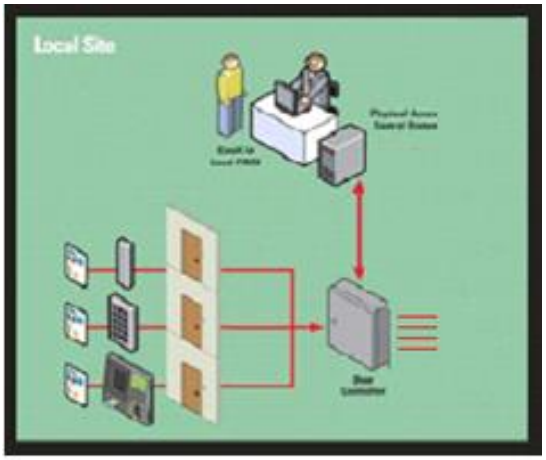
PIV in EPACS Vn. 3.0 PACS Threat vectors

Lars R. Suneborn
Smart Card Alliance

The starting point



Logo

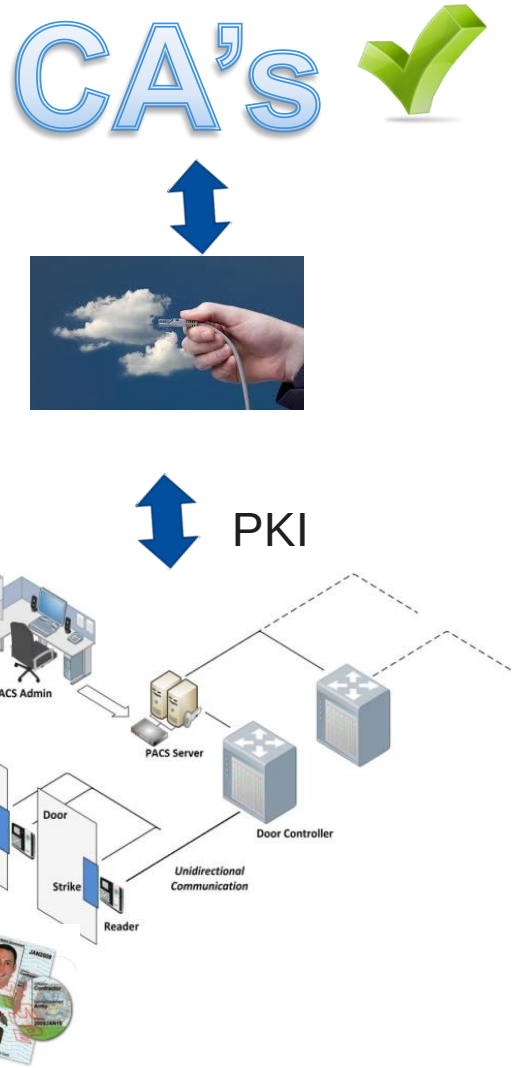
Common PACS threats

Credential

- Inadequate identity proofing policies
- Non-standardized issuance policies
- Non-standardized appearance
- Visual Credential counterfeiting
- Electronic credential counterfeiting
- Social Engineering
- Identifier collision

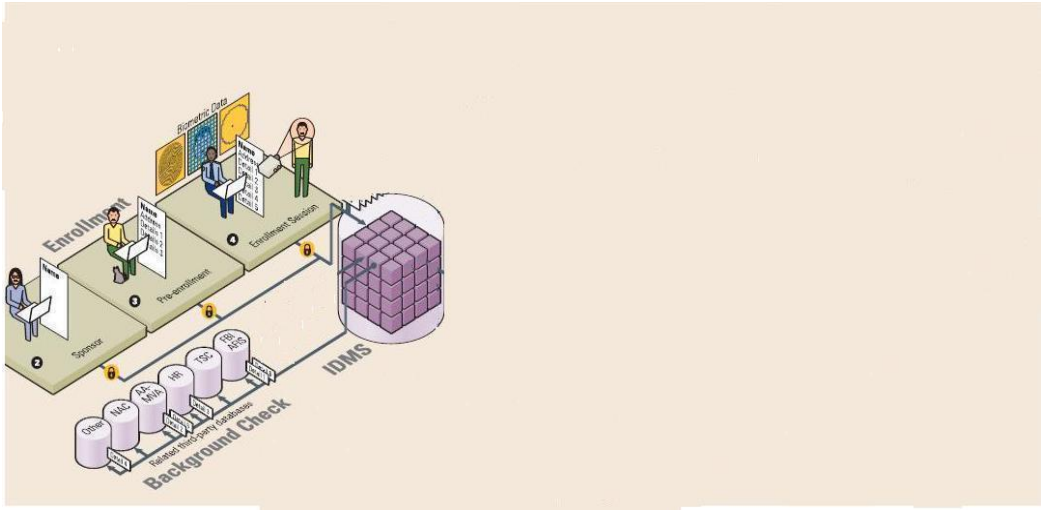
PACS manipulation

- Reader manipulation, replacement
- Communication line
- Controller manipulation, replacement
- Social Engineering
- PACS Operator



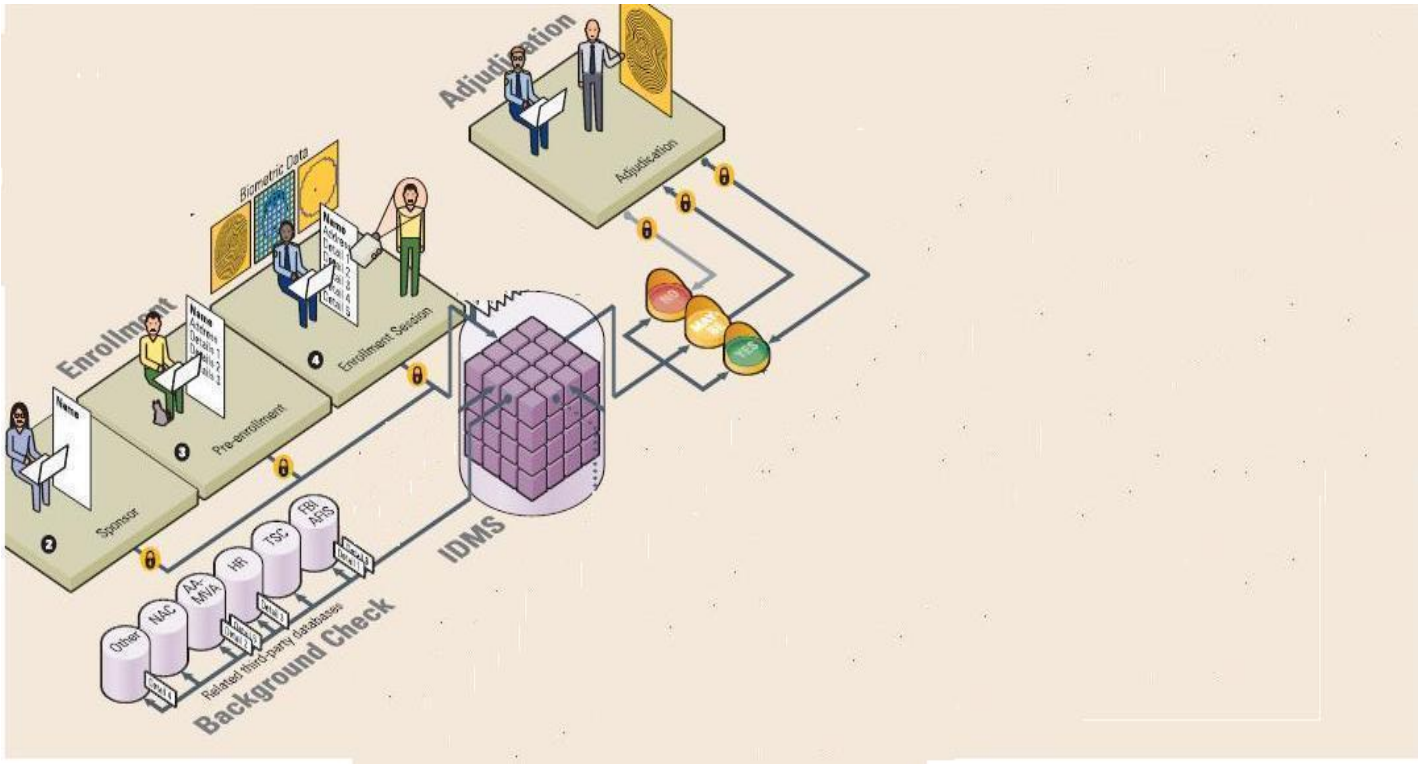
Credentialing Process - Policy

- Applicant
  - Photo,
  - Biometric
  - Breeder Documents
- Issuer
  - Sponsor, Registrar
  - Background investigation



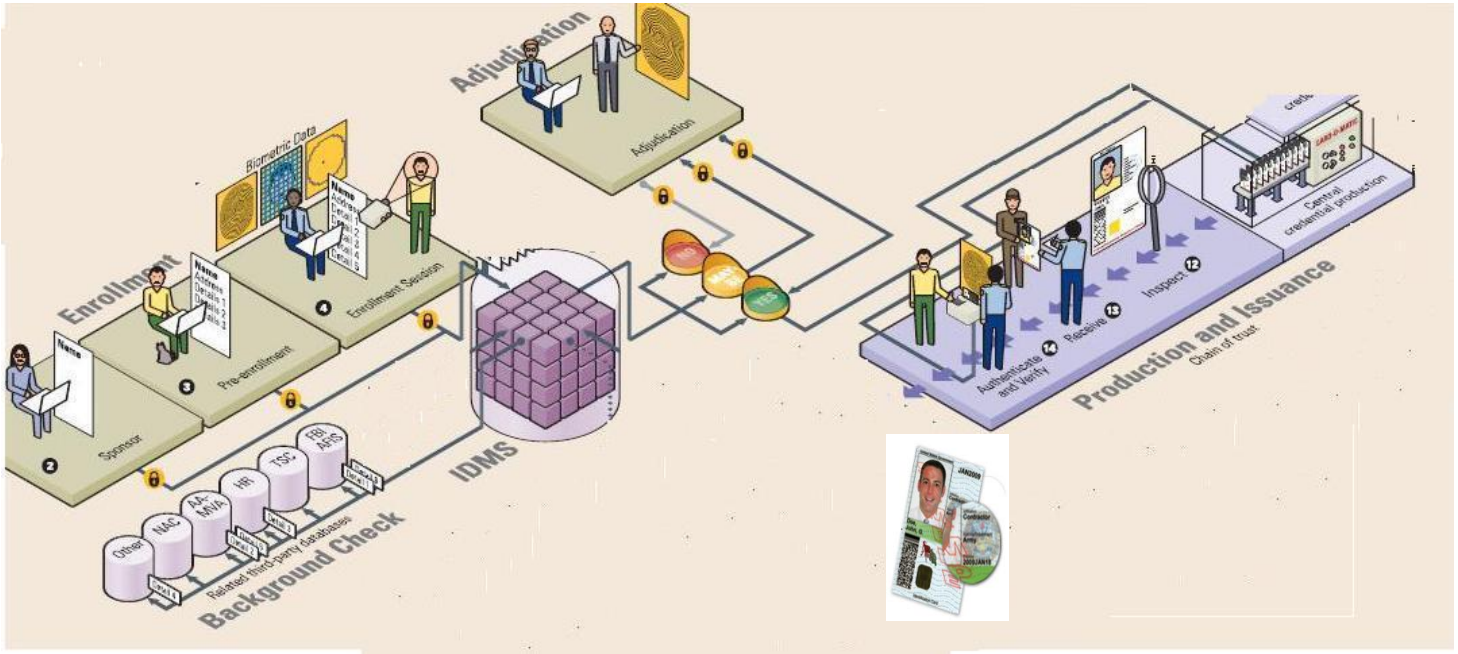
High Assurance Credential - Policy

- Adjudication

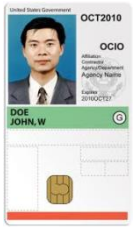


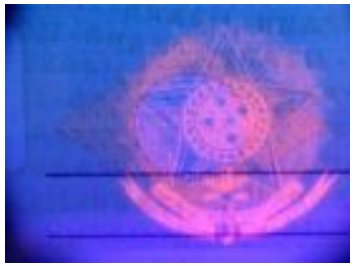
High Assurance Credential - Policy

Data model, Pre–personalization, Production, Issuance, Key creation



Graphic personalization visual counterfeit countermeasures





Level 1 Security

- Naked eye
- Standardized design
- Exact and consistent appearance
- May use special print techniques

Level 2 Security

- Requires trained people, simple equipment
- Hologram, ghost image

Level 3 Security

- Specialist examination
- Specialized print equipment
- Specialized inspection equipment
- Microtext
- Optically variable images

Identifier collision

May not be an attack attempt

- An identifier collision occurs when the identifier used by the PACS is present in more than one card.
- NIST SP 800-73-4 2nd Public Draft mandates the use of the UUID (RFC 4122) for the Card Identifier for PIV

Countermeasure

- PACS must process the full identifier
- Registration process must validate identifier origin

Electronic counterfeiting

Attack method

- Attacker obtains a card and makes a copy of it, then uses it to gain access.
- Attacker substitutes data object on valid card.

Countermeasure

- Use card authentication (PKI-Auth or PKI-CAK).
- Verify the security object on the card
- Authenticate another object on the card in addition to the biometric and verify that the identifiers for both objects are the same.

Social Engineering - Use of unreported lost or stolen card

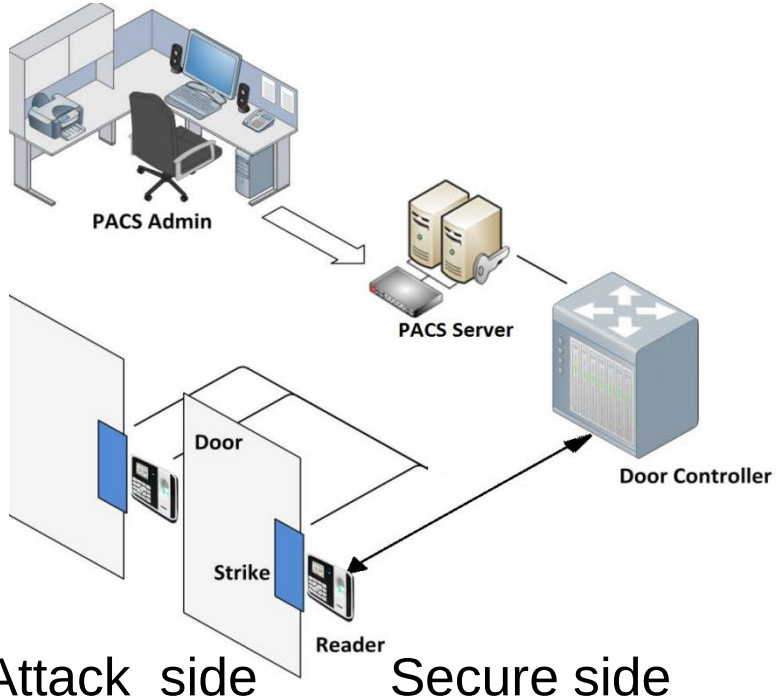
Attack method

- Attacker persuades a cardholder to give them possession of the card.
- Attacker steals or finds a card and uses it to gain access, before it is reported lost or stolen.

Countermeasure

- Use an authentication mechanism that requires PIN or biometric verification of user's identity.
- Establish a policy and process for reporting & de-provisioning lost/stolen cards.

Reader compromise, replacement



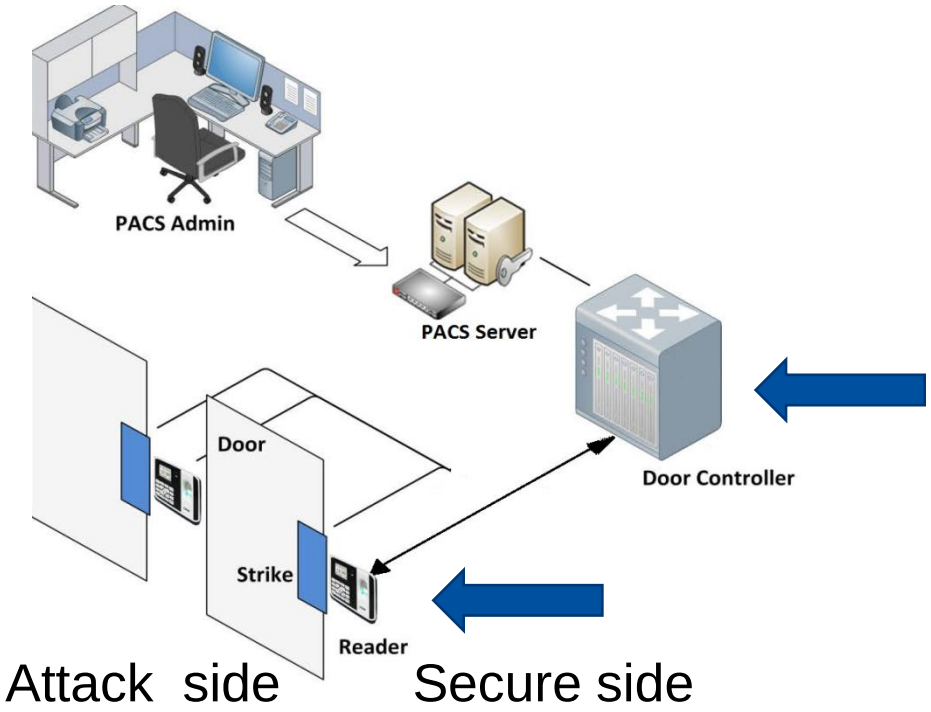
Attack method

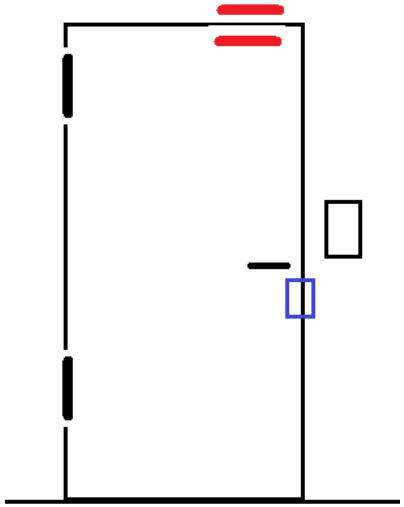
- Attacker inserts device at the PACS reader to capture & replay information from the reader that can be used to gain access.

Countermeasure

- Use PKI-CAK or PKI-Auth
- Tamper detection
- Video activation
- Maintenance policies

Physical PACS component compromise





Attack method

- Attacker tampers with PACS components directly to gain access
- Attacker keeps the door from closing properly

Countermeasure

- Protect all PACS components with tamper detection
- Door position sensor
- Exit device
- Keep in secure area

PACS Threat - Insider attack

Attack methods

- Attacker reprograms PACS polices Access rights, Intrusion detection, video
- Attacker reprograms authorization for cohort or own authority
- Attacker harvest identifiers of PACS user database
- Attacker creates a factious user

Countermeasure

- PACS Operators role definition
- Use same level authentication as required for physical access
- Encrypt PACS user records
- Control non-PIV visitor cards
- Log all operator activity

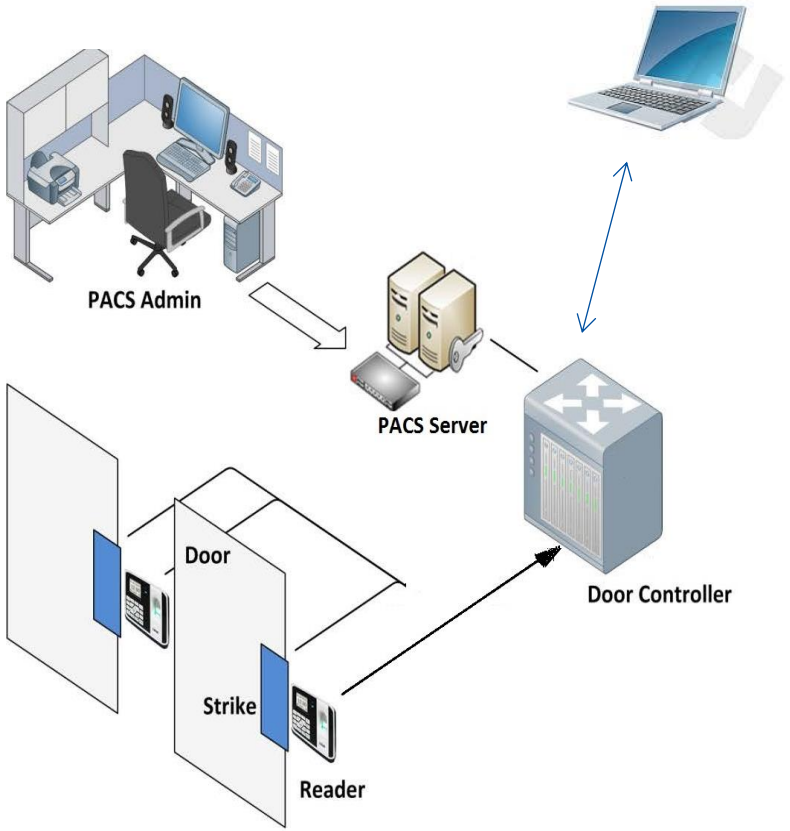
PACS Threat - Server impersonation

Attack Method

- Attacker substitutes server with non-authentic server to manipulate controller database, or stored policies

Countermeasure

- Encryption of data transmitted over server-controller communication line
- Communication line supervision



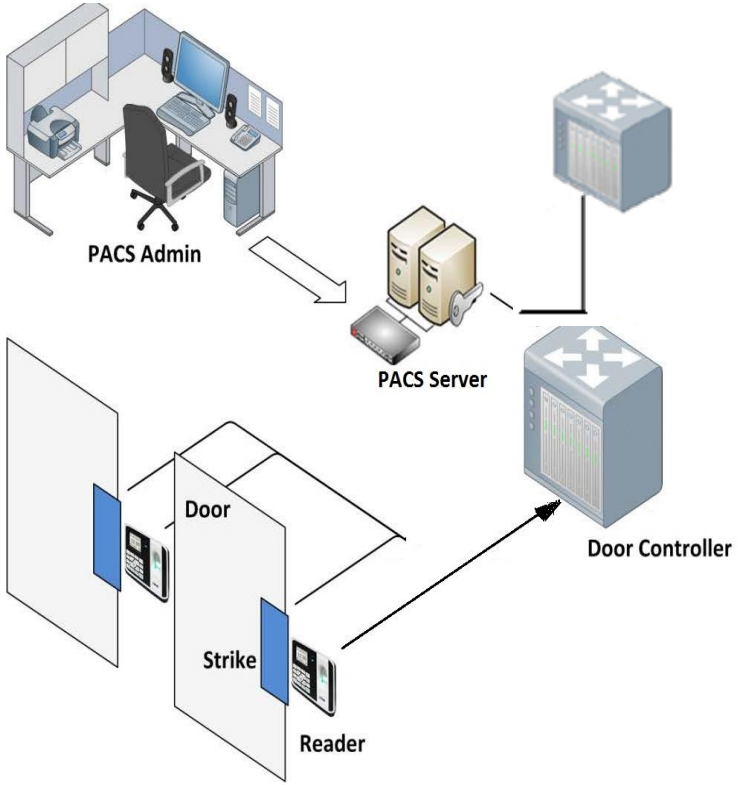
PACS Threat - controller impersonation

Attack Method

- Attacker substitutes controller to manipulate devices connected to authentic controller

Countermeasure

- Encryption of data transmitted over server-controller communication line
- Communication line supervision
- Hardware library with unique device ID
- Device network log-on only through authentic server



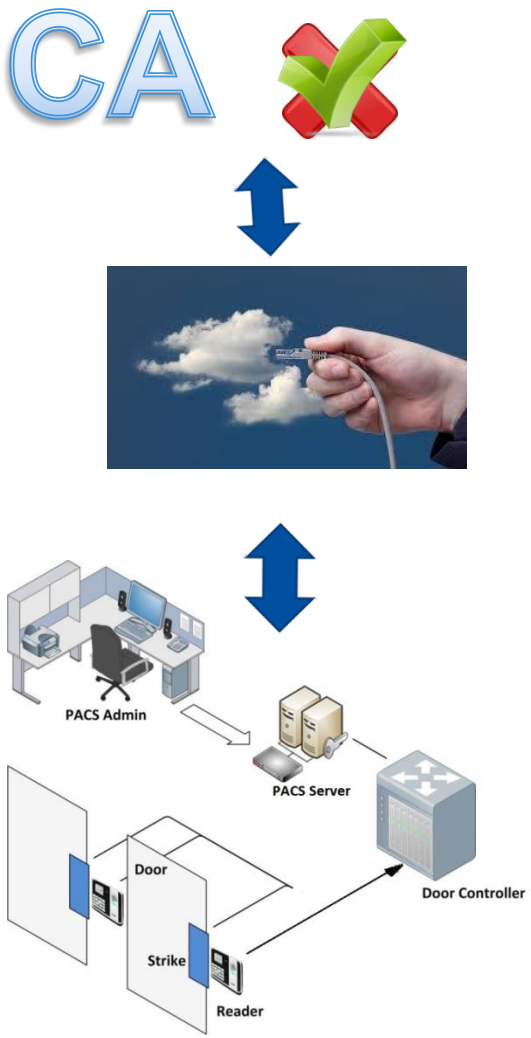
PACS Threat - Insider attack; trust anchor

Attack Method

- Operator modifies trust store to accept bad CA

Countermeasure

- Operator role definition
- Log all operator activities
- Personnel security policies



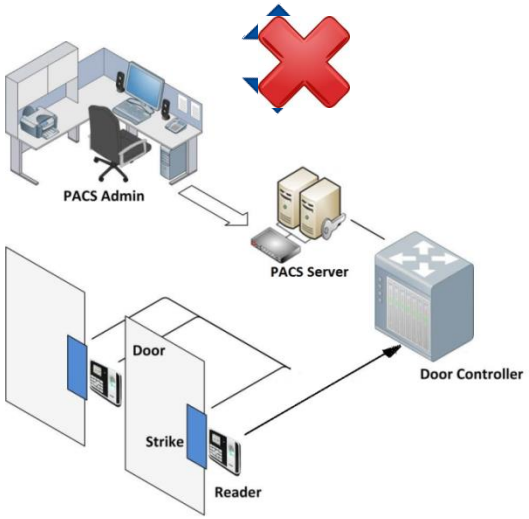
PACS Threat - Denial of Service attack

Attack Method

- Attacker disables external network connection to prevent CRL update
- Allow access to bearer of revoked credential

Countermeasure

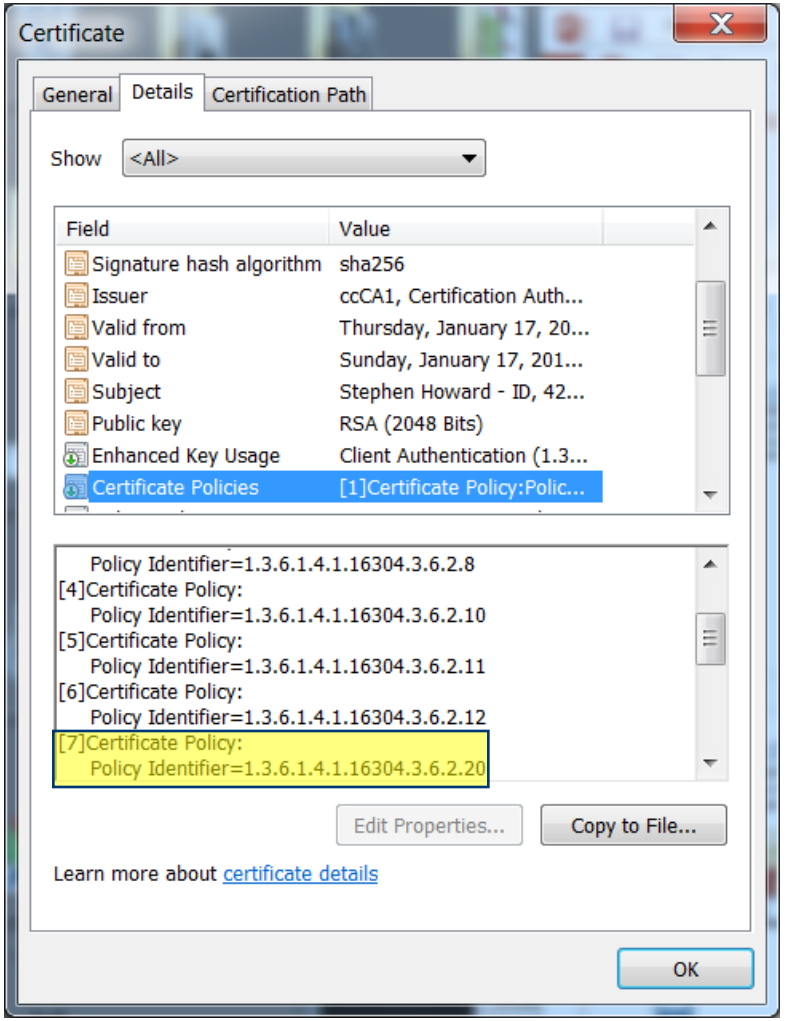
- Cache validation status in local PACS
- Supervise all communication lines; alert when connectivity is lost.



Policy OID

- Commonly, you might think of the following names for policies
  - '**rudimentary**' or '**basic**' (providing very little confidence the certificate holder is who they say they are)
  - to '**PIV**' or '**PIV-I**' (a very high level of confidence)

- For Cassidian Communications' CA, PIV-I is identified as
  - 1.3.6.1.4.1.16304.3.6.2.20



Threats & Countermeasures guidance

	Secures against cards that are						
Auth Modes ↓	**Revoked**	**Counterfeit or Altered**	**Copied or Cloned**	**Lost or Stolen**	**Shared**	**Auth Factors**	**SP 800-116 Security Area**
Chip Serial #						None	Uncontrolled
FASC-N/UUID	Local					None	Uncontrolled
CHUID+VIS	✓	✓				1	Controlled
PKI-CAK	✓	✓	✓			1	Controlled
PKI-AUTH	✓	✓	✓	✓		2	Limited
PKI-AUTH+BIO	✓	✓	✓	✓	✓	3	Exclusion

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

SUMMARY

- When properly used, PIV & E-PACS:
  - Enforces proper identity vetting and issuance policies
  - Validation of trusted origin
  - Mitigate common threat vectors through electronic authentication
- Detects:
  - Non -compliant id vetting and issuance policies
- Prevents:
  - Use of valid credential by non-owner
  - Use of revoked credential
  - Use of Forged or duplicated identifier
- Expanding beyond U.S.

Summary

- Complexities requires new competencies, certified system integrators
  - GSA lead in guiding & enhancing competencies

- Is FICAM E-PACS IT or Security
- GSA editing Schedule 70 SIN 132-62 and creating SIN 162-64 to simplify procurement (and selling) FICAM E-PACS components and services

Thank You!

Lars R. Suneborn, CSCIP/G; CSEIP
Director, Training Programs
Smart Card Alliance
Phone M: 1 703) 904 2389
Phone O: 1 703) 794 7552
E-Mail: Lsuneborn@smartcardalliance.org