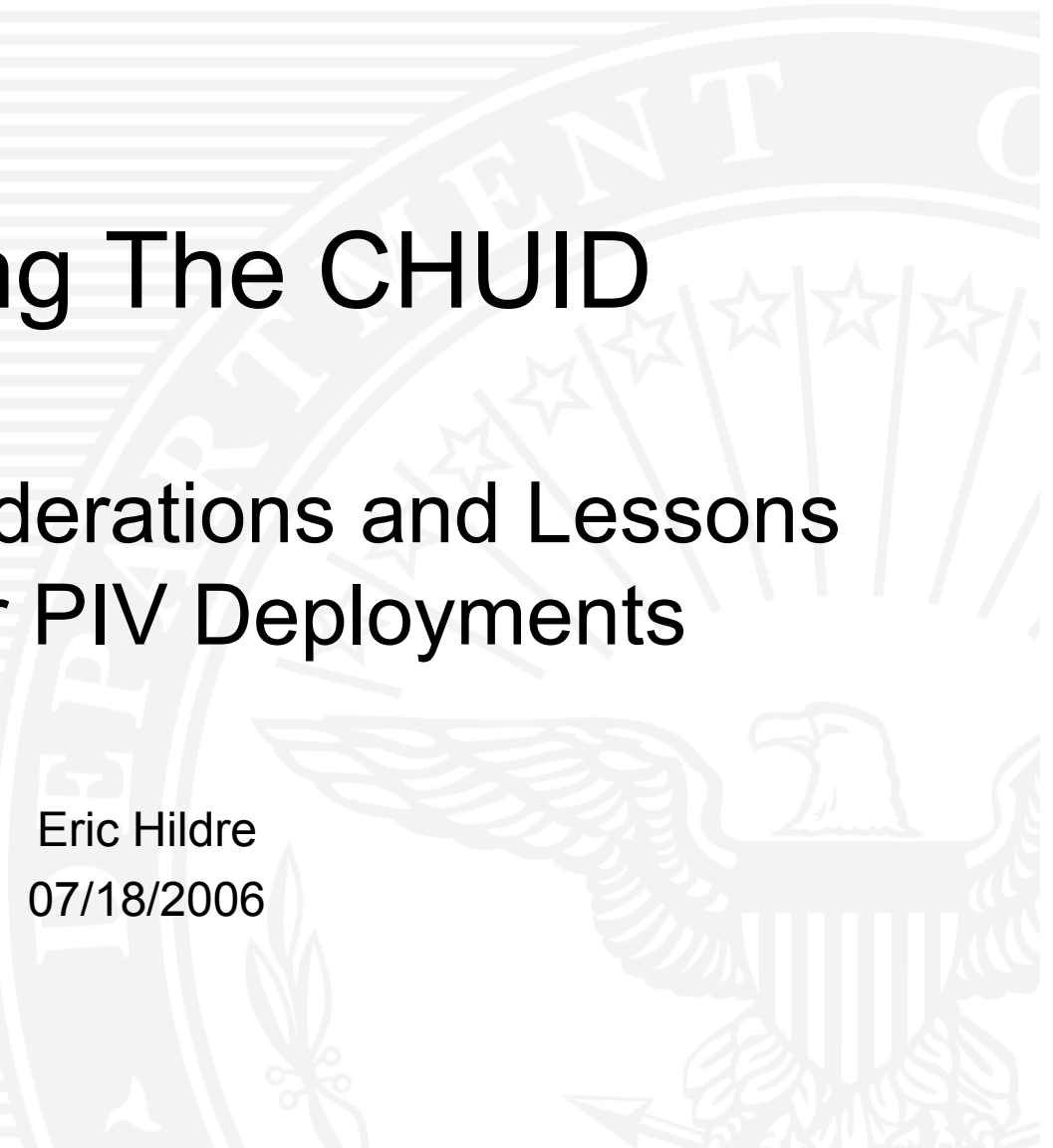


Unlocking The CHUID

Practical Considerations and Lessons Learned for PIV Deployments

Eric Hildre
07/18/2006

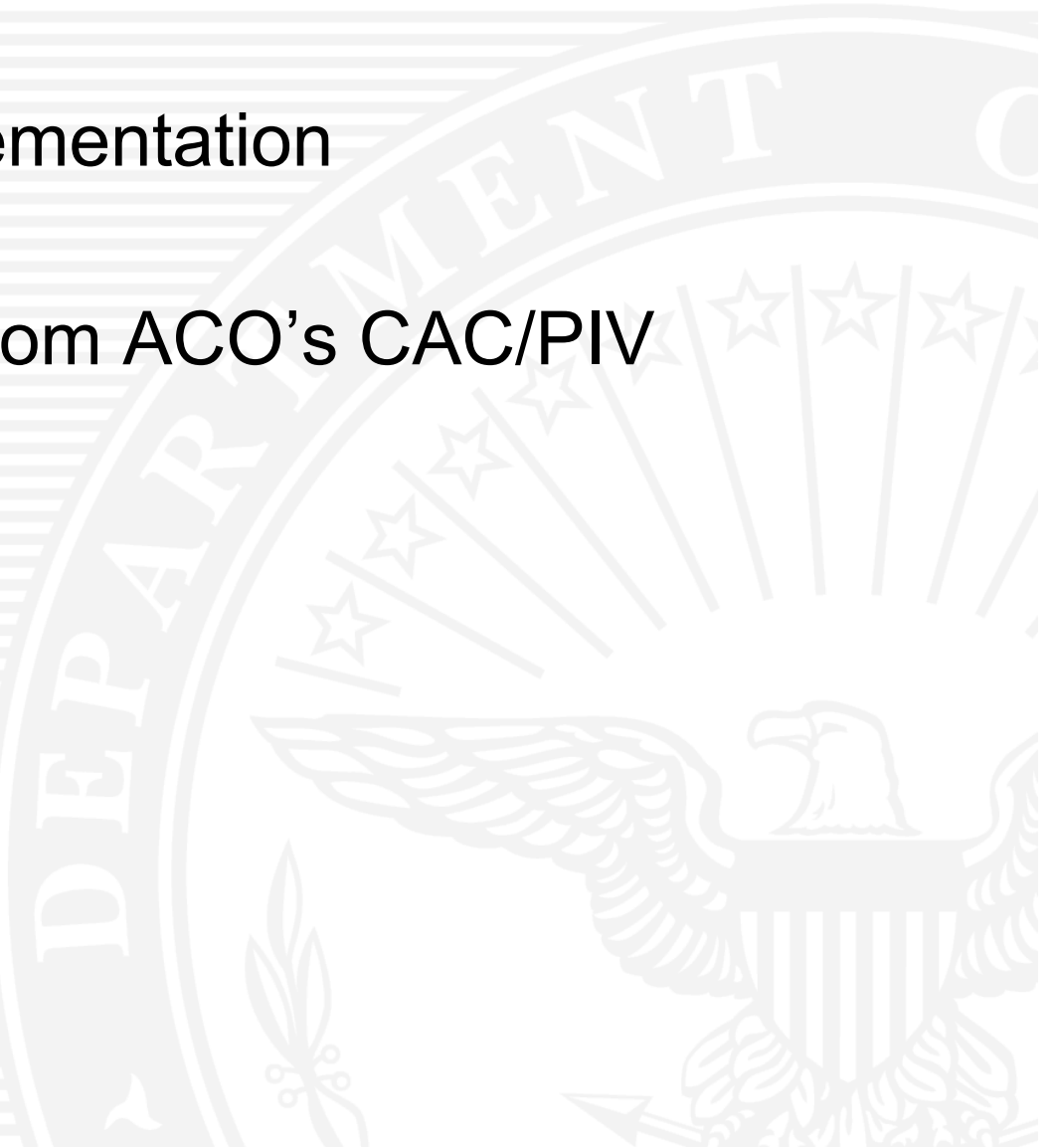


Purpose

Provide practical considerations and lessons learned to the IAB from the Access Card Office's (ACO) pilot CAC/PIV Implementation

Agenda

- CHUID at the Implementation
- Lessons Learned from ACO's CAC/PIV deployment
- Questions



CHUID: Things to Think About

- CHUID = Cardholder Unique Identifier
- CHUID is more than a number- it's *data*
 - More data = better decision making
- The **entire** CHUID is much bigger than a typical legacy PACS credential
 - This can potentially stress or cause issues with existing PACS systems
- Getting the entire CHUID for every transaction is not entirely necessary

 Typical Credential < 10 Bytes

CHUID

~3K

CHUID: Things to Think About

- Important CHUID Components

FASC-N (25)

EXPIRY DATE (8)

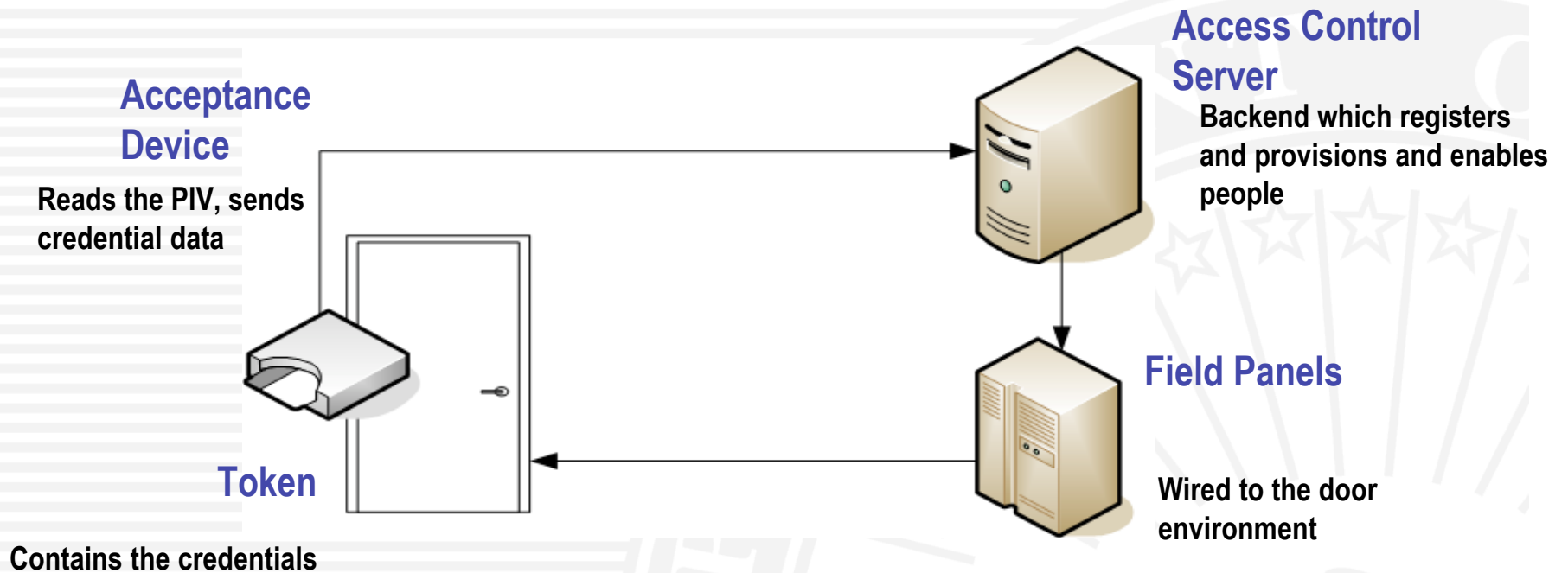
SIGNATURE (2K)

- The FASC-N contains several important data elements
 - **Person Identifier** is the unique reference to that particular person
 - **Credential number** is the unique reference to that particular person's credential (within that agency and system)
 - **Person / Organization Association Category** is the affiliation of the individual to the sponsoring agency
- Expiration date is the expiration date
- Signature tells the PACS that the rest of the CHUID is valid
 - Important distinction: The signature uses the *issuer's* certificate, not the end user's

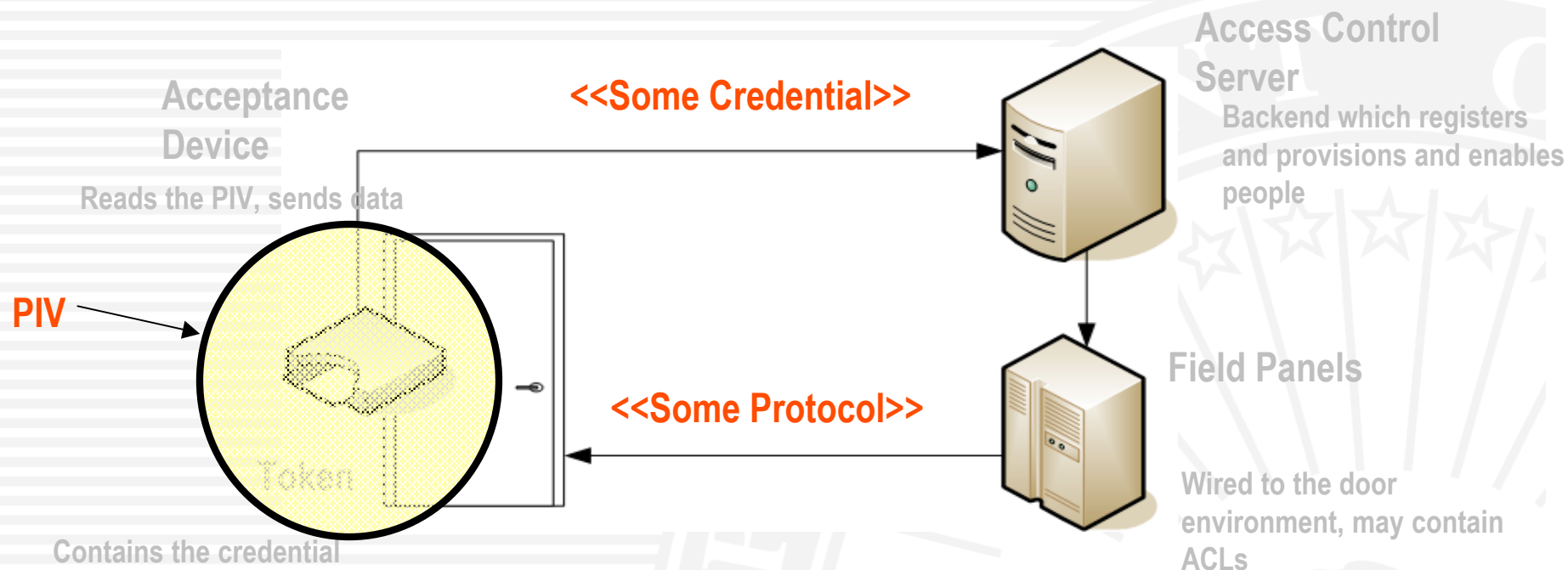
ACO Pilot Implementation

- Focused on Access Control
- Relatively Modern System
 - Both Contact and Contactless (14443) interfaces
- Two buildings / 2 Zones
- Some flavor of visitor management
- Existing credential was Contact-based CAC
- Rollout is 'soon'

Typical Access Control Architecture



Typical Access Control Implementation w/ PIV



- PIV defines (mostly) <<some credential>>
- <<some protocol>> is defined for reader communications and authentication methods
- Most of the rest is undefined!

ACO Pilot Implementation Goals:

- Implement PIV transitional for Physical Access
- Maximize existing ACO investments in People, Plant, and Process
 - Legacy Integration, Backwards Compatibility
- Forwards Interoperability
 - PIV Transitional to PIV End-State
- Seamless as possible to end-users
- Minimal disruption of day-to-day activities

Lessons Learned

- We weren't going to get there 'out of the box'
 - Perfectly understandable, but none the less a challenge!
- "Mixed Mode" is the reality for quite a while
 - Relatively easy to base priorities and project phases based on transaction and population volume (i.e. when exceptions become the rule)
- Establish or create a 'lowest common denominator' data element for each of your users
 - Will help unite stovepipes and silos down the road

Lessons Learned

- The Physical Access System (PACS) doesn't issue the credential
- Consequently, PACS user registration and provisioning is inverted (outside->in vs. inside out) in the PIV model
 - Retrofitting and outfitting existing and new users needs attention
 - Transition phases and credential binding are important to this phase

Lessons Learned

- There is a need to reconcile or resolve enterprise data and policies with local data and policies
 - Should always be a risk-based decision
 - Not super hard, just needs to be addressed
 - Local knowledge is still the best knowledge
- Protocols and specifications tell you how to get data and apply meaning to the data; what they don't completely tell you is how to *think* about it, and more importantly, what to *do* about it
 - This is good

Lessons Learned

- PIV Authenticity is easy; validity is harder to achieve
 - PIVS / CACs are self-consistent via the security objects and CHUID signatures
- Backend Transactions are needed to close the loop on an individual's status and reduce certain risk exposures
 - CRLs are good, but not complete

Practical Considerations

- Baseline or is key to the key to an PIV implementation plan
 - OV 1/2s is a great place to start w/ stakeholders
- Figure out which pieces of the puzzle can or will move and in what way
 - For example, ACO kept their existing PACS system but the PACS could be modified to some extent
 - Where and how people get cards is pretty important
- Identify the capability gaps and go from there

Practical Considerations

- Testing couldn't be more of a pain
 - True for vendors, integrators, and agencies
 - There is too much 'new' for effective training
- Every PIV implementation can and will be different
 - Mandatory data <> technical interoperability
 - 14443 / <Pick a Specification> <> technical or operational interoperability

Practical Considerations

- Look for flexibility and dynamicism everywhere in the solution
 - Technology- readers, field panels etc
 - Business processes
- The more often the PACS examines the data, the better

Practical Considerations

- Start with the most secure and ‘pure’ implementation and then work backwards as reality checks in...but keep an eye on the future and move forward
 - Implement processes to continually raise the bar

Questions

- Contact: Eric Hildre
- EHildre@technologyindustries.com

