NIST FIPS 201-2 Workshop
April 18 – 19, 2011

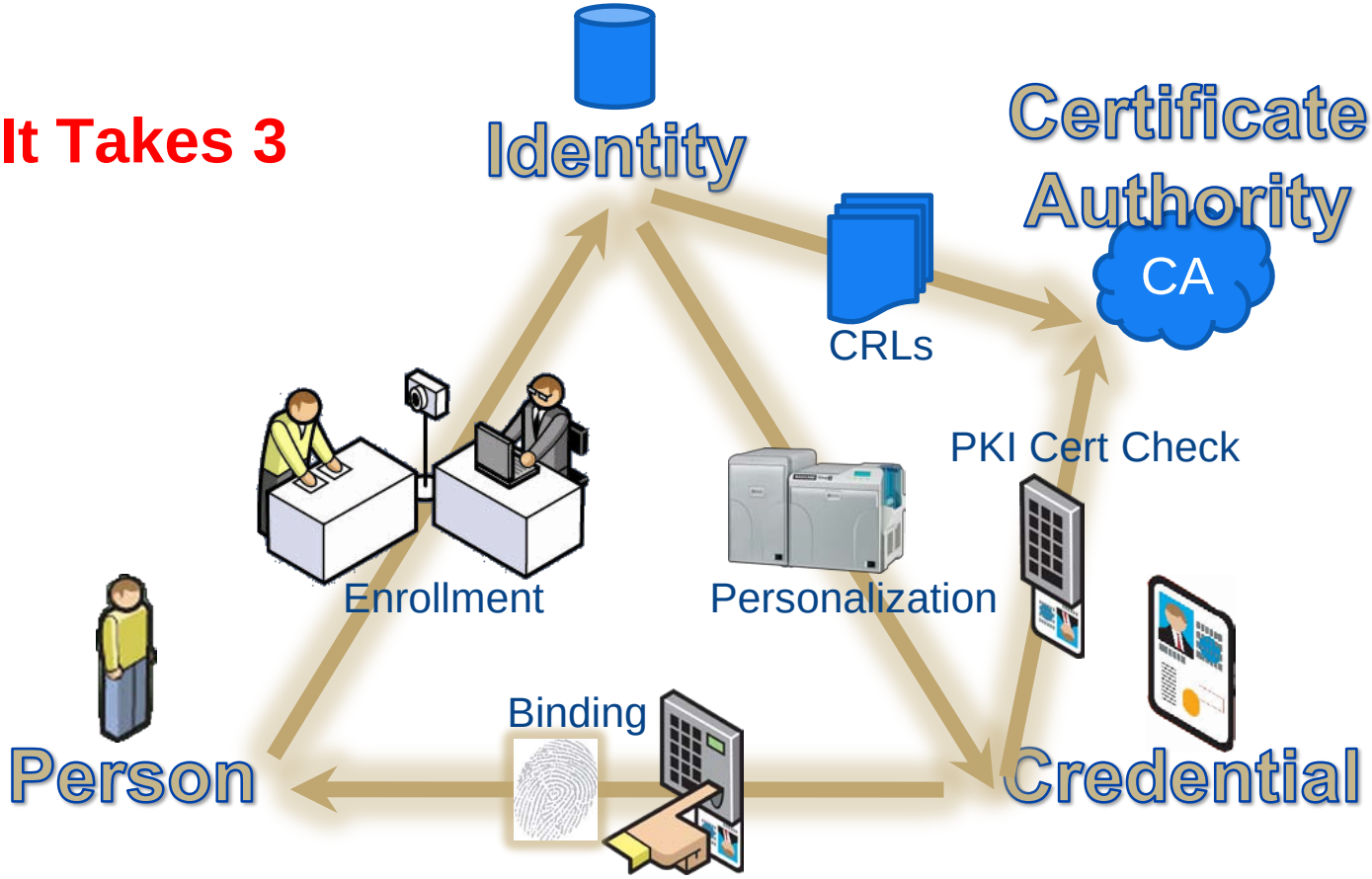
Industry Perspectives on FIPS 201-2 Draft

Rob Zivney
VP Government & Standards
Identive Group

Chair PIV Working Group
Security Industry Association

PKI Is Not Very High Assurance

- **It Takes 3**



Combine Signed CHUID & PKI-CAK

- **No Cost Savings for Much Weaker Signed CHUID**
  - FIPS 140-2 Required
  - Path Validation Required
  - GSA APL Traced to SP 800-116
- **Signed CHUID Has Little value**
  - Uses Signer's Public Key
    - No "Secret" per SP 800-63
- **Both Are "=" in Table 6.2 & 6.3**
  - PKI-CAK is a True Trusted Factor
- **New "Signed CHUID" is Named "CHUID"**
  - Will Be Confused with "Unsigned CHUID"
  - Installed Base will not Upgrade
  - Need to Clarify the "Unsigned CHUID" is "No Assurance"

PACS = Contactless
Contactless ≠ Some Assurance (Only)

- **Entrances are on the "Outside"**
  - Salt Water, Sand, Coke Dust, Vandals
  - Contact Readers are NOT Suitable
    - High Maintenance Cost!!!
- **No High Assurance for PACS**
  - BIO is Contact Only
- **No Very High Assurance for PACS**
  - PKI-AUTH is Contact Only
- **TWIC Pilot "Proved" Need for:**
  - Contactless BIO without PIN
  - Outdoor Solutions
  - Faster Throughput Solutions
  - Better Antenna Bonding Specs and Tests

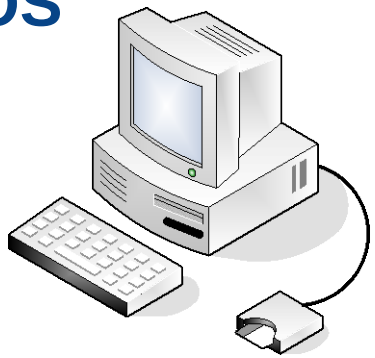
Table 6-2. Authentication for Physical Access

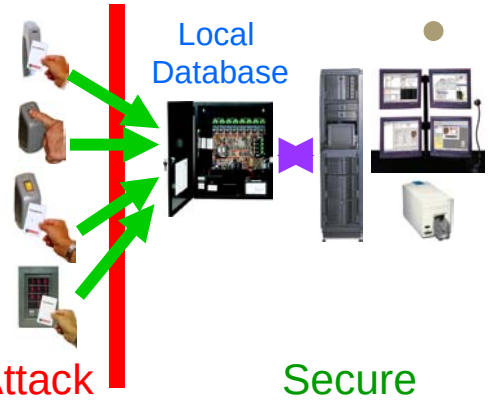
PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
SOME confidence	VIS, CHUID, PKI-CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI-AUTH

FIPS 140-2 & System Architecture

LACS

- **Microsoft OS**
  - FIPS 140-2
- **Changes**
  - Download Software
  - Microsoft
- **Low Cost**
  - Dumb reader
  - Protected Environment



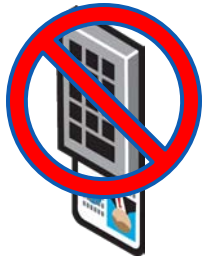


PACS

- **Controller OS**
  - FIPS-140-2
- **Changes**
  - Download Firmware
  - PACS Mfg
- **Higher Cost**
  - Lower Volumes than MS
  - Hostile Environments
  - Smart Readers?

PIN To PACS

- **Docs Now Acknowledge PACS**
  - e.g., ICAM, SP 800-116, & GSA APL
- **Acknowledge "Off Card" as Legit**
  - User Assumes Silence = "Not Allowed"
- **PIN to PACS is More Secure**
  - Easy to Shoulder Surf a "Global PIN" When One Logs on
  - Then Steal the Card and Get in a PKI-AUTH Door
- **PIN to PACS + CAK (Asymmetric) = PKI-AUTH**
  - Lower Cost
  - PACS Friendly
  - Environment Resilient
  - Smaller Form Factor for Retrofit into Existing Reader Housings
  - Two Trusted Factors



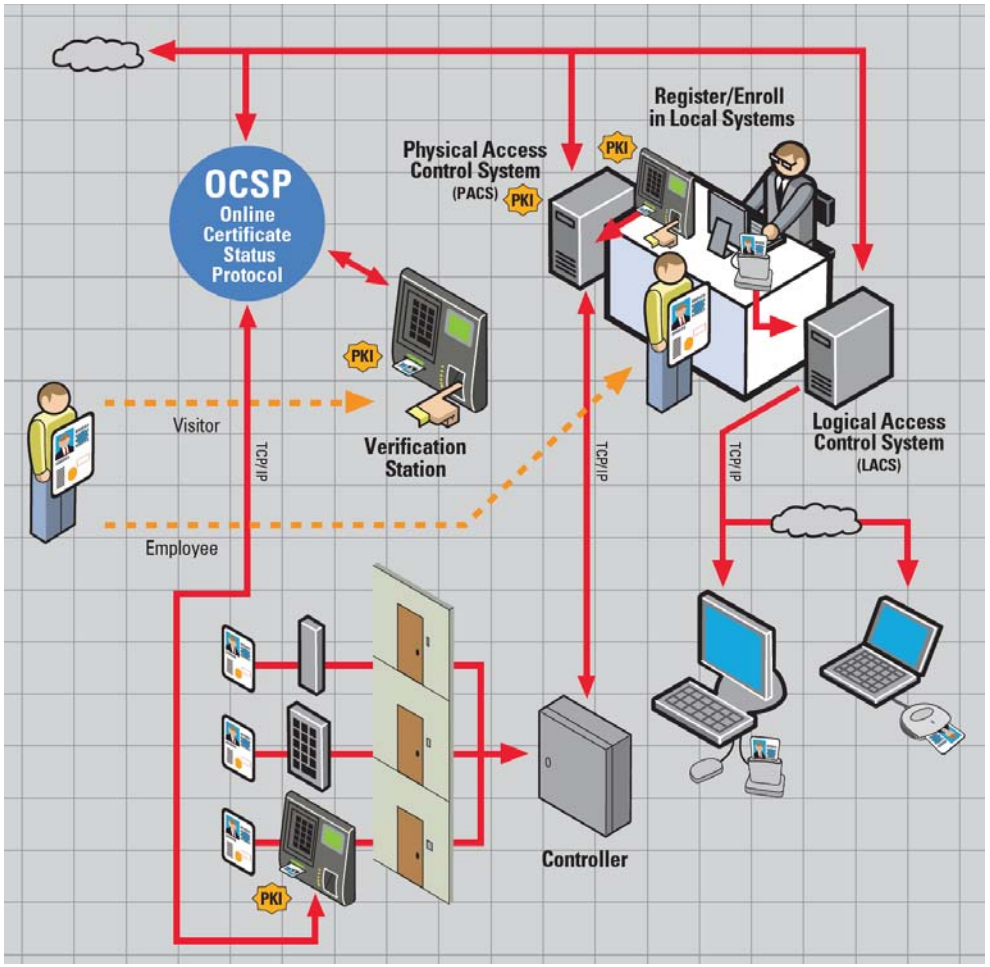
Reissue All Cards !

- **Options Aren't – For PACS/Readers**
  - Read Any and All Encryption Algorithms
  - Read All Sp 800-73, -1, -2, -3
  - Read CAC, FRAC, TWIC, PIV-I
- **PKI-CAK Is No Value for 5-6 Years**
  - If wait a lifetime of issued cards
  - Therefore Only PKI-AUTH will meet ICAM
- **Need a "Card Update" Process/Mechanism**
  - For New Mandatory
  - To Allow Contactless for High and Very High Assurance

- **Else PIV Is Not Truly Interoperable**

Address PACS "Registration"

- **Require 3 Factor**
- **Require Real-Time Cert Check at Registration**
- **Caching Status Proxy at Site for the Door**
  - Else FPKI Cannot Handle
  - Else Throughput is Slow!
  - Else Access Depends on the Perfect Cloud
- **PACS Friendly**
  - Download a "Flag" to the Controller on Status Change
  - Distributed Processing
- **Multiple CSP & SCVP for Enterprise Applications**



Normalize Assurance Levels

- **# Factors = Assurance Level per SP 800-116**
- **Allow Combinations**
- **Be Clear Why Something Is What It Is**

PIV Assurance Level at the Door	Trusted Authentication Factors	Single	Combination
NO confidence	0	VIS, CHUID, BIO, PIN to CARD	VIS + CHUID, CHUID + BIO
SOME confidence	1	BIO (S), CAK, PIN to PACS CHUID (S)	
HIGH Confidence	2	PKI	PIN to PACS + CAK, CHUID (S) + PIN to PACS BIO (S) + CAK, BIO (S) + PIN to PACS, PKI + BIO, CHUID (S) +BIO (S)
VERY HIGH Confidence	3		PKI + BIO (S), PIN to PACS + CAK + BIO (S). CHUID (S) + BIO (S) + PIN to PACS

Summary

- **Create Specs Industry Can Build COTS Products**
  - GSA APL has Virtually Nothing for Physical Access!
- **CHUID Reads are Less Secure than Prox they Replace ➔ Kill**
  - Signed CHUID and Signed BIO go too – or Combine with Other
- **Urgent to Have CAK NOW!**
- **Urgent to Have HIGH & Very High Assurance Contactless**
  - CAK sets a Precedence, PIN to PACS is Low Cost, Simple Path
- **Create Trusted BIO and Use for 3rd Factor**
  - Only 3 Trusted Factors Can be Very High Assurance
- **Recognize PACS are Distributed Architectures In Hostile Environments**
  - Address Registration with Caching Status Proxy and SCVP
- **Develop a Process to Update Issued Cards for Latest Version of Specs**
- **Fix Section 6 Assurance Level Tables to Track # of Trusted Factors**

If Cost to Implement is Too High, It Will NOT Happen