



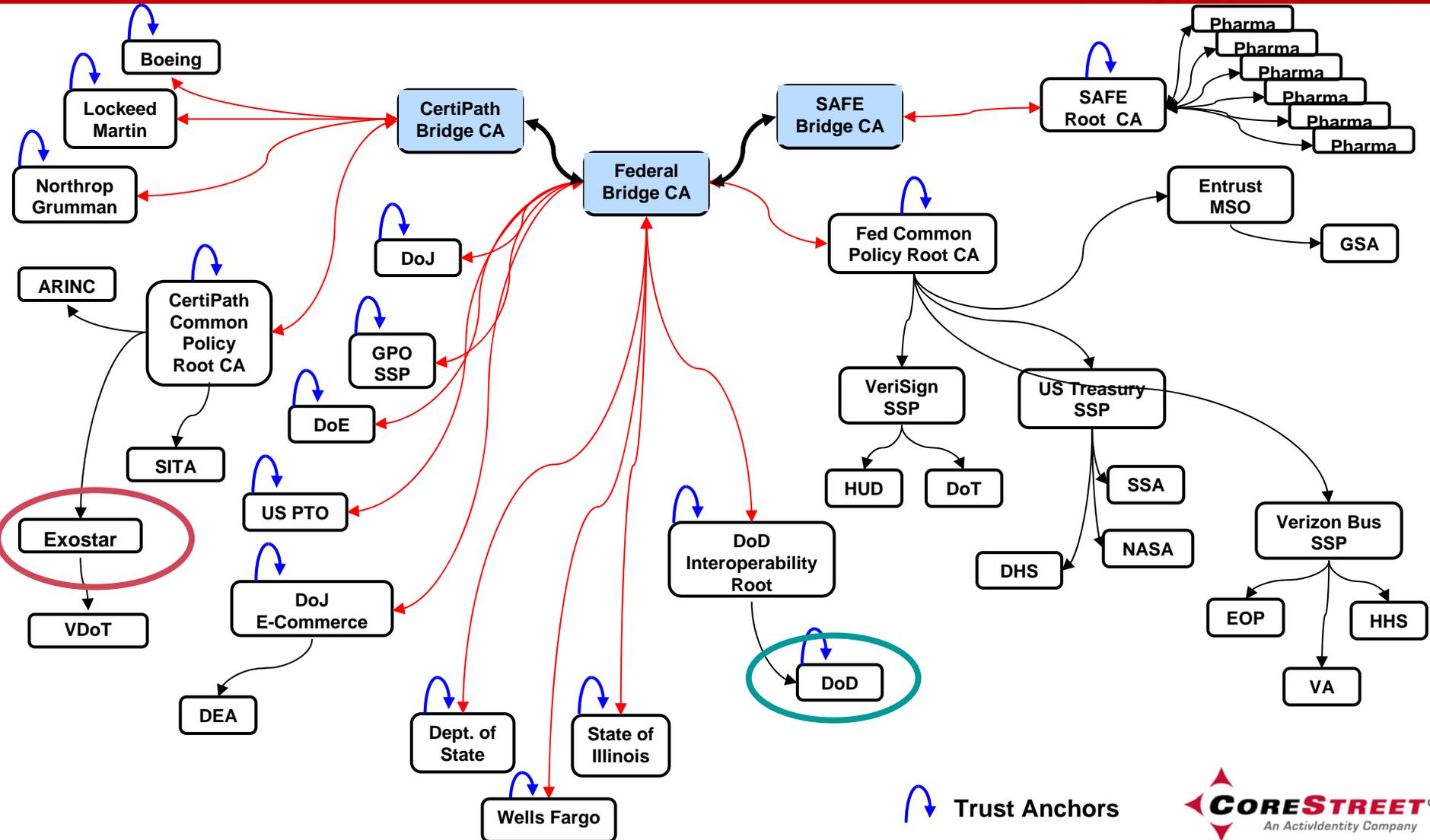
# Achieving a FIPS 201 PACS Solution

Bob Dulude  
CSO

# Project Goals

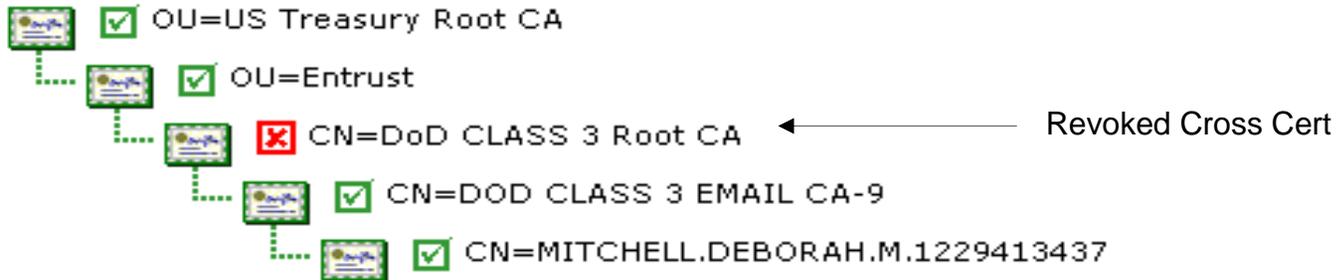
- Demonstrate feasibility of NIST 800-116 authentication options
- Provide access control authentication for any credential whose trustworthiness can be established through the Federal Bridge
- Support FIPS 201 PIV & PIV-I identity cards
- Demonstrate convergence of physical and logical access control in a federated environment

# Establishing Trust in a Federated Environment (drawing not current)

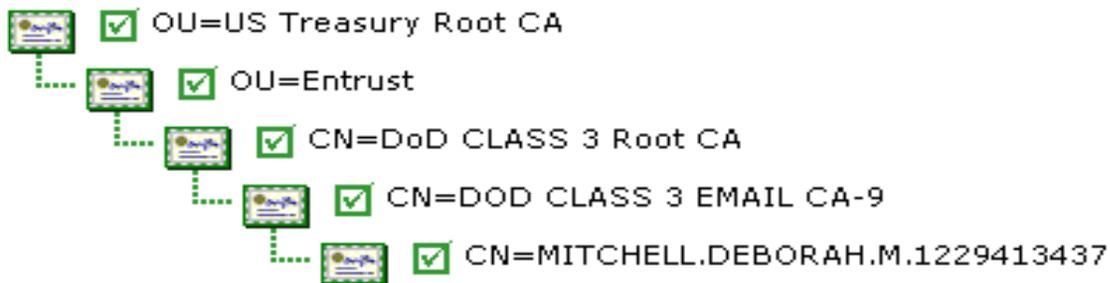


# Path Examples

Found **invalid** path 3 of 8 in 16 ms.

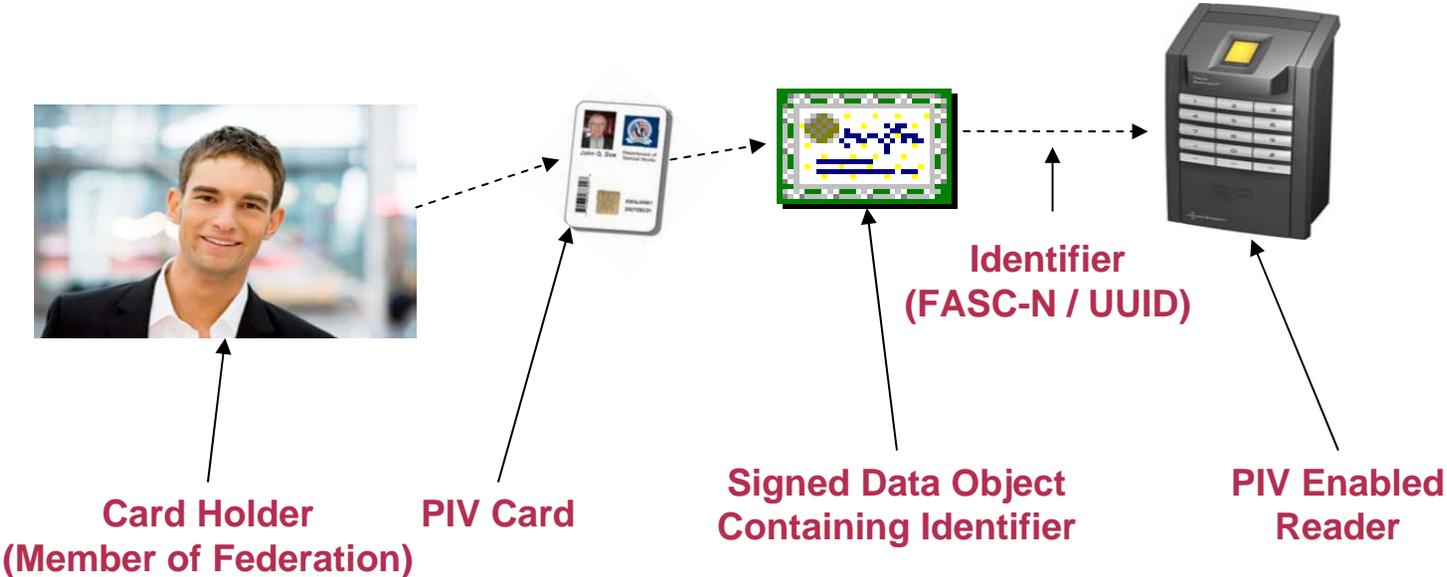


Found **valid** path 4 of 8 in 15 ms.



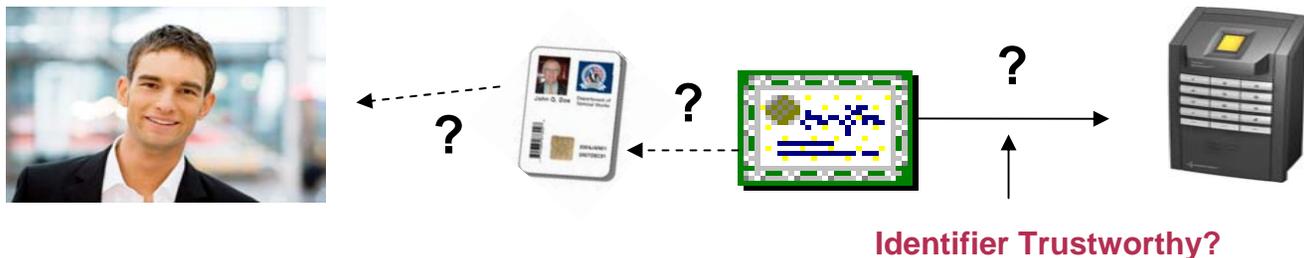
<http://scvp.corestreet.com/demo/index.jsp>

# Fundamental Question



Can we trust it?

# What are the vulnerabilities?



## 1. Counterfeit identifier

- Digital signature by a trusted source ensures data object is genuine and unmodified

## 2. Cloned/Copied identifier (certificate only)

- PKI private key challenge ensures identifier has not been copied

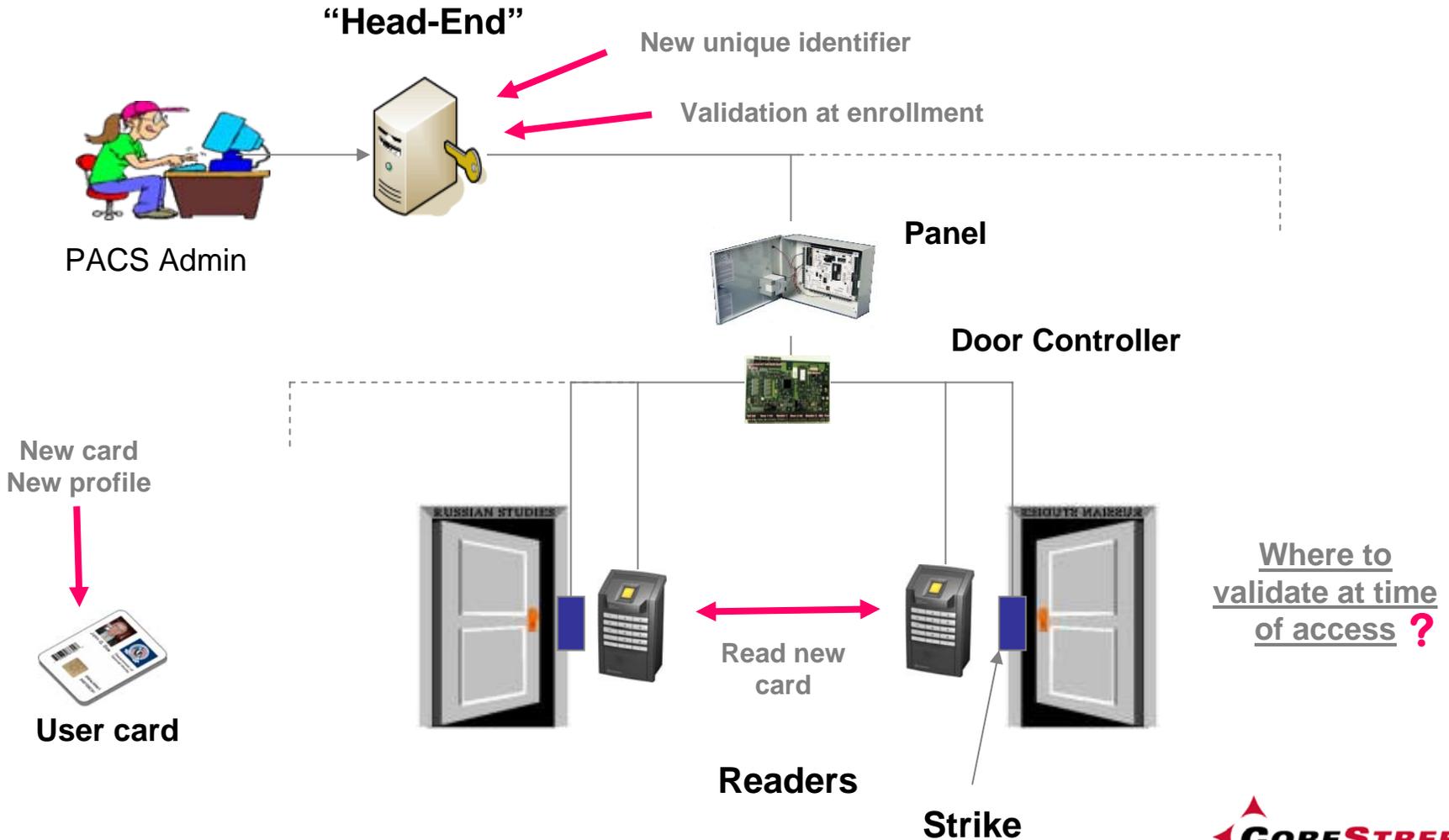
## 3. Lost/stolen card – cardholder does not match identifier

- Check binding of the identity card to individual by checking either/both
  - Something you “know” (PIN)
  - Something you “are” (biometric)

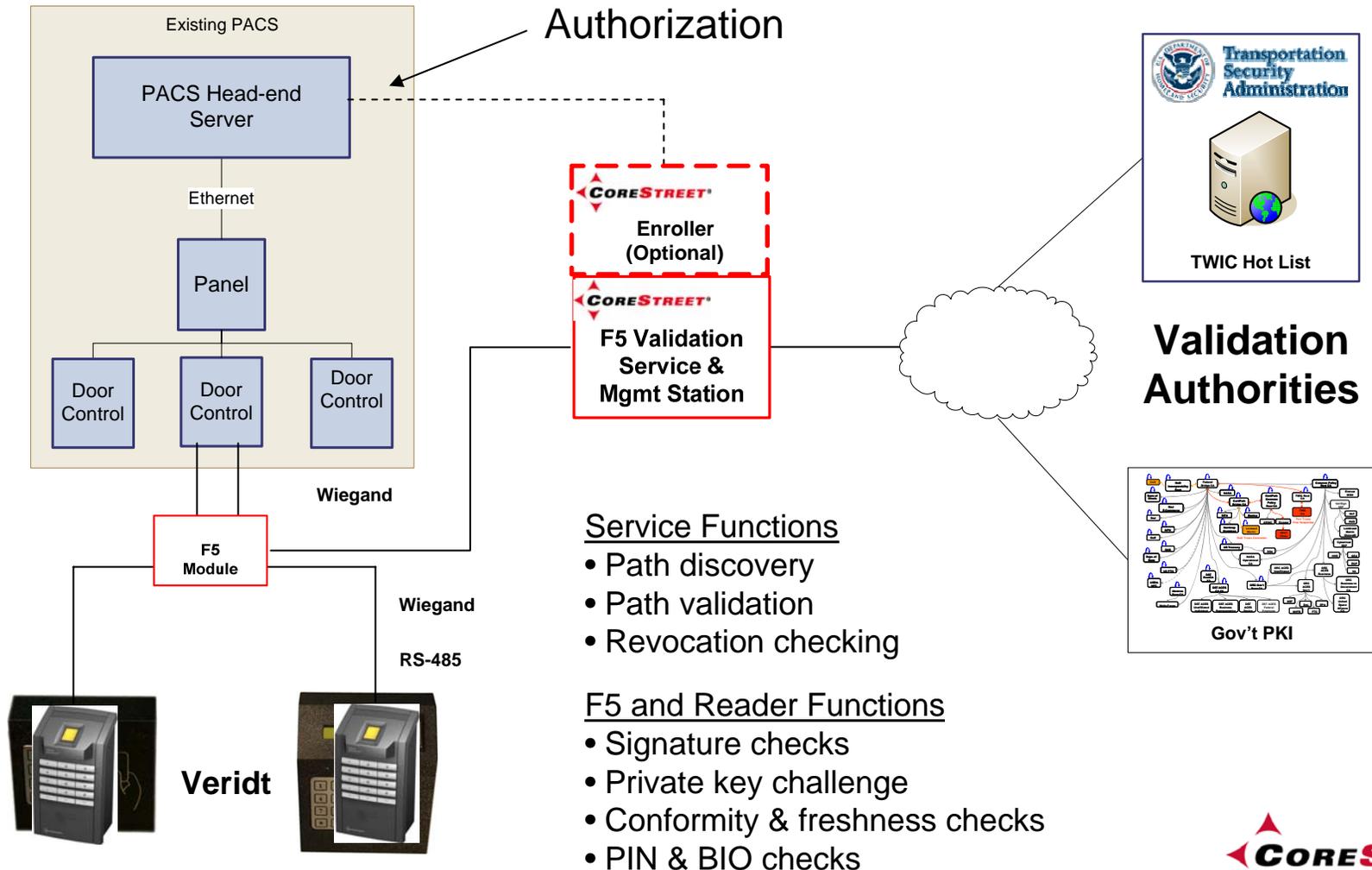
## 4. Revoked credential – Cardholder relationship with issuer is “broken”

- Periodic check that credential has not been revoked

# FIPS 201 Required Changes to PACS



# The F5 Approach



# Supported Cards and Auth Modes

## Card Types

- PIV
- PIV-I
- Legacy CAC
- CAC NG
- CAC EP
- TWIC
- FRAC

## Auth Modes

- FASC-N (unsigned CHUID)
- CHUID
- Card Auth
- PIV Auth + PIN
- CHUID + BIO (TWIC mode)
- Card Auth + BIO (TWIC mode)
- PIV Auth + PIN + BIO

# Mitigating the Threats

Auth Modes	Secures against cards that are				Auth Factors	SP800-116 Security Area
	Revoked	Counterfeit or Altered	Copied or Cloned	Lost or Stolen		
FASC-N	X				None	Uncontrolled
CHUID+VIS	X	X			1	Controlled
CAK	X	X	X		1	Controlled
PIV+PIN	X	X	X	X	2	Limited
PIV+PIN+BIO	X	X	X	X	3	Exclusion

- Performing signature checks and private key challenges at enrollment is not sufficient to achieve these levels of assurance. They must also be done at the time-of-access.
- Revocation checking for FASC-N and CHUID modes must be done using the PIV certificate CRL.



## F5 Approach – why we chose this path

- Works power-out or comms-out
- Reuse most existing wiring
- Reuse existing PACS (Headend, panels and door controllers)
- Match reader type with assurance level requirements
  - For each access location; CHUID, CAK, PKI, BIO, multiple
- Centrally manage assurance levels for each reader
  - Can change assurance level base on threat level
- Retains all PACS functionality at each access point
  - Video, 2 person rule, door ajar, handicap settings, etc.
- Centrally managed firmware updates
  - Support for future PIV applet changes



## For additional information:

- **Bob Dulude**  
**Chief Security Officer**
- **Mobile: (781) 710-0436**
- **Office: (617) 661-3554 x202**
- **Email: [bob@corestreet.com](mailto:bob@corestreet.com)**
- **Website**
  - [www.corestreet.com](http://www.corestreet.com)
- **Cambridge Office Address**
  - One Alewife Center
  - Suite 200
  - Cambridge, MA 02140

