 establishes the standard for Personal Identity Verification (PIV) Cards





Homeland Security Presidential Directive 12

HSPD-12

What is it?

The establishment of a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

FIPS 201-1 The Standard

PIV-1

Control Measures

PIV-2

Usage

<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

The views of this session are those of the presenter and not those of the US Government.

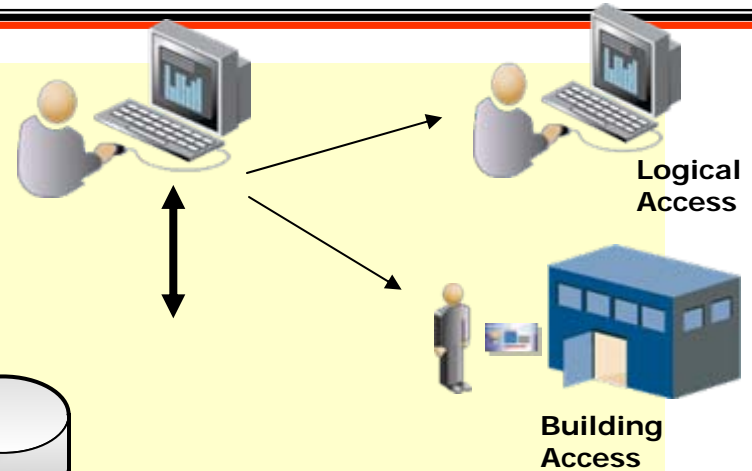
Migrating from PIV-I to PIV-II

IDMS easily links to enterprise Card Management System to incorporate both Physical and Logical Access Control.

PIV-II

Central Card Management

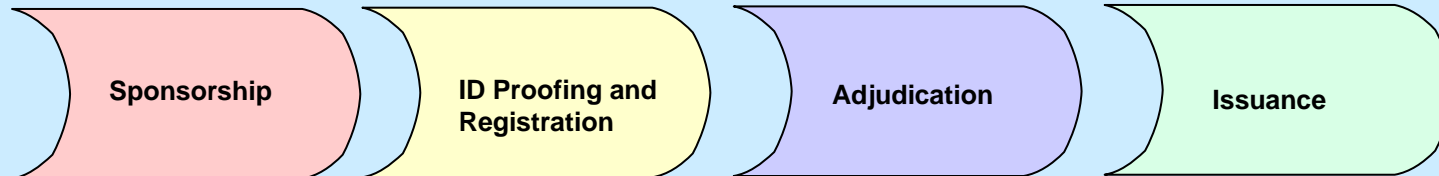
USAGE



PIV-I

Identity Management System
IDMS

Control Measures



HSPD-12
FIPS 201

Systems

Technology

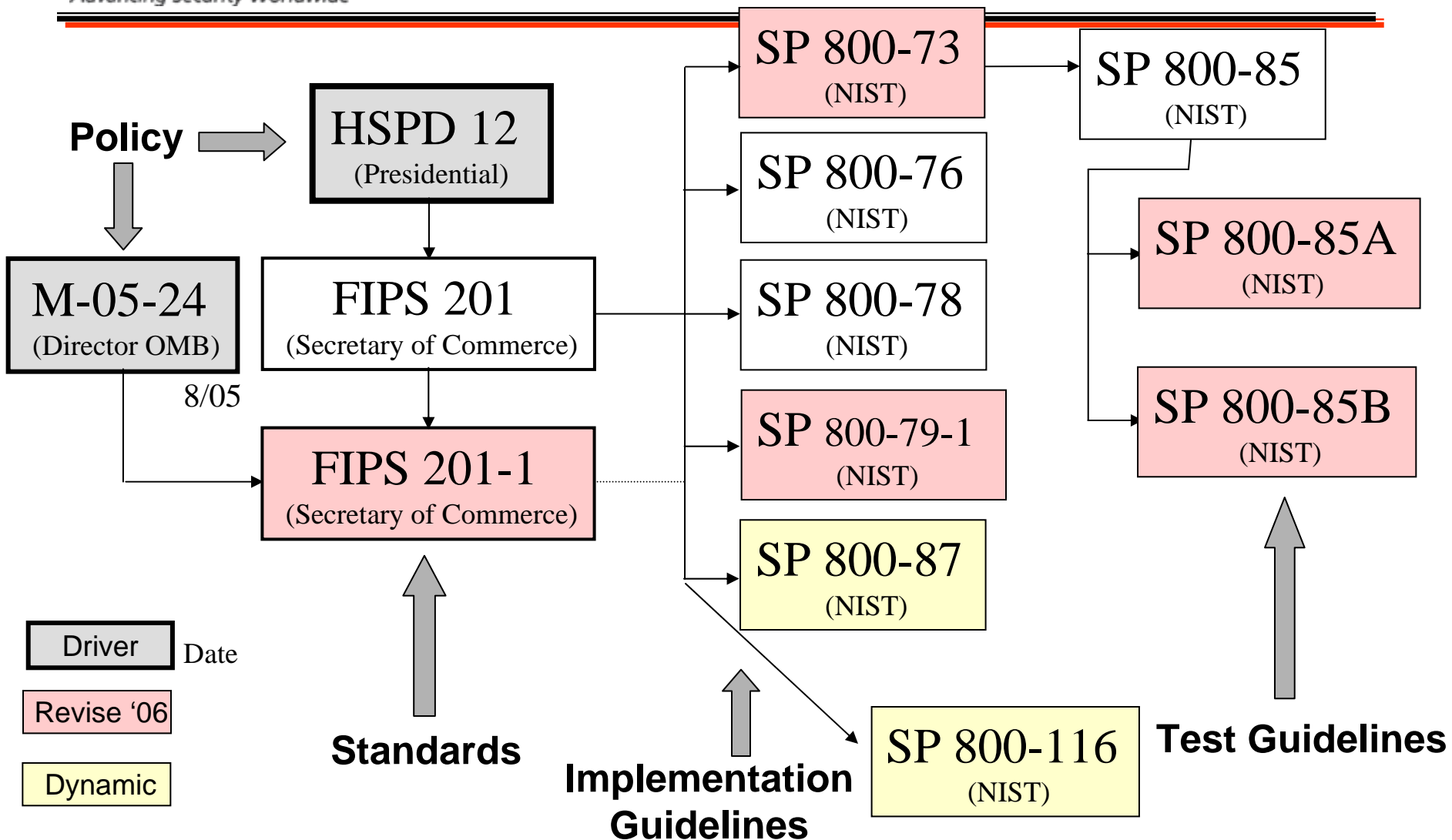
Laws, Policies, Rules

Processes

Federal Information Security Management Act

HSPD #12

PIV Document Relationships





NIST Special Publication 800-116

“A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)”

- Conform to FIPS 201-1 and SP’s in effect
- Review current limitations & threat environment
- State the PIV-in-PACS vision and benefits
- Recommend a PACS model and PIV integration approach
- Propose a PIV Implementation Maturity Model (PIMM)



PIV Implementation Maturity Model (PIMM)

- **Maturity Level 1—Ad Hoc PIV Verification**: A site has the ability to authenticate PIV Cards by performing required authentication mechanisms on an ad hoc, on-demand basis. For example, card and cardholder authentication is achieved with a handheld terminal or a specific PC, for special or occasional uses.
- **Maturity Level 2—Systematic PIV Verification to Controlled Area**: At the outer perimeter of the site (Controlled area), PIV Cards are accepted as proof of identity, possibly in addition to legacy PACS credentials. A visitor registration procedure exists to accept PIV Cards and if necessary convert PIV authentication to a temporary legacy PACS credential.
- **Maturity Level 3—Access to Exclusion Areas by PIV** : Access to Exclusion areas (the most sensitive areas) is permitted by PIV authentication or "exception" only. Here, exceptions are the exceptions to PIV issuance (e.g., less than six months association). However, all access to exclusion areas is also subject to authorization, and authorization would typically only be granted to PIV cardholders. The exception case might be applied to exclusion areas for VIP visitors, for example. At Level 3, legacy PACS or badges are not acceptable for authentication to exclusion areas.
- **Maturity Level 4—Access to Limited Areas by PIV**: Access to Limited areas (generally, those permitting clearance level- or role-based authorization) is permitted by PIV authentication or exception only. At level 4, legacy PACS or badges are not acceptable for authentication to Limited areas.
- **Maturity Level 5—Access to Controlled Areas by PIV**: Access to Controlled areas (showing evidence of organizational affiliation, or registration for a visitor, with or without escort) is permitted by PIV authentication or exception only. At level 5, legacy PACS or badges are not acceptable for authentication to controlled areas.

NOTE: *Maturity levels are progressive*: for example, Maturity Level 1 must be achieved before Maturity Level 2 can be achieved. Maturity levels can be applied to individual facilities, or by extension to multiple facilities within an OPDIV or organization. When applied to multiple facilities, a maturity level is achieved when each of the facilities in the group has achieved the maturity level individually.



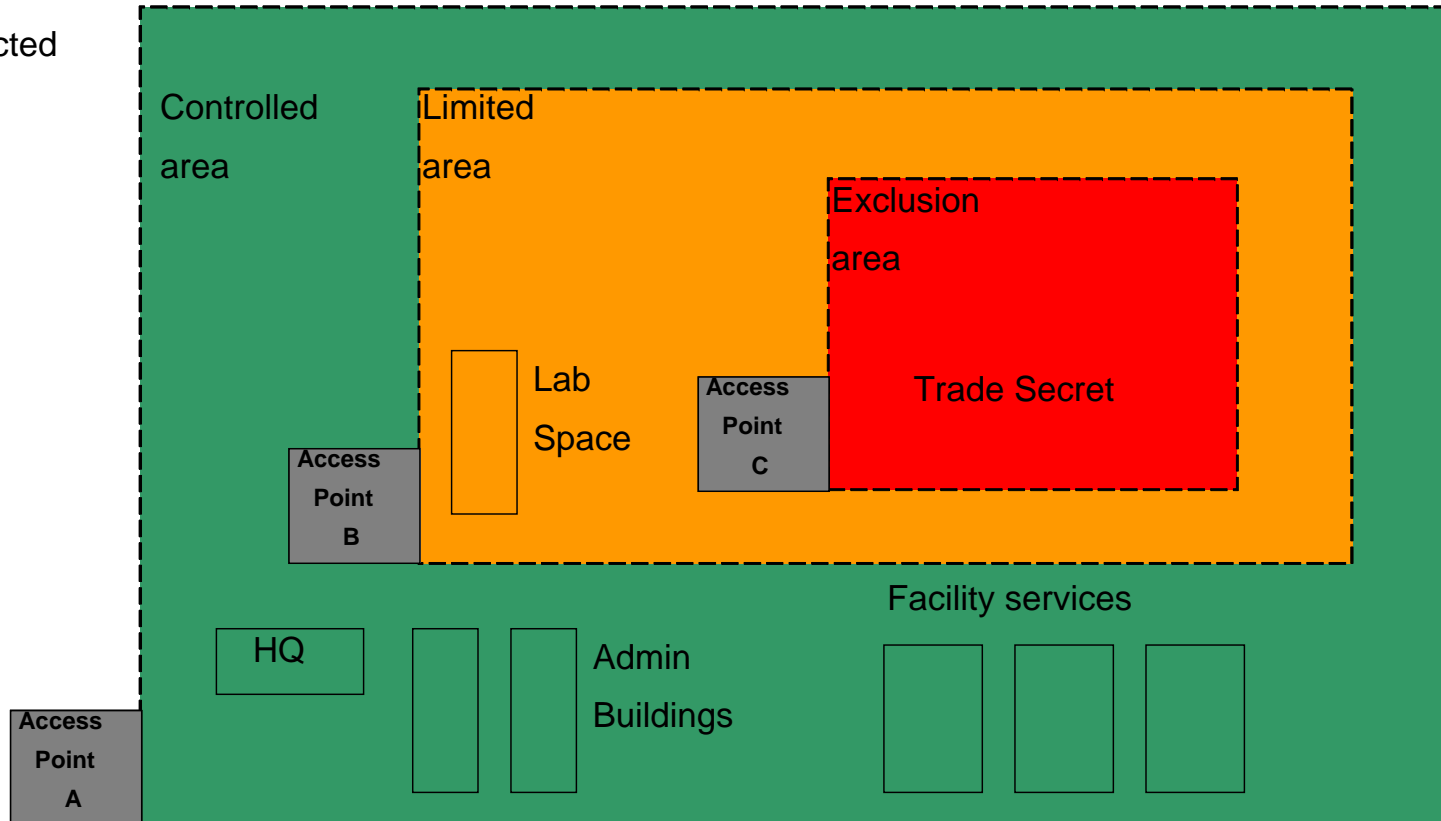
Converting Mechanisms to Factors

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors (HKA Vector)	Interface
CAK + BIO (-A)	x	x	x	3	Contact
BIO-A	x		x	2	Contact
PKI	x	x		2	Contact
BIO			x	1	Contact
CAK	x			1	Contact/ Contactless
CHUID + VIS	x			1	Contact/ Contactless

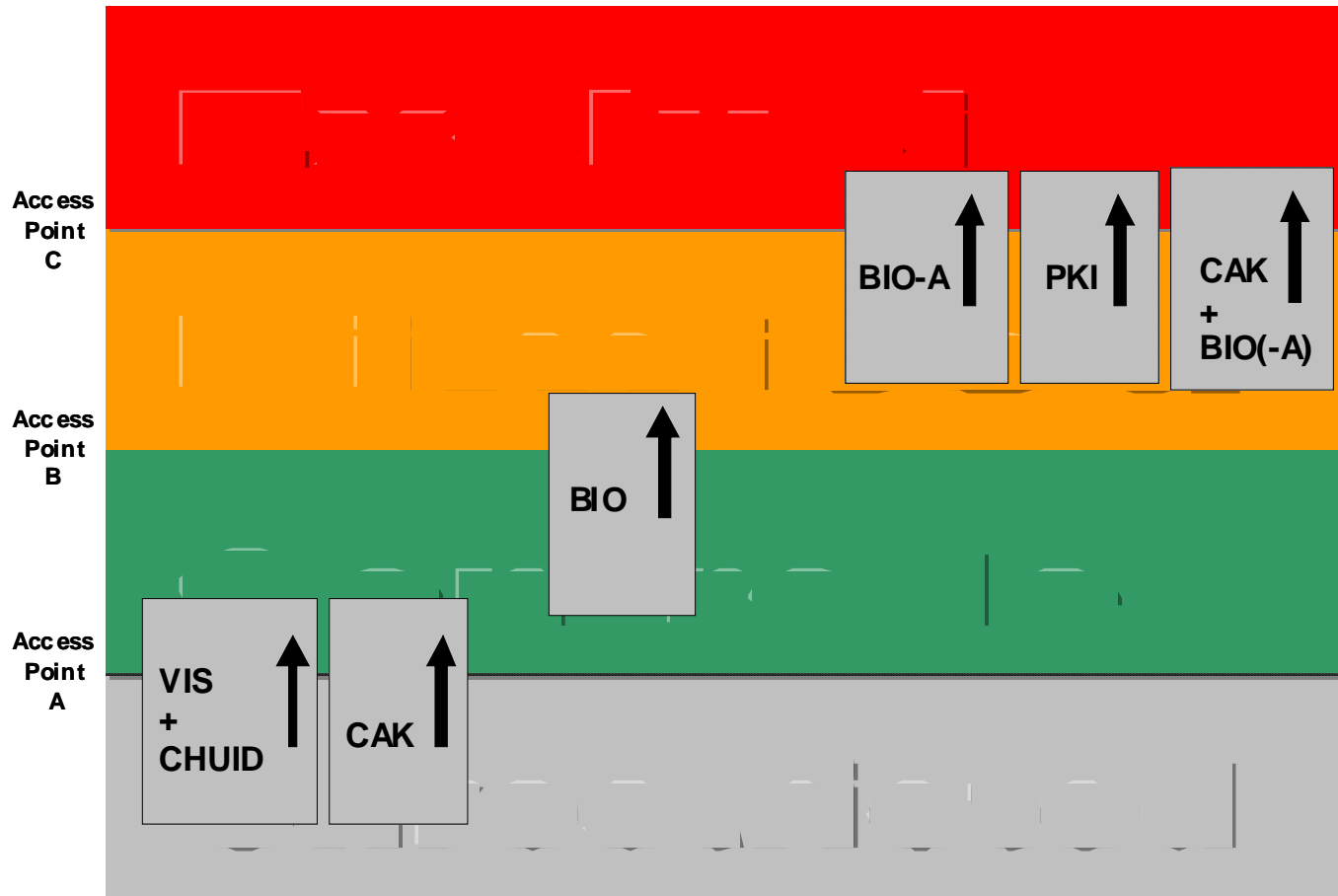
A PACS Model

Unrestricted, Controlled, Limited, Exclusion

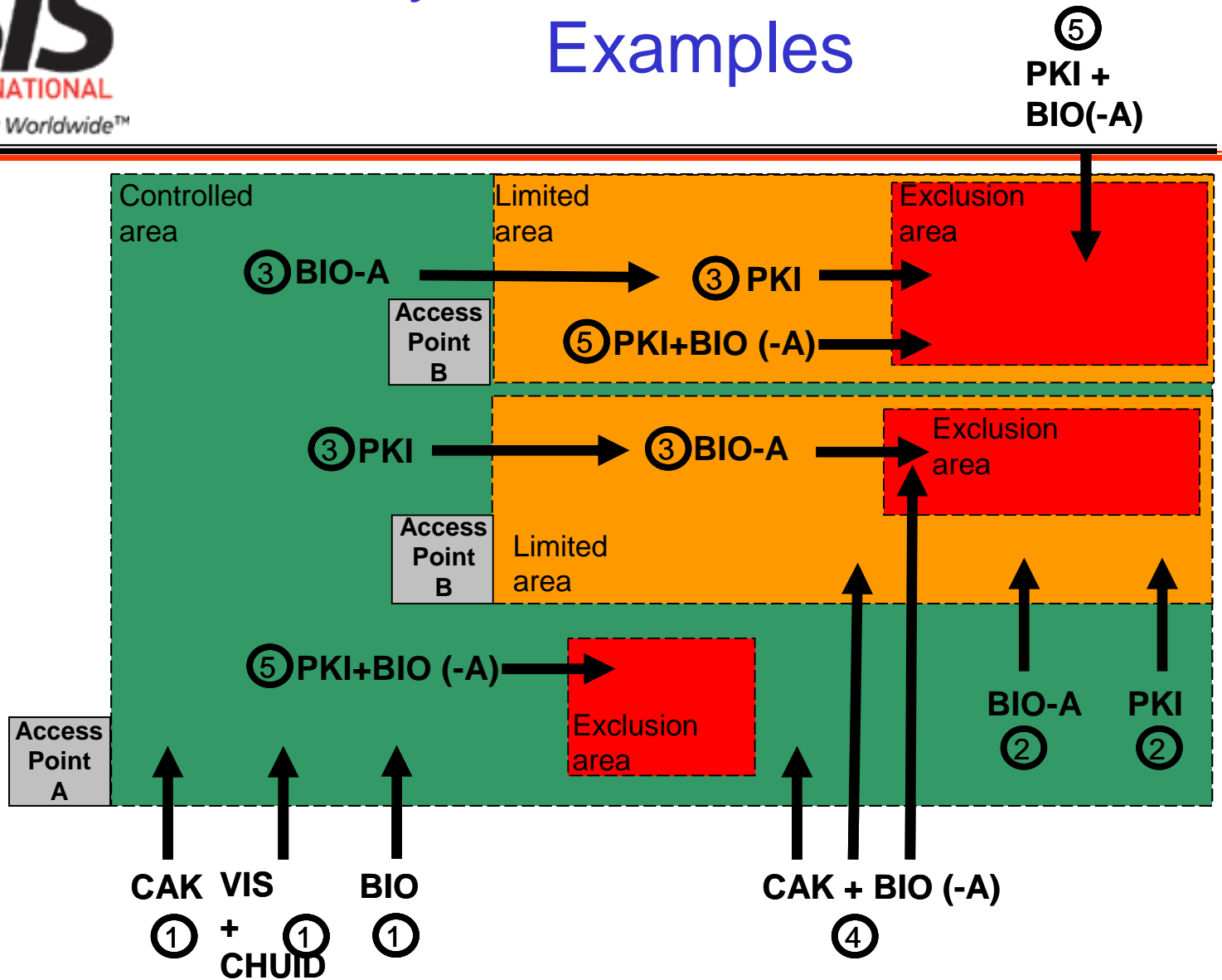
Unrestricted
area



...and, the mechanisms must be used at or below the perimeter shown.



Physical Access Control Examples





ICAM Mission



Fostering effective **government-wide** identity and access management

Enabling **trust** in online transactions through **common** identity and access management **policies and approaches**

Aligning federal agencies around common identity and access management practices

Reducing the identity and access management burden for individual agencies by fostering common interoperable approaches

Ensuring alignment across all identity and access management activities that cross individual agency boundaries

Collaborating with **external identity management** activities through **inter-federation** to enhance interoperability



Federal ICAM Segment Architecture

Phase I



The Federal ICAM Segment Architecture was developed as Phase I of the FICAM Roadmap and Implementation Guidance

- Complies with Federal Segment Architecture Methodology (FSAM)

www.fsam.gov

- Includes an As-is and Target state architecture and a Transition Plan for closing the gaps between the two
- Issued in draft form June 15, 2009
- Draft review period completed on July 15, 2009
- Phase I ends with Public Release of the **FICAM Roadmap**, currently anticipated October 2009

Federal ICAM Segment Architecture Purpose:

*The purpose of the Federal Identity, Credential, and Access Management (ICAM) segment architecture is to provide federal agencies with **a consolidated approach for implementing government-wide ICAM initiatives**. The use of enterprise architecture techniques helped ensure alignment, clarity, and interoperability across agency ICAM initiatives and enable agencies to eliminate redundancies by identifying shared ICAM services across the Federal Government.*



Phase II

Phase 2 includes the development of **ICAM best practices and implementation guidance**. This work is the extension of the Phase I, and will include sections addressing each of the agency-level initiatives included in the Transition Plan:

- Initiative 5: Streamline collection and sharing of digital identity data
- Initiative 6: Fully leverage PIV and PIV-interoperable credentials

– Initiative 7: Modernize PACS infrastructure

- Initiative 8: Modernize LACS infrastructure
- Initiative 9: Implement federated identity capability

Product: Version 2.0 of the FICAM Roadmap and Implementation Guidance document

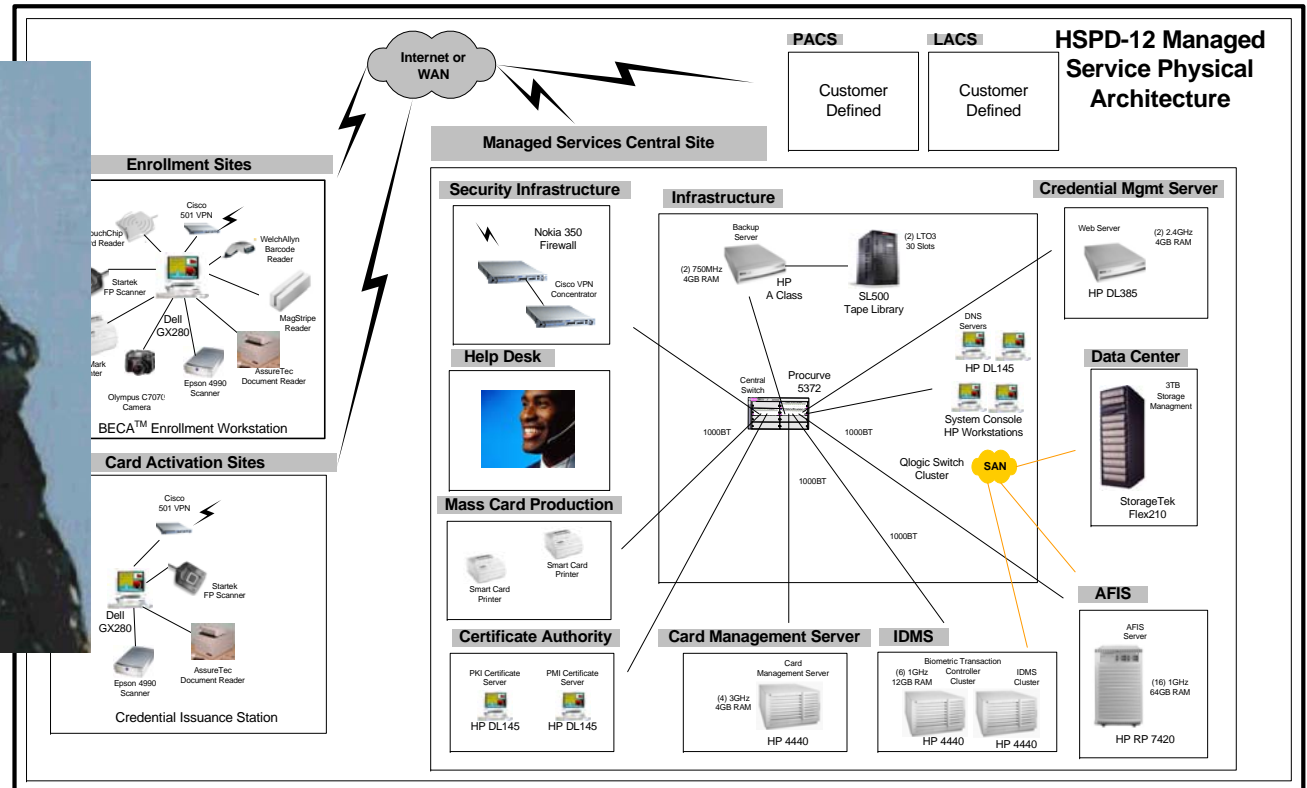
(December 2009)



R. Martin, CPP

HSPD – 12

Resistance is Futile!



LOGICAL & PHYSICAL ACCESS WILL BE ASSIMILATED INTO THE SMART CARD!

Further Info Slide

Ron Martin, CPP

PO Box 681, Dumfries, Virginia 22026

Email: ronasis@comcast.net

