



Smart Card
Alliance



Multiple Credential formats & PACS

Lars R. Suneborn, Director - Government Program, HIRSCH Electronics Corporation



A Smart Card Alliance
Educational Institute Course



Multiple credential factors, formats & PACS

What is a traditional PACS card?

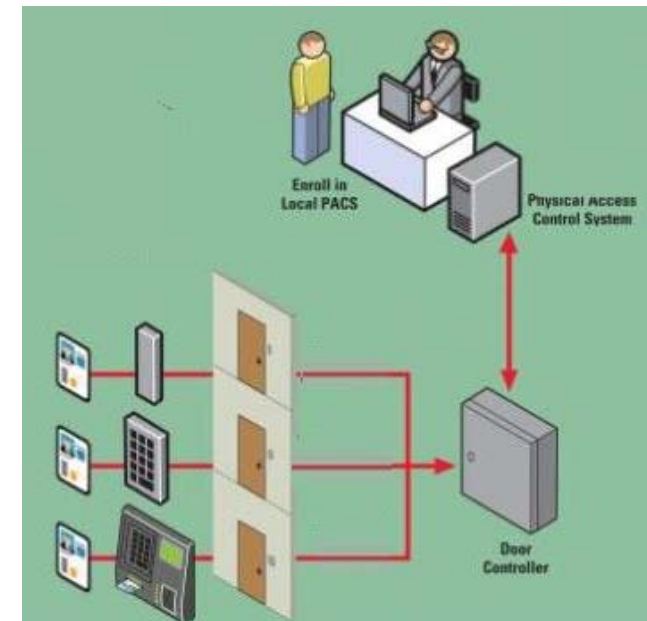
- Facility code, Unique number (255 65000)
- Data released when presented to compatible reader

Main data links

- Card –to- reader
- Reader–to-Controller
- Server– to-Controller

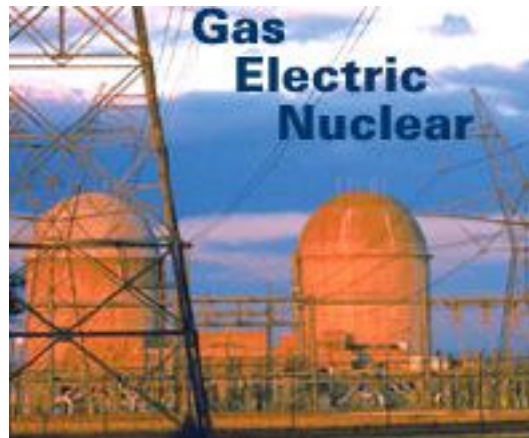
Factors vs. Format

- Multiple factors
- Card
- (Card & PIN)
- (Card & BIO)
- (PIN & BIO)
- Many other combinations
- Same card data format





Traditional Multi-factor Identification applications



Multi facility sites,
single building
Layered approach to
physical security
Exterior perimeters
Cross point
procedures



- One, Two, Three factor authentication



Site exterior perimeter cross point



**Automated authorization:
Card - Vehicle**

**Automated authorization:
Card – Driver**

**PACS must recognize
multiple readers, card
technologies**





Single building - interior perimeters



Lobby exterior control point

Card only





Building perimeter cross point - Two factor



Medium throughput
automated verification
and authorization

-Card or PIN entry,
Card exit



Card & PIN entry



Interior perimeter cross point



Automated, low throughput: Card & Biometric (1;1 match)





Interior perimeter cross point

Interior area control point

Card & PIN

Card & Biometric & PIN,

Two person control,
alarm integration





Multiple credential factors & PACS

PACS must process multiple “factors”

- Card data
- PIN
- Biometric modalities
- Combination of factors



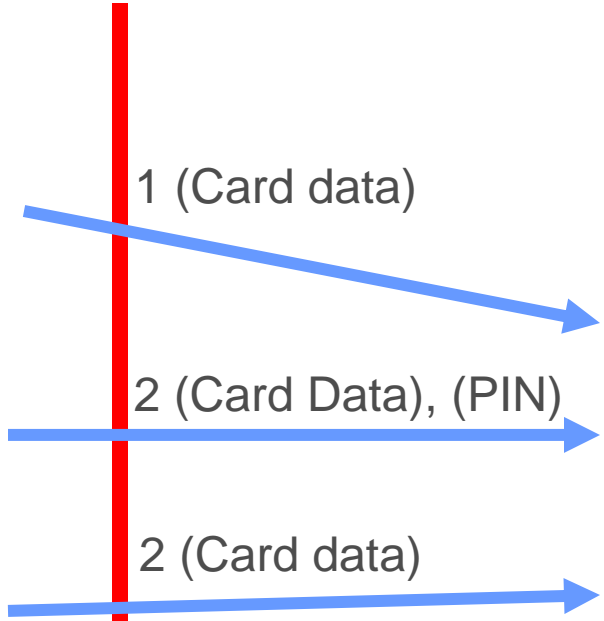
Traditional authentication factors



1 (Card data)

2 (Card Data), (PIN)

2 (Card data)



Attack Side

Secure Side



Modern card formats & PACS

Personal Identity Verification, PIV.

- Data model support large user populations
- High immunity to counterfeiting, data manipulation
- Combination of Factors On Card, Off Card
 - Visual
 - CHUID
 - CAK
 - PKI
 - BIO, BIO –A
- BIO combined with cryptographic challenge/response, PKI + BIO or CAK + BIO, authenticates the PIV Card and thus achieves three-factor authentication.
- Produces FASC-N (AAAA SSSS NNNNNN)

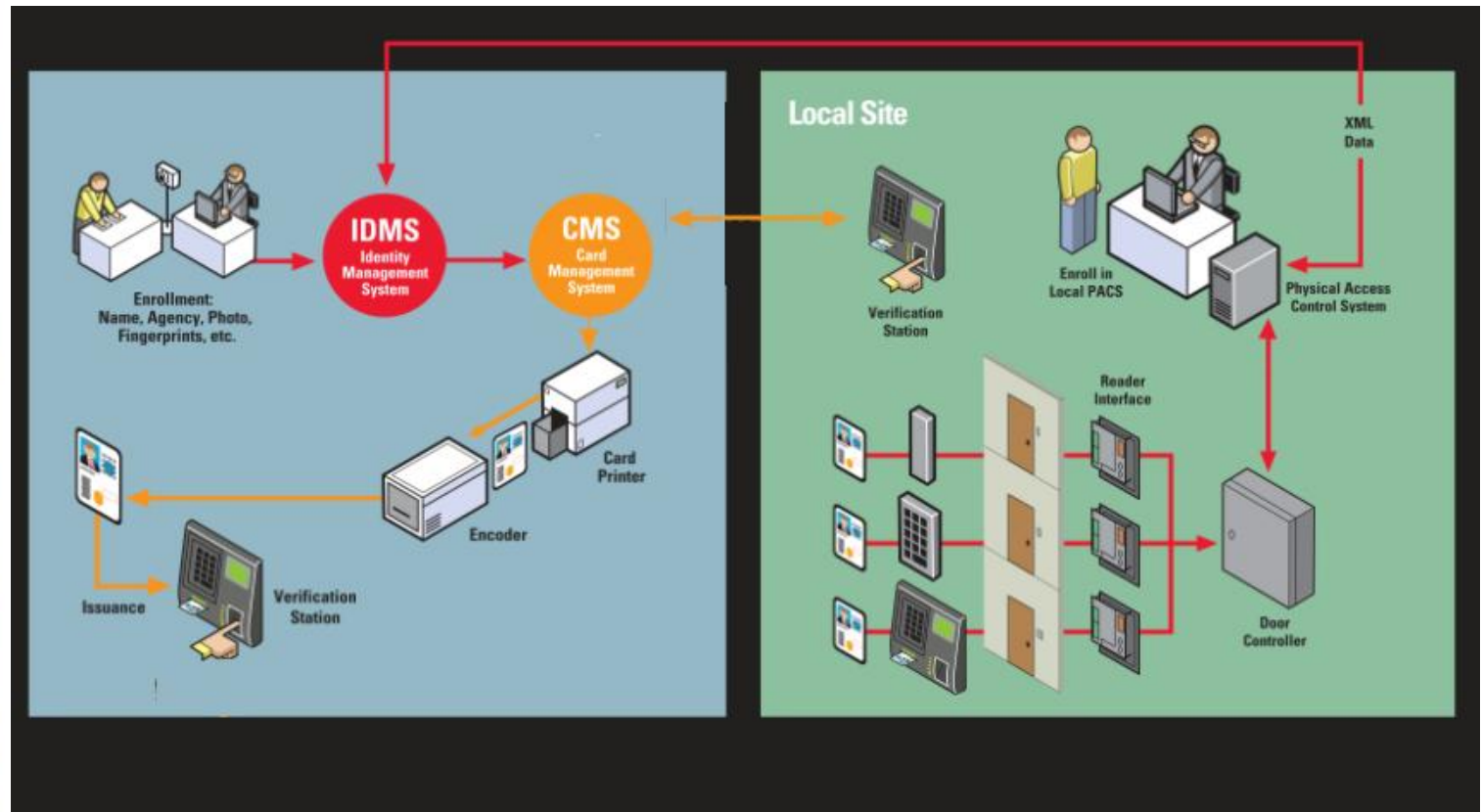
)



Modern card formats & PACS

Server

May be connected to PIV IT Infrastructure





Modern card formats & PACS

NIST SP 800-116 Area definitions

Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

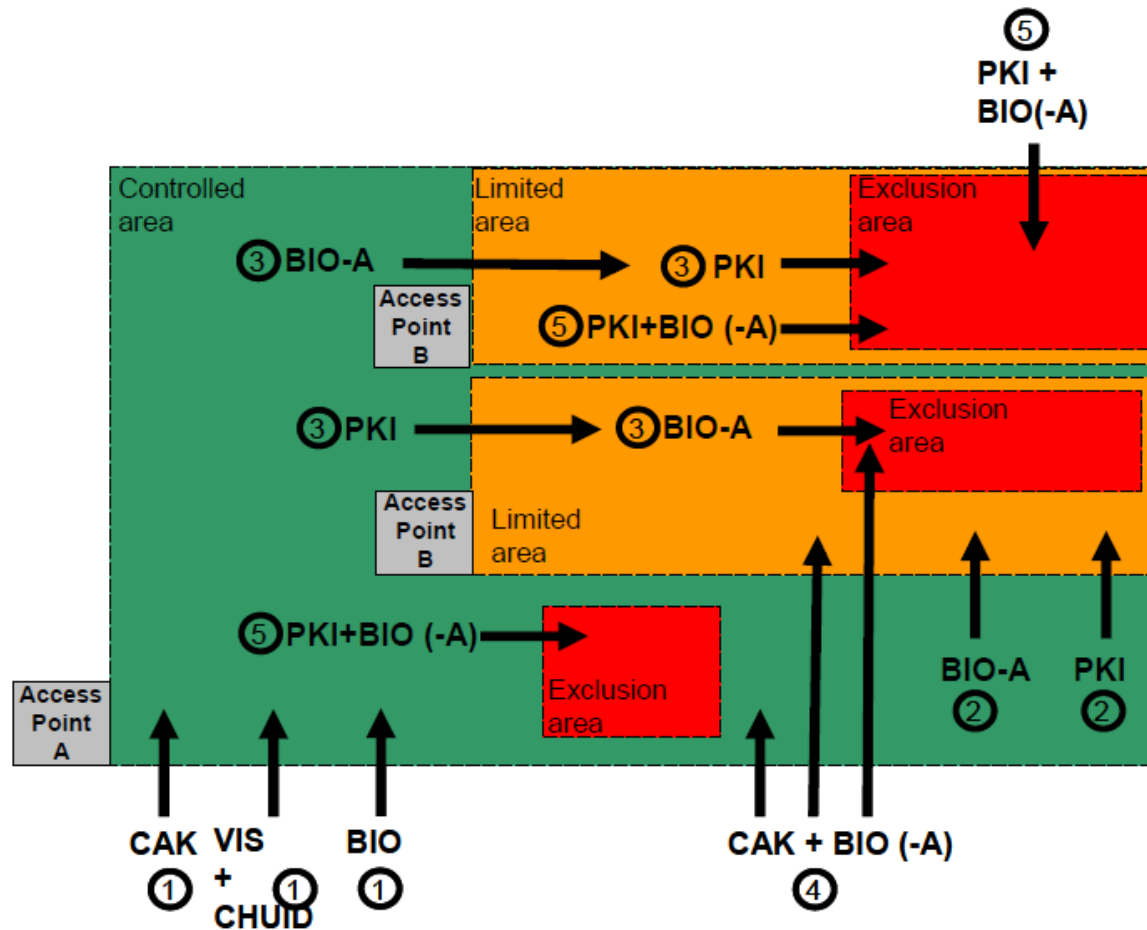


Modern card formats & PACS





Modern card formats & PACS





Multiple card formats & PACS

All PACS users will not have the same card technology

Examples are

Employees who have not yet received PIV

Visitors from other agencies

Non Government visitors



High Assurance vs. High Security



(FASC-N) (Old Card)

(FASC-N), (PIN)
(Old Card) (PIN)

(FASC-N Bio)
(Old Card)

1 (FASC-N Bio), 2 (PIN)

Attack Side

Secure Side





Related Organizations, Documents

SCA – Interoperable ID Credential for Aviation Industry

TSA – ACIS Technical Specification

PIV – Personal Identification Verification

- PIV I – Process & Procedure

- PIV II – Technical Specification (FIPS 201, NIST SP 800-73)

FRAC – First Responder Access Credential

TWIC – Transportation Workers Identification Credential



THANK YOU



LOGO



Smart Card
Alliance



Contact Information:

Lars R. Suneborn
Director, Government Program
HIRSCH Electronics Corporation
1900 Carnegie Ave. Santa Ana, CA. 92705 (949 250-8888)
Lars@Hirschelectronics.com

A Smart Card Alliance
Educational Institute Course