Smart Card Alliance

Implementing PIV in EPACS

Kevin Kozlowski
XTec Incorporated

Topics

- Evolution of PACS
- Security Foundations
- 5 Myths
- Challenges to Implementation
- Mitigation & Best Practices
- Examples
  - Multi-Tenant Facilities
  - Large Throughput Locations
  - Existing Infrastructure

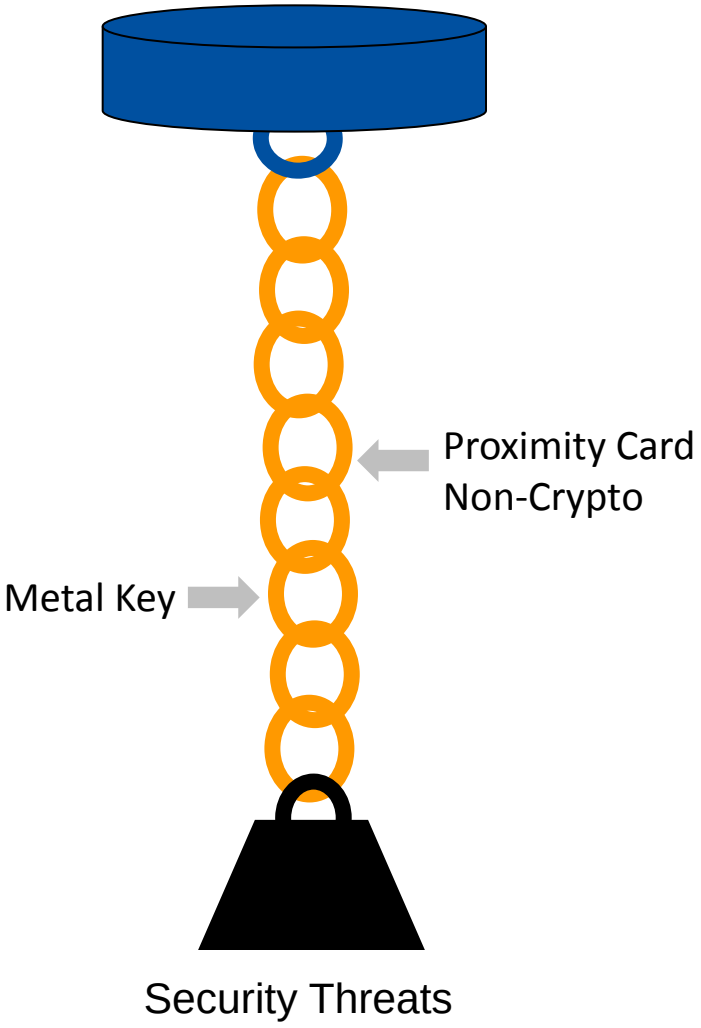
Smart Card Alliance

XTEC™

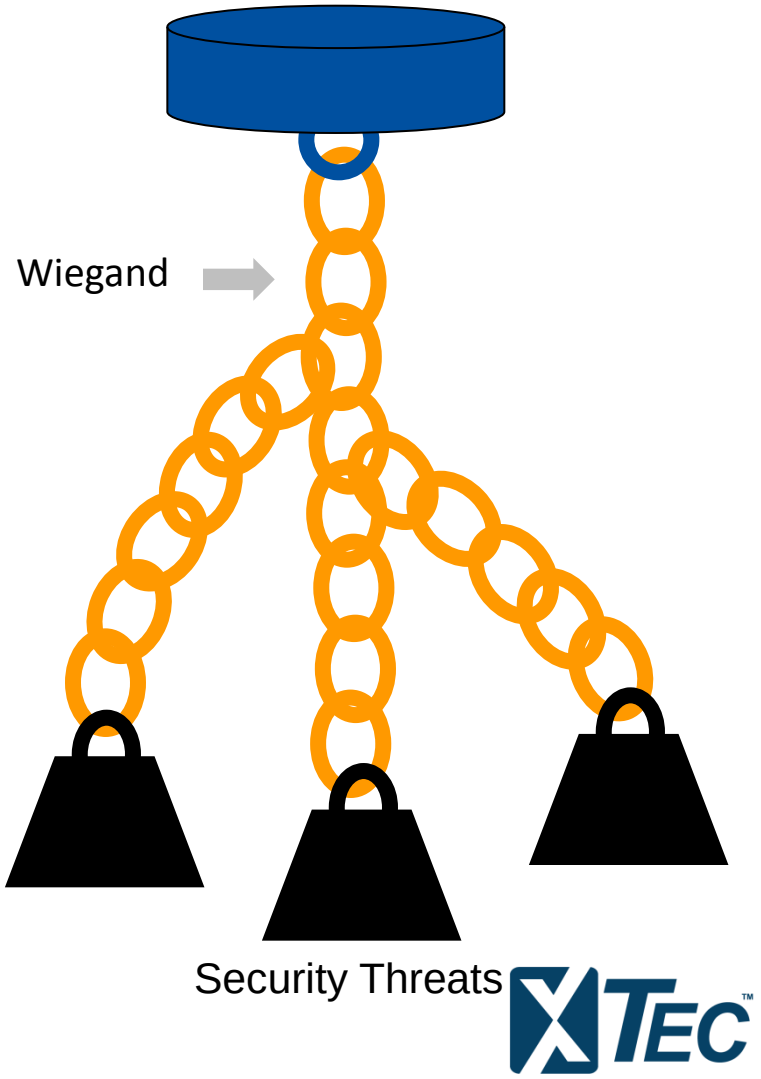
Authentication and security solutions you can trust.℠

Evolution of PACS

Legacy Approach



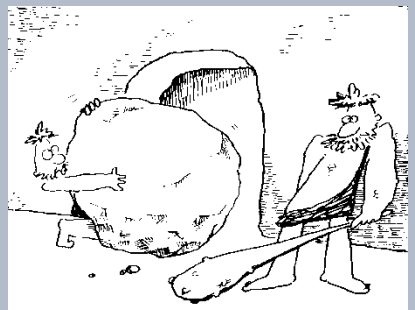
Hybrid Approach

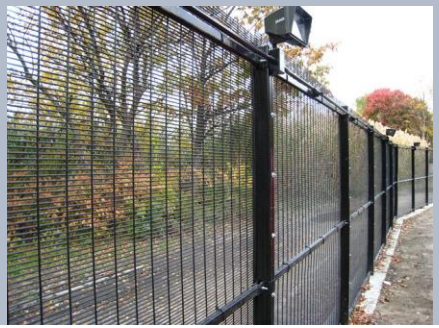


Smart Card Alliance

XTEC™

Evolution of PACS



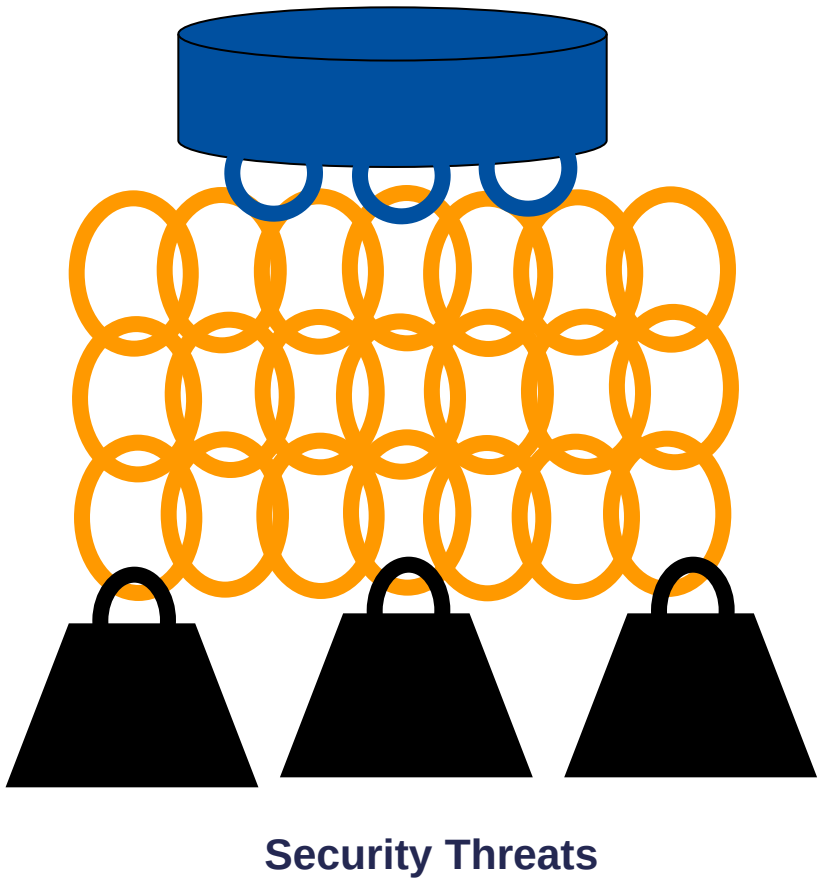


Smart Card Alliance

FICAM PACS

Threats affect only the intended components.

Failure of one component does not affect others.



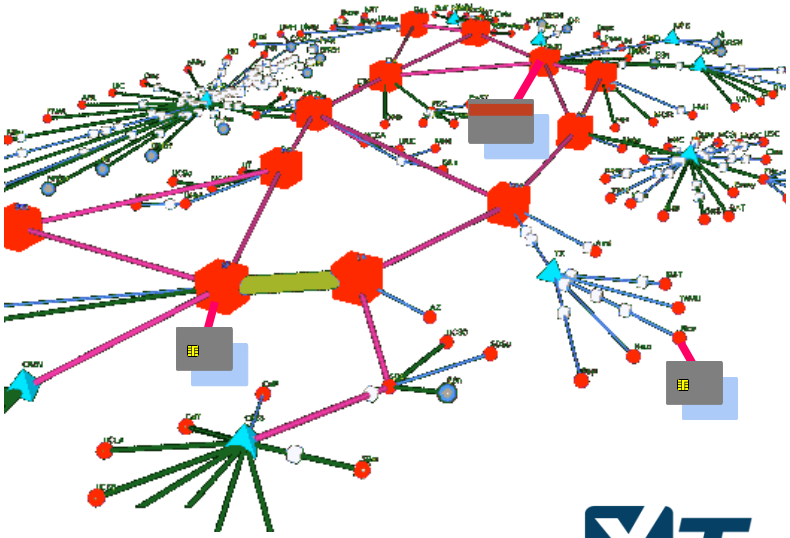
Smart Card Alliance

XTEC

FICAM PACS

FICAM Approach

- New identification method
- New technology for data exchange
- Two-way communications
- Cryptography
- Cloud computing
- Interoperable
- Nationwide locations
- Multi-tenant facilities



Smart Card Alliance

Security Foundations

Authentication

Binding of a person's credentials

Confidentiality

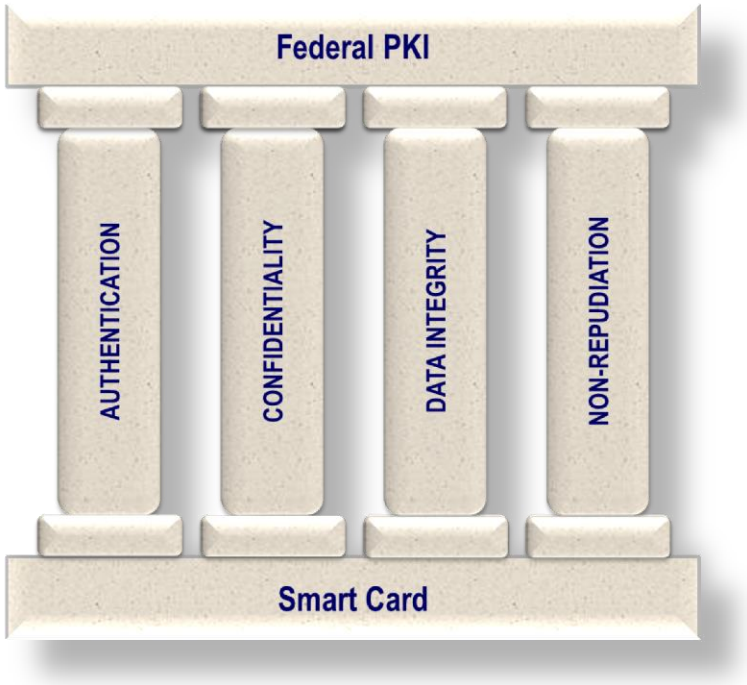
Encryption/Privacy

Data Integrity

No tamping or corruption of the bits

Non-Repudiation

Cannot deny performing that transaction



Smart Card Alliance

XTEC

Reasons for Adopting Smart Cards

- Flexibility
- Multiple Applications
- Greater Storage Capacity
- Dynamic loading of Applications
- Read/Write Capability
- Tamper-resistant
- Rapid electronic authentication
- Interoperability
- ***Improve Security***

Smart Card Alliance

XTEC

5 Most Common Myths

5 Most Common Myths

1. **The Card is the Problem**
   - Use GSA Test Tool
   - Path Validation tool
   - Antenna check
   - Issuer relationship

The culprit can be: **card, reader, wiring, network, power, availability, firmware, certificates, PIN, recent system updates, new cards, cardholder error etc.**

Smart Card Alliance

XTEC

5 Most Common Myths

2 **Readers are PIV & PIV-I Ready**

- Many are not
- Trouble recognizing PIV-I
- Read FASC-N 9999

Get a PIV-I card and test the registration and output.
May be capable of it but not PIV-I ready.

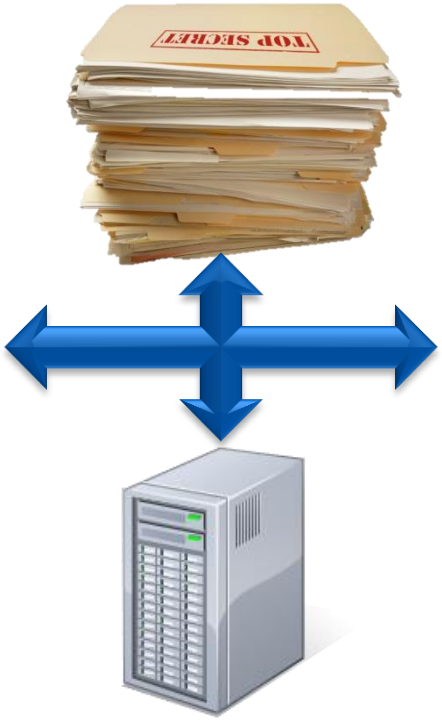
Smart Card Alliance

XTEC™

5 Most Common Myths

3 I Only Need to Secure Selected Access Control Points

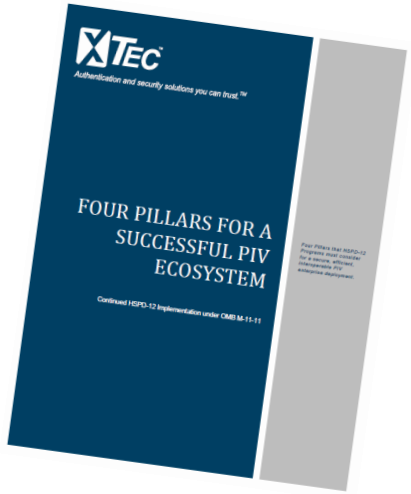
- True that not one size fits all
- Only as strong as your weakest link
- If prox can be presented at the side door…..

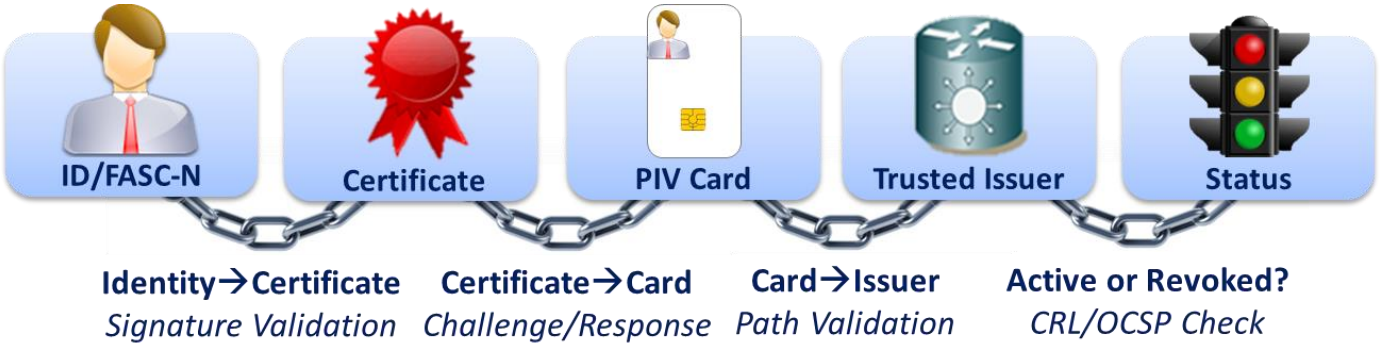


5 Most Common Myths

4 **Encryption = Security**

- Encryption = **Privacy** but NOT security
- Replay, MITM, Skimming, Sniffing, Cloning, Counterfeiting etc.
- Challenge/Response
- Cryptography is not optional





Smart Card Alliance

XTEC™

5 Most Common Myths

5 **Too Expensive**

- Does not need to be over complicated
- Design of security system
- Value of security
- Cost if risks materialize

Target breach cost $148 million in just one quarter

Home Depot cost at $62 million, estimated to double

Smart Card Alliance

XTEC™

Authentication Basics

Use the Card Capabilities

- Consider two or more factors.
- Tokens must be Tamperproof or Tamper-evident.
- Biometric templates must never be divulged.
- Challenge / Response mechanisms should always be used.
- Authentication transactions should always utilize unique keys per session to prevent playback.

Smart Card Alliance

XTEC™

Challenges to Implementation (Management)

Minimum Level Security Needs

- Convenience over Security

End User Adjustment

- Contact v. Contactless v. Prox
- Timing
- Mandatory for entry

Unknown Card Population

- Various issuers = Various CA's
- Registration & Provisioning
- Solving card/reader issues

Smart Card Alliance

XTEC™

Challenges to Implementation (Technical)

Credential format & data

- Duplicate identifiers
- Identifier Collision
- Missing certificates
- Expired certificates
- Certificate updates
- Unknown PIN or card locked

Existing or new infrastructure

- Revocation and validation checks
- Certificate Authority
- CRL, OCSP
- Authentication

Smart Card Alliance

XTEC

Mitigating Challenges

Management Challenges	Mitigation Recommendations
Minimum Security Needs	You don't need systems with 3+ vendors/servers/backend products to be compliant & secure, always require authentication.
End User Adjustment	Training, education, better communication.
Unknown Card Population	Prepare for what you will see; logistics, technical and policy.

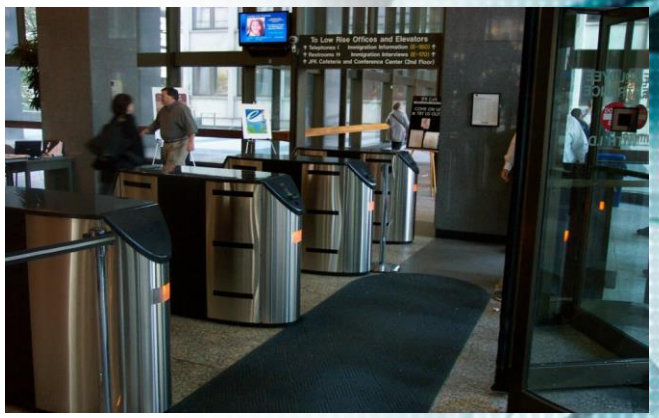
Technical Challenges	Mitigation Recommendations
Credential format & data	Card issuer relationship, prepare for different scenarios
Existing or new infrastructure	Seamless checking, conduct pilot/demonstration with real cards/equipment, gauge benefits to other areas like LACS.
Authentication	Analyze throughput and plan for a learning curve, do not cut corners that compromise security/compliance, explore all compliant authentication mechanisms.

Example Use Cases

Multi-Tenant Facilities

Specific challenges with various card issuers

- More CA, CRL/OCSP infrastructure
- Different Certificate Paths



Identifying card population

- Before implementation cutoff

Phased Implementation

- Cannot flip a switch
- Avoid chaos by easing end users into process

Communications

- Key to management and end user challenges

Smart Card Alliance

XTEC™

Large Throughput Locations

Testing throughput

- Average cardholders at each location
- Day of week, time of day

Determining best method or hybrid of methods for high throughput locations/times

- Asymmetric and Symmetric combination

Card + PIN

- Perceived as taking too much time

Smart Card Alliance

In Closing

Recognize security is an ongoing process

Use existing network and PKI infrastructure when possible

Remember anything from the card, reader, wire, network, power, availability, firmware, certificates, PIN, recent updates etc. can be a culprit

If you expose even one door, expect that to be the door that is attacked

Explore options to shorten “time- at- the- door”

Keep it simple

Smart Card Alliance

XTEC™

Smart Card Alliance

Thank you.
Questions?

Kevin Kozlowski, Executive Vice President
kkozlowski@xtec.com
703-547-3524
www.xtec.com

XTEC™