Physical Access Control Systems and FIPS 201

Physical Access Council

Smart Card Alliance

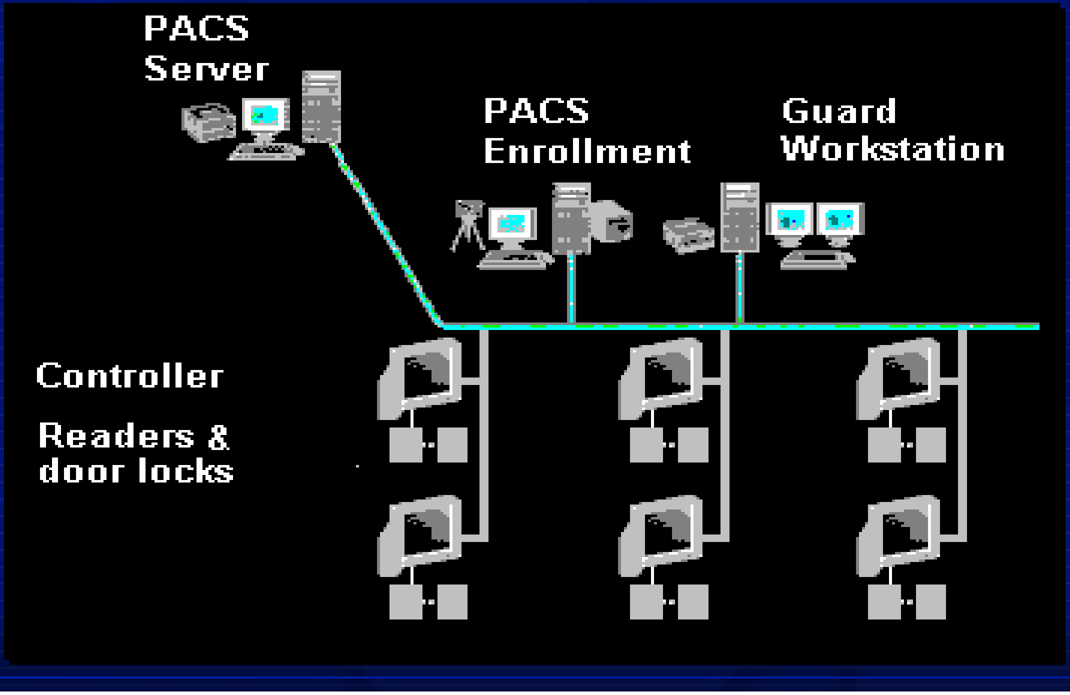
December 2005

Topics

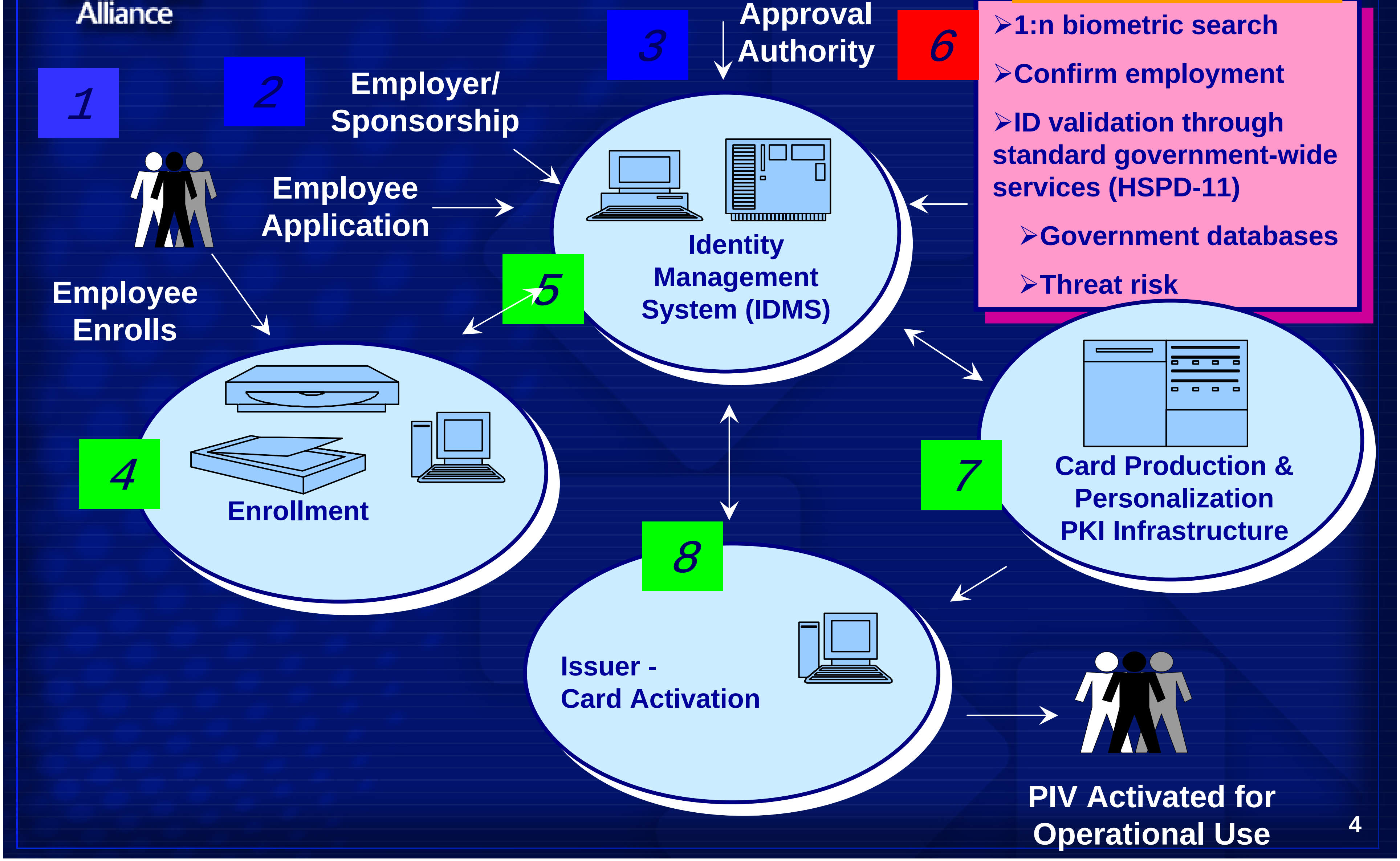
- ❖ Introduction: PACS Overview
- ❖ PIV Card PACS-Related Components
- ❖ PACS Readers
- ❖ PACS Panels & Hosts (Servers)
- ❖ PACS Infrastructure (Cabling, Communications and Interfaces)
- ❖ PACS & Biometrics
- ❖ Privilege Granting & Revocation
- ❖ PACS Certification & Accreditation
- ❖ Conclusions

Introduction: Traditional PACS

- System operator verifies an employee's identity according to organizational policy
- User credential is created and enrolled at PACS enrollment station
- Credential data and access privileges are downloaded to controllers database
- Readers at control points read data from credential and send data to controller for access decision



Introduction:
PIV Identity Verification and Issuance



1

2 Employer/ Sponsorship

3 Approval Authority

Employee Application

Employee Enrolls

4 Enrollment

5 Identity Management System (IDMS)

6

Identity Verification

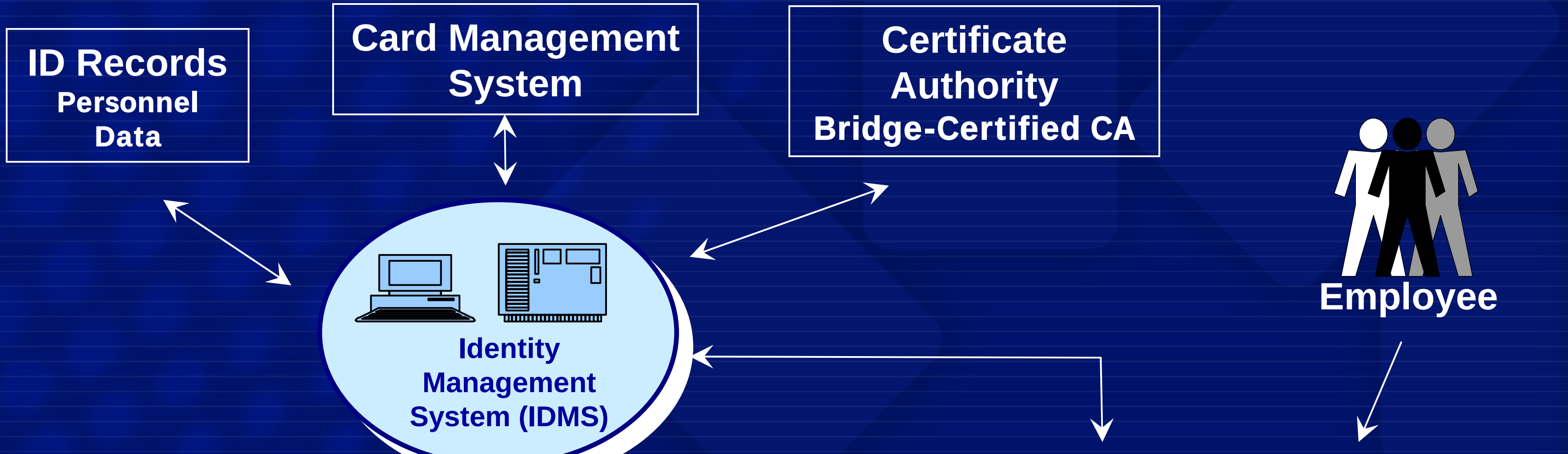
- ➢1:n biometric search
- ➢Confirm employment
- ➢ID validation through standard government-wide services (HSPD-11)
  - ➢Government databases
  - ➢Threat risk

7 Card Production & Personalization PKI Infrastructure

8 Issuer - Card Activation

PIV Activated for Operational Use

Introduction: FIPS 201 – PACS Relationship



ID Records

Personnel Data

Card Management System

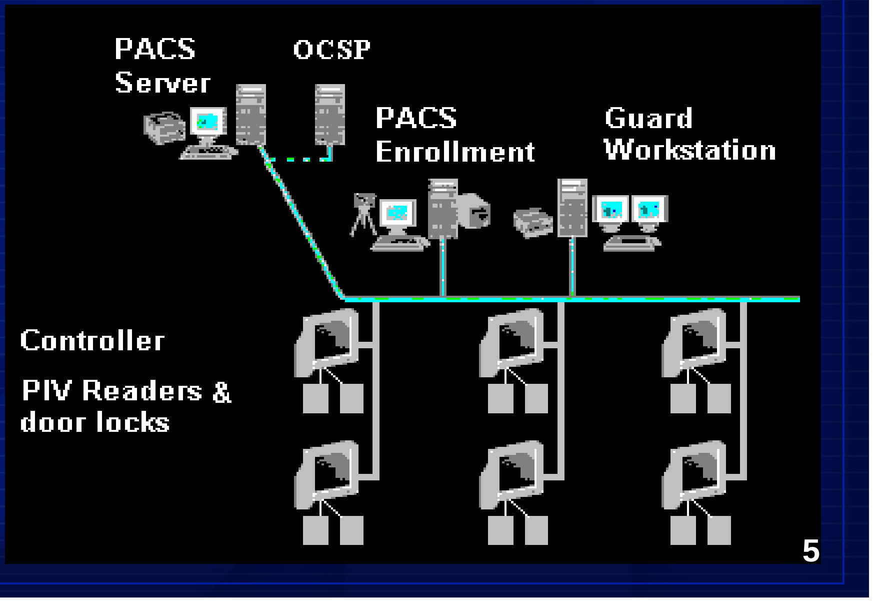
Certificate Authority

Bridge-Certified CA

Identity Management System (IDMS)

Employee

- A PIV cardholder arrives
- OCSP (or other means) confirms with IDMS that credential is still valid
- Enrollment officer confirms ID with PIV and biometrics
- Enrollment officer confirms access requirements
- PACS enrollment officer adds PIV card CHUID to PACS
- PACS enrollment officer registers physical access privileges to PACS
  - Uses low or medium assurance profile
- PACS performs periodic validity checks with IDMS



Smart Card Alliance

Physical Access Control Systems and FIPS 201: PIV Card Components

Physical Access Council

Smart Card Alliance

Smart Card Alliance

PIV Card Issues/Recommendations

- ❖ FASC-N Usage Requirements – How many of the FASC-N BCD digits (14 up to 32) need to be read/processed to be considered FIPS 201 compliant?
  - ❖ Since PACS v2.2/2.3 states that a minimum of the first 14 BCD digits (Agency Code, System Code, and Credential Number) need to be used to ensure a unique number across the Federal Government, this should be the minimum required for FIPS 201 compliance.
- ❖ GUID Usage Requirements – Cannot currently be relied on to be a unique number across the Federal Government.
  - ❖ Guidance should be provided to PIV Issuers on using unique IPv6 addresses for the GUID.
  - ❖ Since there is no currently established standard for assigning a GUID and its uniqueness cannot be ensured, it should only be used locally.

Smart Card Alliance

PIV Card Issues/Recommendations

- GUID Usage Requirements – What is the timeframe for implementing this?
  - Since OMB policy has set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure, this should be the target implementation date.
  - Work should begin as early as possible to meet this target implementation date.
- Expiration Date Usage Requirements – When and/or how often does this need to be checked?
  - The PIV card contains multiple expiration dates (e.g., printed on the PIV card, inside CHUID, printed info buffer (optional), within PKI certificates).
  - Expiration dates need to be synchronized.
  - This should initially only need to be checked/validated at the time of initial registration and not at each access control event.

PIV Card Issues/Recommendations

- CHUID Asymmetric Signature Usage Requirements - When and/or how often does this need to be checked?
  - The CHUID asymmetric signature should initially only need to be checked/validated at the time of initial registration and not at each access control event.
  - At some later time this could be expanded as infrastructure matures.
- Card Authentication Key Usage Requirements - When and/or how should asymmetric keys be used in PACS?
  - PACS 2.2/2.3 includes the use of symmetric keys for PACS in the high assurance profile, but does not include the use of asymmetric keys mentioned in FIPS 201 and SP 800-73.
  - To ensure interoperability, this needs to be made mandatory and the PACS document must be updated to include this as a PKI high assurance profile.

Smart Card Alliance

PKI High Assurance Profile: Strong, Standards-based Token Authentication

Physical Access Council

Smart Card Alliance

Smart Card Alliance

Recommendation and Benefits to Use Certificates for Authentication

- ❖ Uses industry standard and FIPS 201 compliant authentication methods with x.509 certificates (Card Authentication Certificate)
- ❖ Uses asymmetric authentication that is already required to read CHUID signature (no additional requirements for reader functionality)
- ❖ Provides acceptable physical access performance with dual-interface credentials
- ❖ Card Authentication Certificate does not require use of PIN for high throughput physical access applications
- ❖ Provides common solution across Federal agencies
- ❖ Eliminates key management issues with Shared Secret Keys

Current PACS 2.2/2.3 Authentication Profiles

- **CHUID Low Assurance**
  - Free read data, sent to panel
  - Small volume of data
  - Low anti-counterfeiting, low anti-tampering
- **CHUID Medium Assurance**
  - Free read data, subset sent to panel
  - Medium volume of signed data
  - Low to medium (with security guard observation) anti-counterfeiting, higher anti-tampering
- **CHUID High Assurance**
  - Authentication key stored on card
  - Key verified by readers/panels holding Site Secret Key (SSK)
  - Can't use on a reader without a copy of an SSK
  - Compromise of an SSK could permit batch counterfeiting
  - SSK distribution/management challenges

Smart Card Alliance

PKI High Assurance Profile

- ❖ On-card generation of private key (RSA, ECC)
- ❖ Public key bound to card/FASC-N in X.509 certificate
- ❖ Standard card authentication certificate from SP 800-73, certificate profile from FICC
- ❖ Card verification without shared secrets (no SSK)
- ❖ Highest anti-counterfeiting
- ❖ Interoperation with logical security uses

Smart Card Alliance

PKI High Assurance Notes

- PKI-capable cards required (e.g., current dual-interface cards)
- Readers (or bi-directional panels) with real time clock and RSA/ECC signature verification required to use certificates (i.e., same level required for CHUID verification in medium profile)
- No on-card second factors (PIN, biometric) required for contactless use. Second/third factors would require use of contact interface (on-card) or panel-side match (i.e., same as the other profiles)

Smart Card Alliance

Physical Access Control Systems and FIPS 201: PACS Readers

Physical Access Council

Smart Card Alliance

PACS Readers: FIPS 201 Requirements

- FIPS 201 defaults to PACS 2.2 for access control – low, medium and high assurance profiles.
- There is not a requirement to read and output the entire CHUID to open a door.
  - Reading the entire CHUID would add more time to the actual transaction and could not all be processed by modern day access control systems.
- Enough information should be read to output either the FASC-N or the GUID and to be able to calculate the HMAC for a higher level of assurance. If the highest assurance security level is required, the reader will also need to be capable of symmetric or asymmetric keying. Another option would be passing the card certificate from the contact chip.
- Whether ISO 14443 is used for contactless or ISO 7816 is used for contact chips, output to the access control panels should remain the same since the same CHUID data is used through either interface.
- Read speed is not believed to be an issue if the system is only reading and outputting the FASC-N/GUID alone or with the HMAC. Read speed may be an issue with reading/verifying very large biometric images or meeting higher security assurance profiles.

PACS Readers: Issues/Recommendations

- ❖ **FIPS 201 defaults to PACS2.2 for access control, low, medium and high assurance profiles.**
  - ❖ NIST should consider updating FIPS 201 to reference PACS 2.3 or latest update.
- ❖ **Readers can be configured to output many different configurations to the panel. The data that is output will be dependent on whether the agency is working with a legacy installation or new installation.**
  - ❖ For legacy installations, each access control vendor’s system is different and may initially require different data imported from the reader.
  - ❖ For new installations, a minimum set of data to be passed from the FASC-N or GUID should be specified (e.g., 16 GUID digits).

Smart Card Alliance

PACS Readers: Issues/Recommendations

- **There has been no clear guidance from NIST or any government agency or committee on whether an access control card reader needs to go through conformance testing.**
- **There is an absolute need for NIST or some governing agency to publish a test data model set for an entire CHUID.**
  - Without an official data model set to test with, no reader vendor can truly build and test products to meet the SP800-73 "End Point" solution. This is an absolute must for the industry to deliver product in a timely manner.

Smart Card Alliance

Physical Access Control Systems and FIPS 201: PACS Panels and Hosts (Servers)

Physical Access Council
Smart Card Alliance

Smart Card Alliance

PACS Panels & Hosts: Overview

- **FIPS 201 does not specify requirements related to the physical access control system.**
  - Implementation is manufacturer specific.
  - Interoperability between PACS is not part of FIPS and therefore still open to interpretation by individual agencies.
- **There is a lack of formal protocol or standardization for the interface between PACS and IDMS.**
  - Industry should define the interoperability standard to support FIPS 201 functionality.

PACS Panels: Overview

- **Panels are configured by head-end (host), but can work standalone in offline mode to control door access. High throughput is required (e.g., turnstiles at start of shift).**
- **Cardholders are identified by matching card data from readers to cardholder data in panel database. Additional checks can be made on expiration date (either from card or from head end) and PIN.**
- **Connection to readers: Readers are connected to panel via Wiegand, RS-232/422/485, or other wired interface.**
- **Connection to head-end**
  - Card holder record including FASC-N fields or GUID, PACS expiration date, PIN, clearances

Smart Card Alliance

PACS Panels & Reader Data

- **There is a need to specify what data to use: FASC-N data or the full GUID. There are multiple data formats supported by the various reader vendors (e.g., 200-bit, 128-bit, 64-bit, 40-bit)**
  - For full interoperability across agencies, the reader FASC-N data should minimally include the following (14 digits)
    - Agency (4 digits)
    - System (4 digits)
    - Credential (6 digits)
  - For legacy applications, a fewer number of digits can be output, but the number will not be unique across Federal agencies and must be assessed for risk by local security manager.
  - Optionally, for medium security applications, the reader can also output a Hashed Message Authentication Code (HMAC) which is used to verify that the card has not been modified since cardholder enrollment into the PACS
  - Optionally, the reader can also output the card's expiration date

PACS Hosts (Servers): Overview

- The PACS host is the primary application for configuring, controlling, and disseminating information about the access infrastructure (particularly controlled doors) and the cardholders who have access privileges to those doors. The host has a configuration database, a cardholder database, administrative functions for configuring doors, readers, panels, clearances, schedules, cardholders, and other various features. All configuration activity is journaled for audit purposes.
- The host communicates to administrative clients, guard/monitoring station clients, and panels
- The host interfaces to the IDMS and other enrollment systems.

Smart Card Alliance

PACS Hosts: Cardholder Database

- Name
- Privileges
- Clearances
- Card number data
  - FASC-N data fields and/or GUID
  - HMAC for medium security
- Other user-defined fields
- Expiration date
- Picture (This does not have to be in the database, but can be the path of a picture file.)

Smart Card Alliance

PACS Hosts: Cardholder Enrollment

- Enrollment GUI in the admin client allows data to be entered manually.
- Methods to interface to other applications
  - IDMS used to issue the badge
  - Local enrollment application where cardholders present their badges the first time they access the facility. A reader would read the card and populate the cardholder database with the data encoded on the card.
  - A revocation list monitoring application can un-enroll a cardholder who appears on the revocation list.

Smart Card Alliance

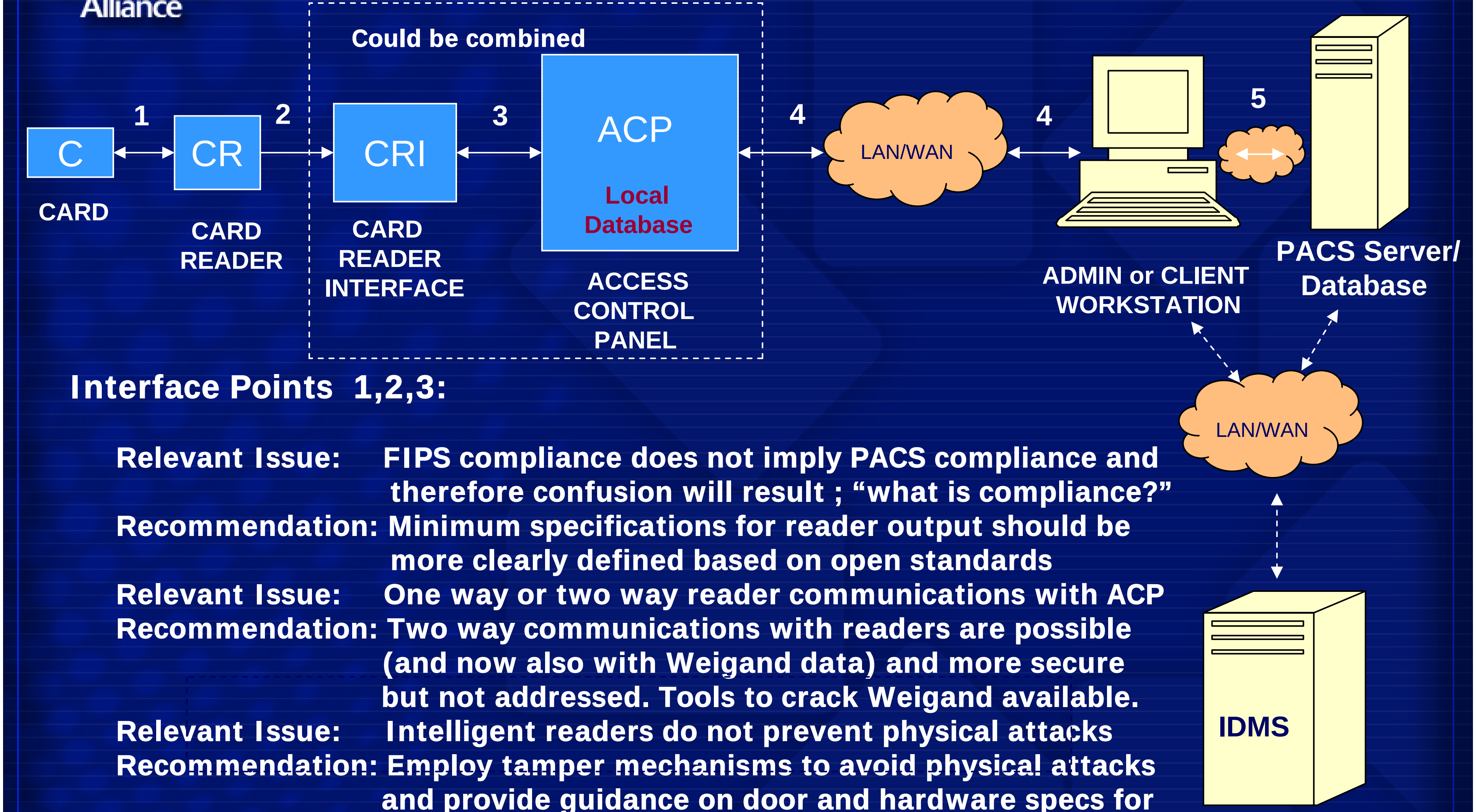
Physical Access Control Systems and FIPS 201: PACS Infrastructure (Cabling, Communications & Interfaces)

Physical Access Council

Smart Card Alliance

Smart Card Alliance

PACS Infrastructure: Issues / Recommendations



Interface Points 1,2,3:

Relevant Issue: FIPS compliance does not imply PACS compliance and therefore confusion will result ; "what is compliance?"

Recommendation: Minimum specifications for reader output should be more clearly defined based on open standards

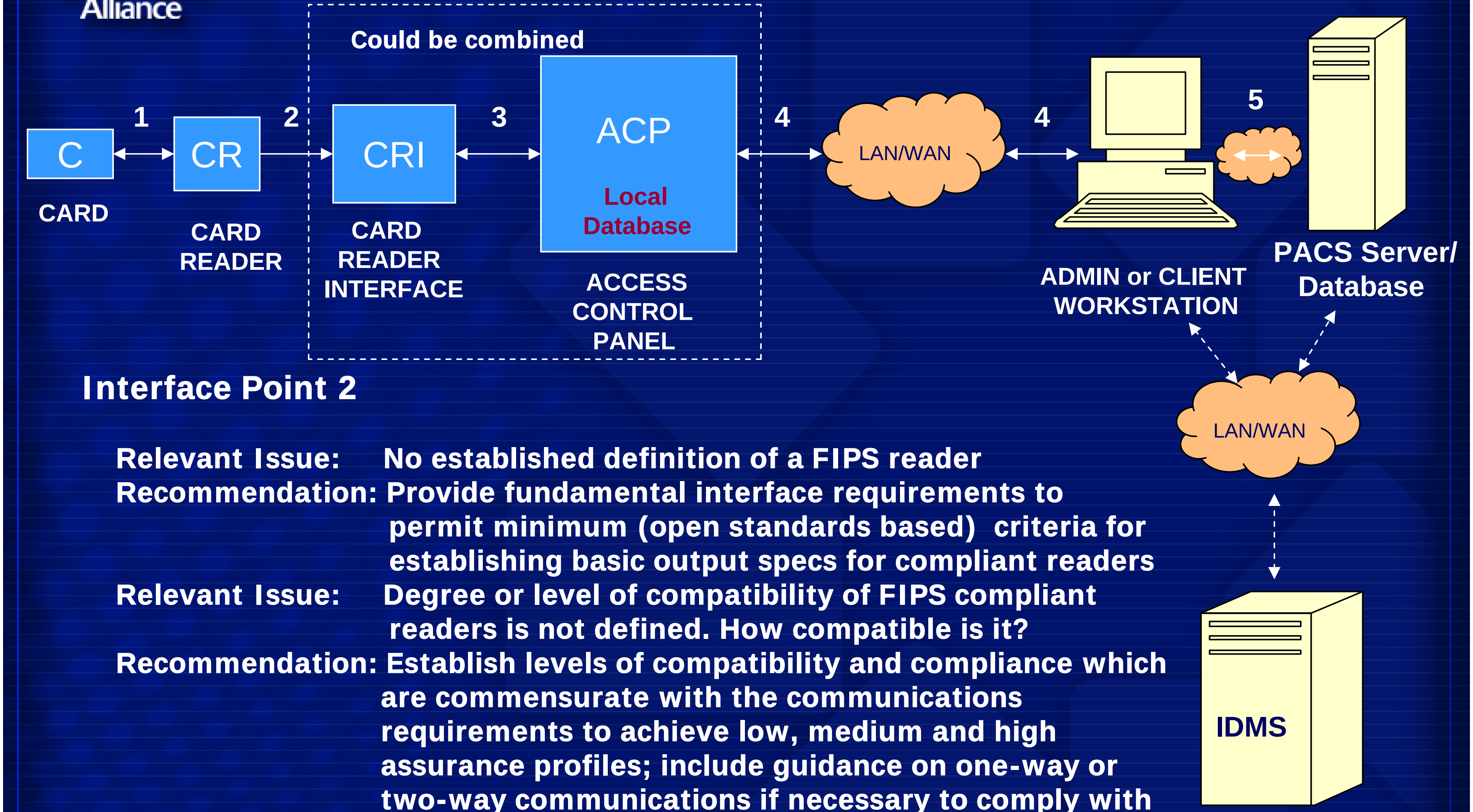
Relevant Issue: One way or two way reader communications with ACP

Recommendation: Two way communications with readers are possible (and now also with Weigand data) and more secure but not addressed. Tools to crack Weigand available.

Relevant Issue: Intelligent readers do not prevent physical attacks

Recommendation: Employ tamper mechanisms to avoid physical attacks and provide guidance on door and hardware specs for high assurance applications

PACS Infrastructure: Issues / Recommendations



Interface Point 2

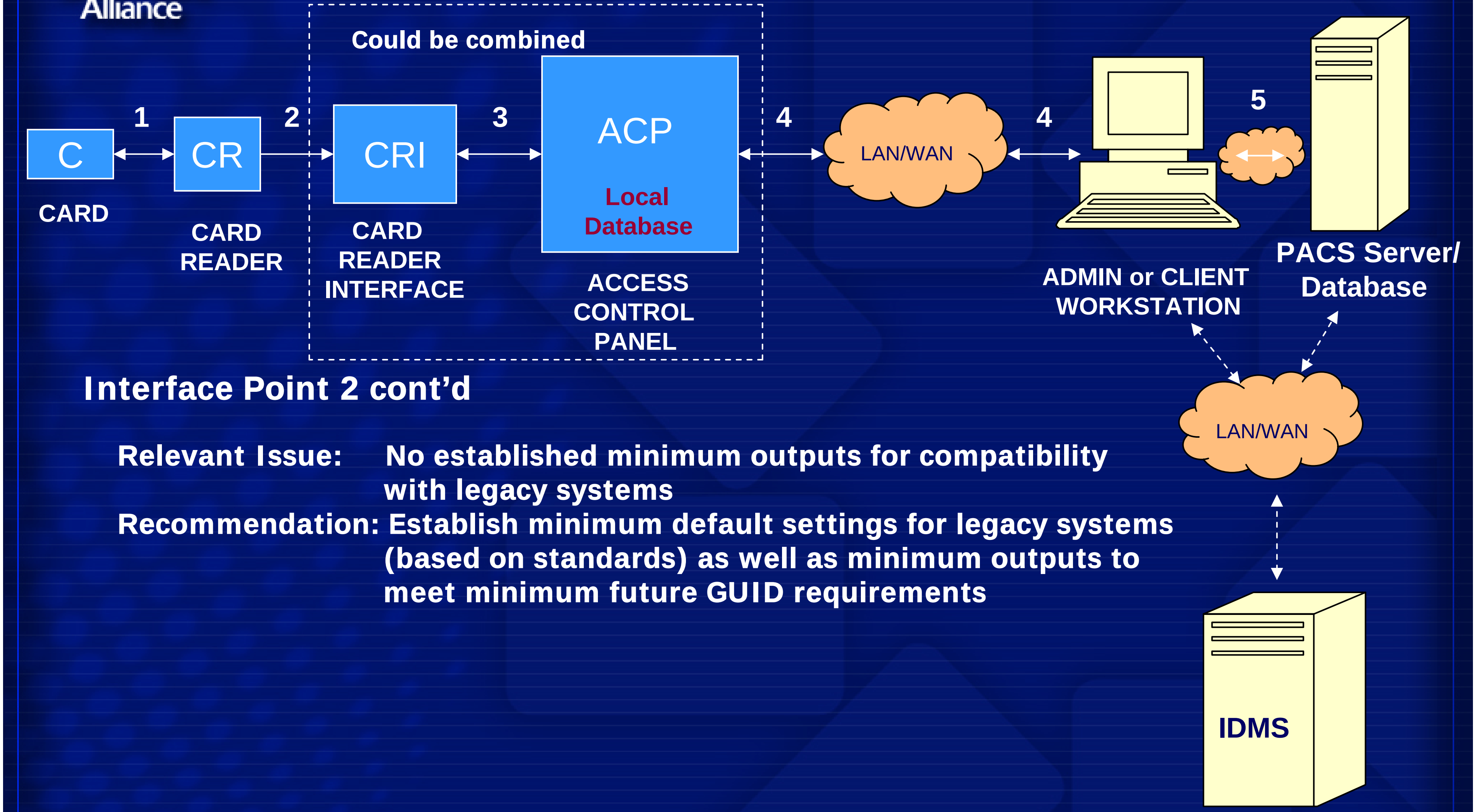
Relevant Issue: No established definition of a FIPS reader

Recommendation: Provide fundamental interface requirements to permit minimum (open standards based) criteria for establishing basic output specs for compliant readers

Relevant Issue: Degree or level of compatibility of FIPS compliant readers is not defined. How compatible is it?

Recommendation: Establish levels of compatibility and compliance which are commensurate with the communications requirements to achieve low, medium and high assurance profiles; include guidance on one-way or two-way communications if necessary to comply with high assurance and PKI applications

PACS Infrastructure: Issues / Recommendations

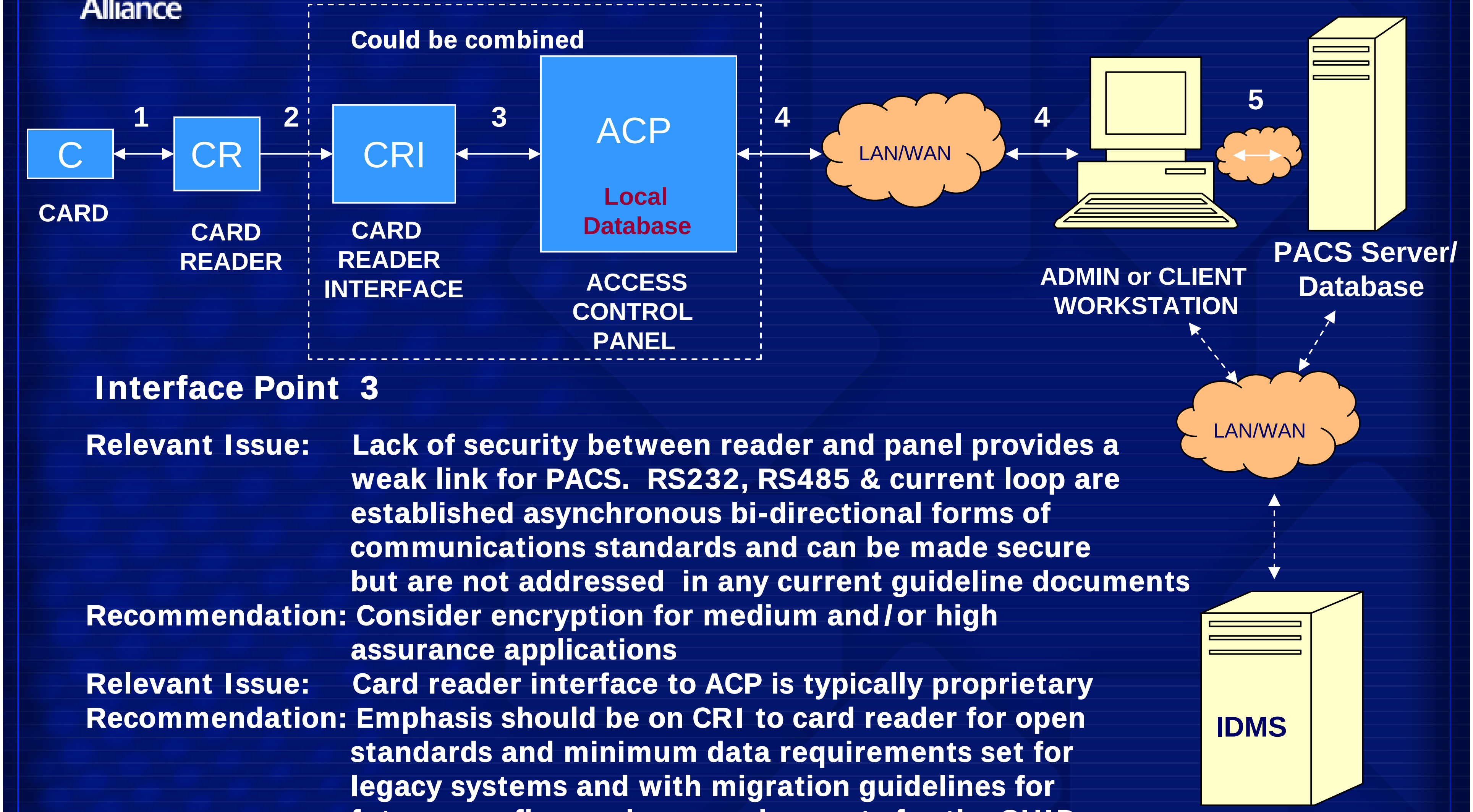


Interface Point 2 cont'd

Relevant Issue: No established minimum outputs for compatibility with legacy systems

Recommendation: Establish minimum default settings for legacy systems (based on standards) as well as minimum outputs to meet minimum future GUID requirements

PACS Infrastructure: Issues / Recommendations



Interface Point 3

Relevant Issue: Lack of security between reader and panel provides a weak link for PACS. RS232, RS485 & current loop are established asynchronous bi-directional forms of communications standards and can be made secure but are not addressed in any current guideline documents

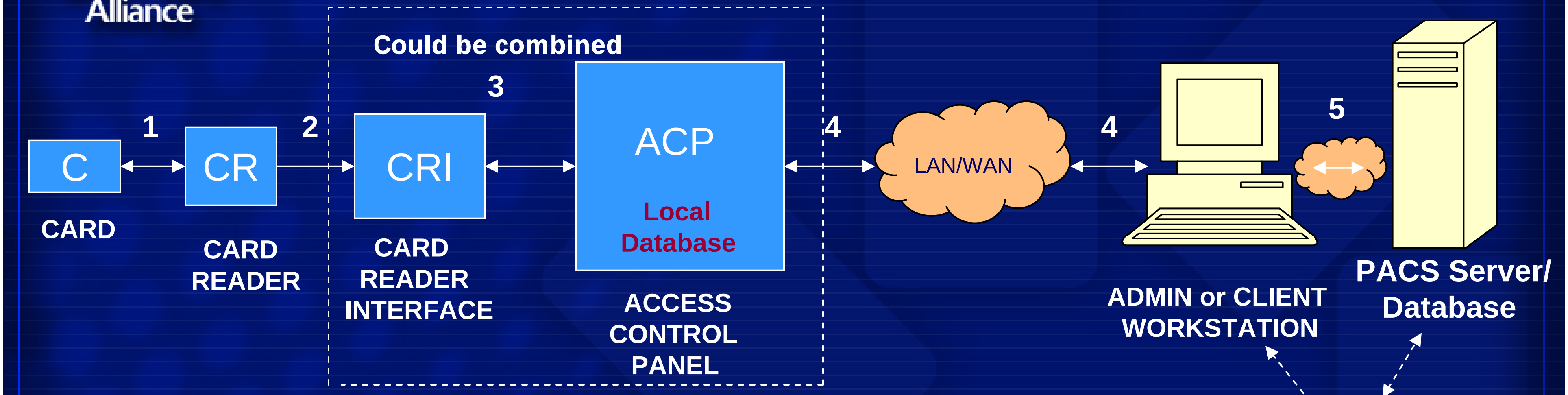
Recommendation: Consider encryption for medium and/or high assurance applications

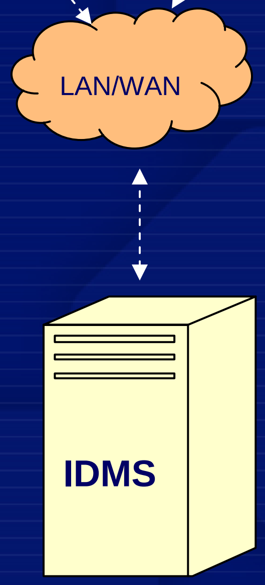
Relevant Issue: Card reader interface to ACP is typically proprietary

Recommendation: Emphasis should be on CRI to card reader for open standards and minimum data requirements set for legacy systems and with migration guidelines for future proofing such as requirements for the GUID

Smart Card Alliance

PACS Infrastructure: Issues / Recommendations





Interface Point 4 / 5

Relevant Issue: Data fields within the schema of the PACS database server are not identified and may not correlate to those in the CHUID fields for easy migration to the host from the IDMS. Every system will therefore have to be customized at a cost

Recommendation: Establish a minimum set of data to be imported and the method of transfer for standardization (for example, XML). All systems would have same set

Relevant Issue: There is much confusion on what is open and what is proprietary when PACS systems are evaluated and purchases are made on beliefs and assumptions

Recommendation: Clearly define what portions of the PACS are to be based on open standards and what does not have to be

Physical Access Control Systems and FIPS 201: Biometrics

Smart Card Alliance
Physical Access Council

Smart Card Alliance

Biometrics

- ❖ An access control reader with biometric capability is required for assurance levels of high confidence or very high confidence
- ❖ NIST Special Publication 800-76 provides interoperable biometric data specification for storage on the PIV card
  - ❖ Requires storage of minutiae templates from two index fingerprints
    - Templates must comply with ANSI-INCITS 378 standard
    - Alternative fingers are allowed if index fingers cannot be imaged
  - ❖ SP 800-76 is in draft mode and is still subject to change

Smart Card Alliance

Biometrics: Issues/Recommendations

- **Use of contact readers and PIN entry for release of the mandatory fingerprint templates may not be appropriate for PACS due to throughput performance requirements or environmental requirements**
- **Use of alternative biometric paradigms for contactless operation is not precluded in FIPS 201**
  - However, such implementations may not be interoperable with other agencies
- **Examples of alternative biometric paradigms include:**
  - Different modalities (e.g., fingerprint, iris, face, hand geometry, etc.)
  - Store on card – match on reader (agency specific PIV container)
  - Store on server – match on server (CHUID acts as pointer to biometric record in external database)
  - Store on card – match on card (PIN replacement option)

Biometrics: Issues/Recommendations

- If fingerprint templates are used for alternative authentication paradigms, they should comply with the INCITS 378 standard (as defined in SP 800-76) to allow interoperability with various manufacturer's hardware sensors and algorithms that may be used within an agency
- If biometric templates are stored off the PIV card, consider the requirement for an external communications link from PACS reader
- PIN entry or contact reader is not required if an alternative biometric paradigm is chosen

Smart Card Alliance

Physical Access Control Systems and FIPS 201: Privilege Granting and Revocation

Physical Access Council

Smart Card Alliance

Privilege Granting and Revocation

- PACS privileges (authorizations) for PIV cardholders are granted and revoked based on local security policies.
  - The biggest issue related to granting privileges is trust in the PIV cardholder’s identity.
  - This trust can be established at varying levels of assurance through the FIPS 201 PIV authentication mechanisms.
  - Asymmetric key related authentication mechanisms require network connectivity to CRLs and/or OCSP responders.
  - Continued trust in the PIV card requires that the issuing agency support the card’s validity by distributing or providing access to pertinent status change information.

Privilege Granting and Revocation

- PACS revocation pertains to the revocation of privileges and not the revocation of a PIV card.
  - PACS privileges can be revoked even though the PIV card has not been revoked, but PACS privileges should be revoked if the PIV card (PIV authentication certificate) is revoked.
  - Automated PACS privilege revocation for revoked PIV cards is not mandatory, but is recommended.
  - Automated PACS privilege revocation based on a revoked PIV authentication certificate requires network connectivity to the PKI infrastructure (e.g., CRLs and/or OCSP responders).
  - There is no requirement that each access point triggers a credential status request, as long as the PACS is updated according to agency-specific FIPS 201-compliant procedures.

Smart Card Alliance

Privilege Granting and Revocation

- System processes that update and synchronize PIV card status in affected PACS databases are essential.
  - In addition to CRLs and OCSP responses, a PIV card hotlist could be maintained on some or all revoked or terminated PIV cards. This hotlist could be made accessible online or could be distributed on a scheduled basis (e.g., hourly, daily).
  - For added security, the hotlist could be digitally signed by its issuer/maintainer.
  - FIPS 201 mandates a maximum 18 hour update of CRLs, which should be the maximum update time for the hotlist.
  - In cases where 18 hours is an unacceptable delay, alternate procedures must be implemented to disseminate this information within a shorter and acceptable timeframe.

Smart Card Alliance

Physical Access Control Systems and FIPS 201: Certification & Accreditation

Physical Access Council

Smart Card Alliance

PACS Products Issues

- **GSA has not published a methodology for PACS equipment to be on its approved product list.**
  - It is recommended that GSA only certify the PACS readers.
  - The PACS system vendors need GSA-approved transitional and end-state smart card samples encoded with the finalized data model to do system development and testing.
  - Contactless reader approval process need to conform to the current ISO/IEC 14443 standard.
- **Industry (e.g., SIA, NFPA, UL) needs to define interoperability standards to support FIPS 201 and other functionality**
  - Communications security: reader-panel, panel-panel, panel-host, host-host
  - Interoperability: Host-host communication, ODBC, XML, common database format (issuer authentication, camera call up, visitor management systems)

Facility Security Guidance

- **There is no defined guidance to inform agencies about what level of equipment should be purchased**
  - Equipment selection criteria needs to be based on the accreditation level that the facility needs.
  - The PACS needs to be configured to support the accreditation level.
  - Throughput - transactions per second (card reads, alarm events, panel down/up loads) - needs to be part of the design criteria.
- **Legacy PACS and interoperability**
  - Majority of legacy PACS can support a single agency PIV2 credential using the FASC-N by upgrading the PACS readers and host software.
  - At this time, support for end state cards with IPv6 addresses used as global unique IDs has not been developed by the majority of PACS vendors.

Certifying PACS

- The Authority Having Jurisdiction (AHJ) will have a number of overlapping regulations that the PACS will need to be certified to meet:
  - Physical security
  - IT security
  - Life safety
  - PIV processes
- The AHJ will have to develop a program to maintain the certification & accreditation
- Facilities would receive certification & accreditation
  - Low: self-certify
  - Medium, High: third-party certify

Smart Card Alliance

Physical Access Control Systems and FIPS 201: Conclusions

Physical Access Council

Smart Card Alliance

Conclusions

- FIPS 201 and associated NIST special publications and guidance from the OMB, GSA and IAB PAIIWG provide an excellent framework for deploying an interoperable secure ID credential, addressing many of the issues about FIPS 201 and PIV card implementation
- Key open areas needing guidance
  - Usage requirements for PIV card data elements (FASC-N, GUID, CHUID expiration date, asymmetric signature, card authentication key) CHUID test data model set
  - Conformance testing or specification for access control readers
  - Specifications and standards for PACS interface points to reflect FIPS interoperability and security requirements
  - Biometrics: use of biometrics over contactless interface
  - Enrollment and revocation: Methods for synchronizing PIV card status and PACS databases
  - Methodology for adding PACS products to GSA approved products list
  - Guidance for agencies on level of equipment needed to support facility accreditation level
  - Certification and accreditation of PACS

Conclusion

- **The Smart Card Alliance Physical Access Council is focused on helping agencies understand how to implement PIV cards and deploy FIPS 201 compliant PACS**
- **Follow-on Smart Card Alliance efforts include:**
  - Working with NIST, OMB, GSA, IAB, PAIIWG, SIA and IBIA on updates to specifications and guidance going forward
  - Providing educational workshops on HSPD 12 and FIPS 201 implementation

Smart Card Alliance

Physical Access Council

- **Mission: Accelerating the widespread acceptance, usage, and application of smart card technology for physical access control**
- **Participation from 48 Smart Card Alliance member organizations**
- **Other resources**
  - "FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems" white paper, published Sept. 2005
  - FIPS 201 resources web page

Physical Access Council

❖ Participants in FIPS 201 and PACS issues project

Tim Baldridge, NASA
Simon Barnes, Indala
Calai Bhoopathi, SCM Microsystems
Tom Casey, DHS
Sal D'Agostino, CoreStreet
Tony Damalas, Actcom
Mike Davis, HID Corp.
Dave Engberg, CoreStreet
Paul Evans, Booz Allen Hamilton
Robert Fee, LEGIC Identsystems
Bob Gilson, DoD
Walter Hamilton, SafLink/IBIA
Steve Hopper, Infogard
Steve Howard, IDTP
Eric Joseph, Lenel
Won Jun, G&D
Mike Kelley, BearingPoint
Russ Kent, EDS
Lolie Kull, DHS
Irene Lam, Tyco Software House
Erik Larsen, Lenel
Philip Lee, Identity Alliance
Stafford Mahfouz, ADT
Cathy Medich, Smart Card Alliance
Bob Merkert, SCM Microsystems

Mike Miley, SAIC
Ram Mohan, Northrop Grumman
Cathy Mrosko, SIA
LJ Neve, Maximus
Dwayne Pfeiffer, Northrop Grumman
JC Raynon, SCM Microsystems
Mike Regalski, Lenel
Patrick Rodwell, Lenel
Roger Roehr, BearingPoint
Steve Rogers, Integrated Engineering
Adam Shane, AMAG Technology
Jim St. Pierre, MDI
Jeffrey Stephens, EDS
Dario Stipisic, DoD
Chris Stotts, Cubic
Michael Sulak, US Dept. of State
Lars Suneborn, HIRSCH Electronics
Rod Taylor, US Dept. of Justice
Radu Tenenbaum, Tyco Software House
Beth Thomas, Honeywell
Steve Treado, NIST
Mark Visbal, SIA
Steve Weyman, Infogard
Eric Widlitz, HID Corp.
Rob Zivney, HIRSCH Electronics

Smart Card Alliance

For More Information

- **Physical Access Council**
  - Bob Merkert, SCM Microsystems, Council Chair - rmerkert@scmmicro.com
  - Dwayne Pfeiffer, Northrop Grumman, Council Vice Chair - dwayne.pfeiffer@ngc.com
  - Steve Rogers, Integrated Engineering, Council Secretary - steve@smart-id.com
- **Smart Card Alliance**
  - Randy Vanderhoof, rvanderhoof@smartcardalliance.org
  - Cathy Medich, cmedich@smartcardalliance.org