Physical Access Control System (PACS) in a Federal Identity, Credentialing and Access Management (FICAM) Framework

PACS Best Practices using PKI-Authentication

A SIA White Paper

Security Industry Association
Silver Spring, Maryland
siaonline.org/standards

Acknowledgements

This paper was developed through the joint efforts of two Security Industry Association communities of interest. The SIA Standards Access Control & Identity Working Group and the SIA Personal Identity Verification Working Group. SIA gratefully acknowledges the efforts of the many volunteers listed below from the security industry that helped produce the paper.

Contributors:

AMAG, Adam Shane

Apiary, Avigdor Dagan

Brivo, Jim Sheahan

Codebench, Bob Fontana

Gallagher, Steve Bell

Identitification Technology Partners, Rob Zivney (**Project Lead**)

IDmachines, Sal D'Agostino

Intellisoft, Steve Rogers

Oberthur, Lars Suneborn

XTec, David Helbock

Participants:

AT&T, Jimmy Salinas

Brivo, Steve Van Till

Deister, Bill Nuffer

HID, Kathleen Carrol

HID, Nathan Cummings

Identive Group, Pat Finnegan

Mercury Security, Frank Gasztonyi

Quantum Secure, Mark Steffler

Roehr Consulting, Roger Roehr

Siemens, Perry Levine

Smithee, Spelvin, Agnew and Plinge, Inc., Rodney Thayer

Transtech Systems, Jim Gingo

Tyco Integrated Security, Donald Woody

XTec, John Schiefer

Executive Summary

Physical Access Control Systems (PACS) are constantly evolving. As networked information technology systems, PACS take advantage of Moore's Law and the continuously improving price/performance of computer systems. PACS are constantly incorporating improvements in communications and security technologies. PACS and physical security systems use wide area, local, fixed and wireless networks at a range of frequencies across a wide range of devices from mobile phones to millimeter wave radars. In the 1990s, Internet protocol (IP) technologies were incorporated in servers, controllers and network devices. More recently, cloud and smart phone and tablet technologies have been driving industry to incorporate new technologies and solutions. During this period, SIA has established a longstanding record of leveraging standards to promote safety, security and interoperability.

Since 2005, Personal Identity Verification (PIV) credentials have provided a high level of identity assurance. These high-assurance credentials have been incorporated in a variety of ways into PACS. SIA has issued guidance1 on cryptography and its use in security systems, and there are now more than 5 million government users who should be strongly authenticating for access every day.

HSPD-12 and FIPS 201 involve a two-step process. In creating and binding PIV cards to more than 5 million people, the government and NIST have accomplished much. These Level 42 high-assurance credentials meet the highest practical national and global standards. It is understandably a requirement to have systems authenticate users in a way that leverages a high-assurance identity credential.

Current PACS controllers and other edge devices implement PIV, PIV Interoperability (PIV-I) and other forms of strong authentication. This is not at issue. What is at issue is that the APL to date enables manufacturers to gain listing without meeting the requirement to do the high-assurance authentication that was the point of making the PIV investment. In addition, agencies have acquired APL-listed PACS that don't perform high-assurance authentication.

Manufacturers have taken a variety of approaches, from minimum compliance to significant investment in solutions that meet the goals and requirements for the use of PIV credentials and a wide range of smart card technologies for federal and other high-security PACS deployments. Going forward, industry and end-users will pursue solutions that provide the best value for the lowest total installed cost, lowest lifecycle cost and high availability, reliability, security, usability, flexibility and scalability.

There is no single architecture or topology offered by manufacturers to meet the value propositions. Current solutions cover a wide range of processors, operating systems and components. Given the breadth of technology, rate of innovation and commercial-off-the-shelf-options, there is no specific approach, and prescribing one would stifle innovation. PACS need to adapt to new technology and incorporate upgrades over their lifecycle, be it as a traditional five-plus-year capital expenditure or a more modern three-year IT lifecycle.

[1] http://www.siaonline.org/WorkArea/showcontent.aspx?id=11356

[2] http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf NIST SP 800-63-1, Electronic Authentication Guidelines, December 2011

Accordingly, test and conformance standards cannot dictate a single approach. Rather, they must establish functional requirements and perform tests to ensure that these are met. This typically cannot be achieved in a lab by examining individual components[3] configured in a specific or limited manner. The real world does not break down into a limited number of configurations, even within a given federal enterprise. Further, any federal PACS deployment will require compliance with the Federal Information Security Management Act where system testing will take place. In order to leverage functional testing of PIV authentication capabilities, the user, integrator and solution provider need to make sure the PACS is configured correctly in the context of an installed and operating system. Functional and system testing need to complement each other.

There are many existing testing and conformance processes in place in industry and in government. Redundant tests, particularly those referred to as PACS tests, which are overly focused on authentication and PKI are counterproductive. That is not to say that functional PIV authentication testing does not need to take place but it should be recognized and organized as such, and in fact, this already exists in the APL authentication categories. This is a completely separate issue from the need for agencies to understand their requirements, be able to procure systems that meet the requirements and have an ability to test systems to make sure they are configured and operated and maintained to do so.

Regardless of whether it is functional testing or system certification, any testing program must have as a counterpart the enforcement of requirements, not simply memoranda that refer to, but do not implement, enforcement. This white paper examines testing with a focus on the functional requirements, inclusive of those required to support PIV and, generally, standards-based strong authentication. It examines the current APL and other requirements and also the goal of interoperability while looking to continue to include industry best practices for PACS in an evolving world.

[3] The issue is related to the level at which functional tests are performed. Functional tests for PIV authentication require credential and infrastructure for testing. The exception would be an "all-in-one" component (authentication system) capable of meeting the functional requirements. SIA believes these functional requirements already exist in the authentication categories on the APL.

Foreword

Following a March 1, 2013, submission of comments from industry to the GSA's EPTWG on the first nine draft documents of the APL 2.0 test and approval procedures and a presentation at the Interagency Advisory Board (IAB) on the Open Supervised Device Protocol (OSDP), a SIA specification for reader-to-controller communications, GSA requested a meeting with a small group of SIA representatives. The purpose was to promote understanding of each other's position and intent regarding PIV authentication and PACS industry development and, it was hoped, find common ground. One of the outputs of this meeting, which was held at GSA offices on March 26, was a GSA request for and SIA to produce a white paper that would provide industry guidance on how "best" to ensure that PACS can be provisioned to use PIV credentials and the associated cryptographic and public key infrastructure operations for authentication of federal employees and contractors in a way that meets the interoperability and security goals of HSPD-12 and FICAM.

Topologies and Why They Don't Matter

The GSA Evaluation Program (EP) has chosen to identify one particular PACS configuration (Figure 1: "Representative Architecture for a Validation System" on line 70 of the Validation Approval Procedure), which it now refers to as a topology to meet the requirements of FIPS 201.

Industry responded that the initial "representative validation system architecture" was unhelpful in that it called out a *specific approach* that involved adding an additional or parallel subsystem to the PACS specifically to address the requirements of FIPS 201. This early "proof of concept" is one way in which industry addressed requirements. But industry moved on quite some time ago from this single approach.[4]

Subsequent to the aforementioned meetings with SIA representatives, the EP issued the "Draft: Topology Adoption Process," dated March 28, 2013, which offered a process for suggestions of alternatives. This document asked for further topology definition.

Neither the topology nor the way validation is done should matter. It also becomes obvious that the existing example should be removed and the manner of functional and system testing be revisited. One example becomes a rule without additional examples to clarify that other approaches are acceptable (and, in this case, preferable to the example) to achieve functional objectives. Further, the approach will be very dependent on the existing PKI at the enterprise or locations being secured.

Authentication testing is already part of the existing APL. As for validation, these components are also part of the existing APL. PACS need to leverage – not duplicate – these components as part of the enterprise authentication services. Validation done properly should be part of the enterprise authentication dial-tone that PACS leverage.

A PACS does need to demonstrate that it can properly handle any of the PIV authentication modes that a manufacturer claims to support. How the PACS components are configured (what topology) is partly the result of how a PACS manufacturer designs the system and partly how an installer configures the system to fit the unique requirements in the field.

There is a big jump from testing PIV authentication modes to testing PACS or access control systems, in general. There are a number of functions that PACS (and access control systems) must support in addition to authentication. From a high-level, PACS functionality consists of the "four A's": Authentication, Authorization, Administration and Audit. (Some might add a fifth: Analytics.) The four A's of functionality must be present in an access control system for it to meet the goals of HSPD-12 in addition to the particular keys and objects in PIV cards and infrastructure. The EP needs to maintain and complete its mission on FIPS 201 authentication before it moves on to other FICAM functionality. FIPS 201 is about identity, credentialing and authentication in accordance with a specific credential functionality supported in different ways by some current PACS. FIPS 201 is

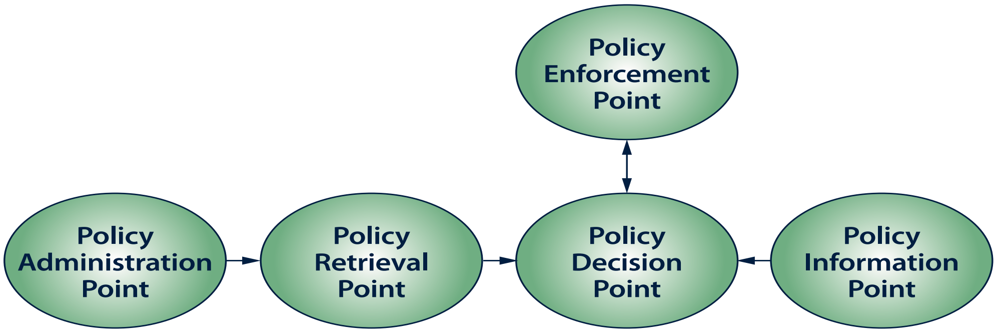
[4] These add-on solutions also map to a specific product that an EP subcontractor has used for its own proprietary "certified product list" and as a configuration for integrator training. So there are issues of poor representative choice as well as potential conflict of interest with the goals of the EP and GSA.

also built on standards-based cryptography, and its inherent interoperability requirements were new for many PACS. Industry has moved well past that and participates in tests for this functionality, including the existing APL categories.

The more recent effort by the EP to begin to test authorization and other functions seems inconsistent with the charter of HSPD-12 and out of sync with FICAM goals. Given the need to do authentication testing, and given that PACS are unique to their particular agency or facility context, it seems the EP's insistence on pursuing testing beyond the existing authentication categories is inappropriate at this time.

More to the point on topologies, PACS are a particular type of access control system used as an electronic security countermeasure. They are access control systems, just like logical and network access control systems, and are specific to their context. The granularity and ability to enforce policy across access control systems continues to evolve. From access control lists (ACLs) to role-based access control (RBAC) to attribute-based access control (ABAC)[5] and policy-based access control, the components of authorization continue to combine in multiple ways and, thus, need to be topology-agnostic.

Looking at authorization in the abstract can be more helpful to PACS vendors than prescribing topologies. As an example, XACML[6] looks at access control in the following manner.



XACML does not prescribe a topology to do this. Using this way of looking at access control, one can see that each of the PACS components *could* be put into a specific category. However, many alternatives exist, as sometimes a PACS will physically relocate where these processes occur or combine them into common physical components to meet the changing needs of the market or a site's risk management objectives. These decisions should be left up to the system designer, manufacturer and installer, who can take into account the requirements and risks in context.

[5] Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft) http://csrc.nist.gov/publications/drafts/800-162/sp800_162_draft.pdf

[6] eXtensible Access Control Markup Language (XACML) https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

	Policy Administration Point	Policy Retrieval Point	Policy Decision Point	Policy Information Point	Policy
Reader	x	x	x	x	Primary
Controller	x	x	Primary	x	x
Head-End	Primary	Primary	x	Primary	x

For these and other reasons, we believe that the EP needs to leverage existing categories in a functional testing approach.

Comparison and Discussion of Architectures and Topologies

While topologies don't matter, it is useful to show that alternatives exist. The topologies shown below are *not* recommendations for testing or deployment. Rather, they are presented to show that the EP's objectives and resulting test procedures need to be adaptable to multiple solutions and that there are more informative representations.

PACS infrastructures up till now have typically handled the identity, authentication and authorization components of physical access control. HSPD-12 and the associated FIPS 201 PIV standards have effectively separated the identity component and FICAM required PACS to leverage identity and authentication as enterprise services. PACS must leverage the FIPS 201 identity and public key infrastructure in making authorization decisions. In this sense, the PACS is no longer the authoritative source for identity.

The FICAM functional workflow of identity verification with an agency PACS is illustrated in Figure 3-5, "General FPACS Functions," in the publication *PIV for E-PACS 2.0.2*. Extracted as Figure 1 below, it depicts a functional topology that may not necessarily match the PACS topology of any particular manufacturer. The drawing is problematic in that it calls out a box as the agency PACS and limits its capabilities to only access control rules, when, in fact, everything in the drawing except the certificate authority is the agency PACS. Further, most access control decisions are actually made by the logic in distributed controllers. The only hint of a controller is the mention of a "door panel with reader." Perhaps the most critical component of a PACS – the controller – is not represented anywhere in the drawing. The figure also states that, "Authentication mechanisms are based on assurance levels." Yet, SP 800-116 points out "there is not a simple one-to-one mapping between FSLs and PACS Identity Authentication Assurance Levels at access control points; generally, higher-risk areas will need stronger identity assurance."

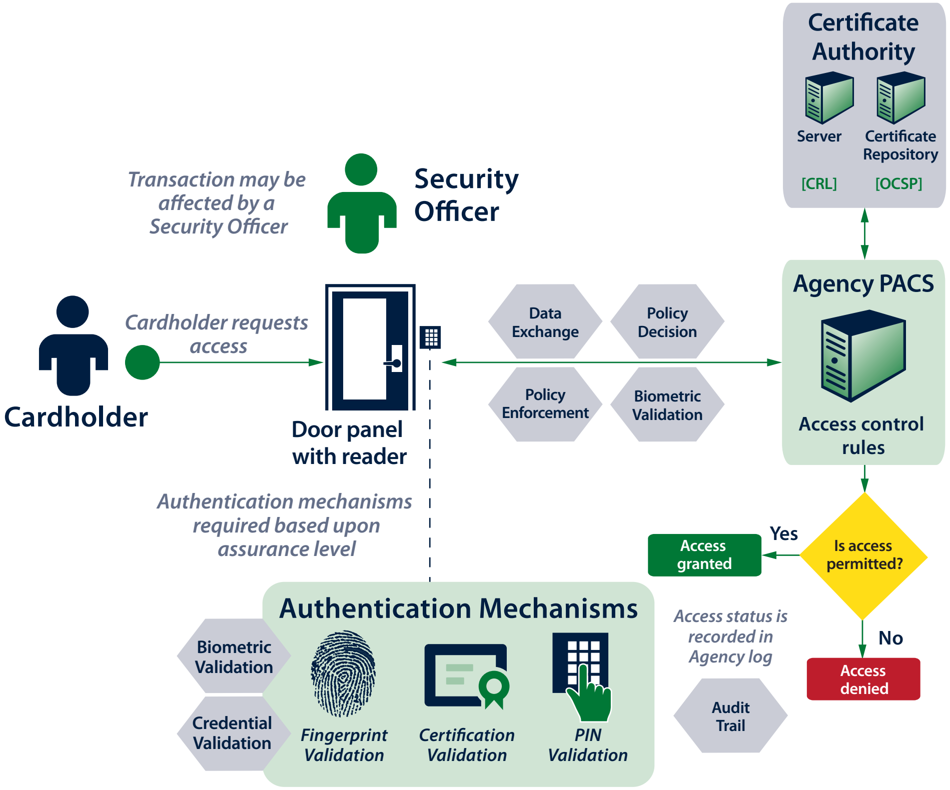


Figure 1 - Generic FPACS Functions

As an alternative to this approach, Figure 2 below separates the functionality of the "agency PACS" into a distributed architecture. This drawing, like a contemporary PACS, uses robust, self-sufficient, embedded devices in the field, which enforce the necessary policies and implement the specific level of authentication required for the security area being accessed.

Authentication mechanisms can take place at various locations in the architecture including at the reader, at the controller, or at the head-end.

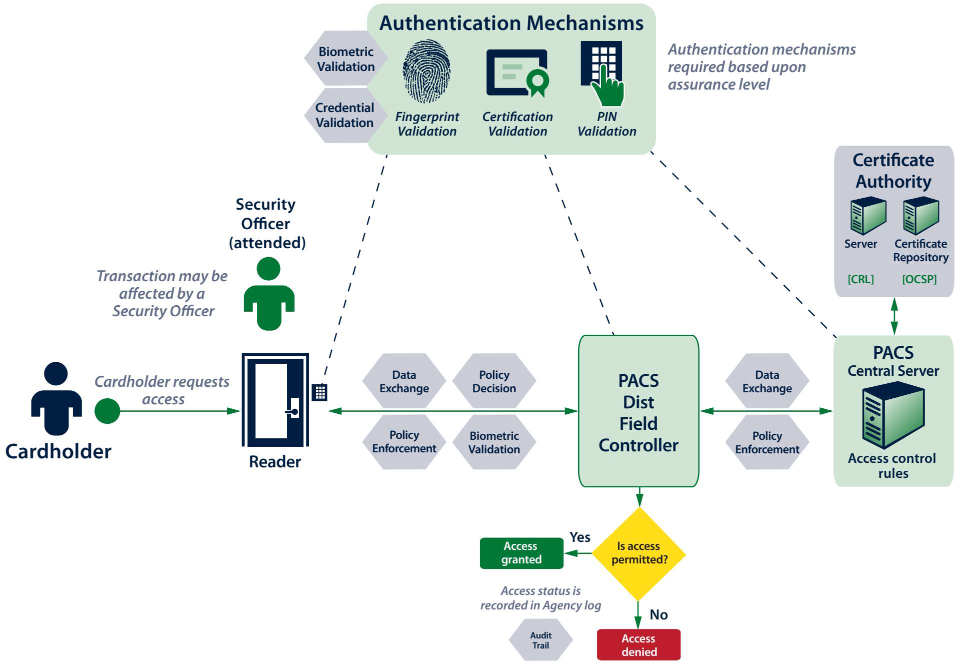


Figure 2 - Generic FPACS Functions based on Existing PACS Architectures

Recognizing the limitations on innovation that are imposed by illustrating specific product topologies, a more functional approach would better serve the interests of testing, compliance and creating a stable reference model. An identity, credential and access control abstract paradigm of adjacent functions with predefined input and output characteristics would be a better way to represent the functional requirements.

Functional Representations

This methodology uses an abstract association of functions in the identity, credential and access infrastructure. Functional certification can consist of systems combining one or more adjacent functional building blocks. Systems and components could be certified by combining one or more abstract functional modules.

The following diagram illustrates the practical procedures and information flow from credential through FICAM enterprise services and back. It works equally well in providing PACS identity registration, either manually by a human operator or automatically using a trusted identity source such an IDMS.

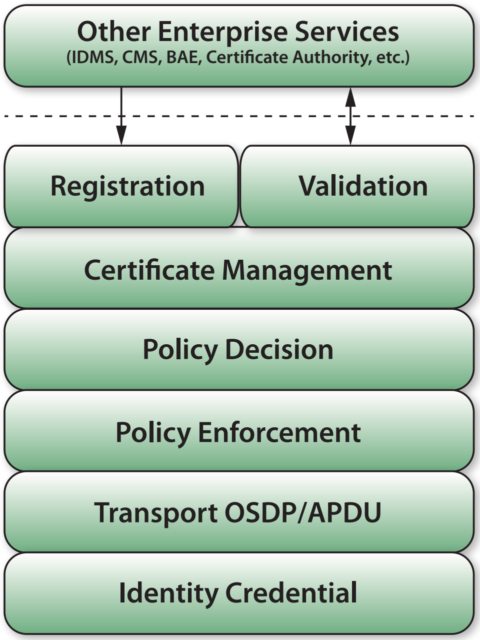


Figure 3 - Abstract Architecture

Building Blocks

Systems build functionality based on available building blocks and the particular problem they're trying to solve. In FICAM, Figure 106 acknowledges that there is no specific configuration for PACS infrastructure or components and it is topology-agnostic. The EPACS document and the draft FICAM test plans, however, take a different approach in specifying PACS configurations and topology. Again, we recommend a configuration-agnostic or topology-agnostic approach that is consistent with the FICAM Roadmap target state. For example, a PIV credential registration process must validate identity and other certificates at the time of registration and place the validated public key certificates and other pertinent information into a database for use by the relying system. In such a case, the functional building blocks consist of:

- Registration
- Certificate Management
- Validation

Each capability performs a specific function or series of functions. Using the registration station example above, the "Registration" function would be responsible for interfacing with the card and cardholder to collect the appropriate certificate information used by the "Certificate Management" and "Validation" function and storing valid public key certificates and personal information into the PACS database upon a positive identity verification result with appropriate care.

Registration/Provisioning

Registration and privilege provisioning captures credentials into the relying system. Registration/provisioning directly from an IDMS/CMS typically will not validate certificates at the time of provisioning (because these systems are considered to be trusted), whereas manual registration typically validates the credential's certificates before registration is complete.

Manual registration must validate identity certificates before placing the corresponding public certificate into the key store database and entering any credential identifier or personal information into the PACS database. Manual registration can utilize the capabilities of Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP) responder, or Server-based Certificate Validation Protocol (SCVP) server is performing path discovery and validation the "Validation" function block. Untrusted IDMS/CMS would be required to implement the "Validation" functional building block similar to the Manual Enrollment functional stack.

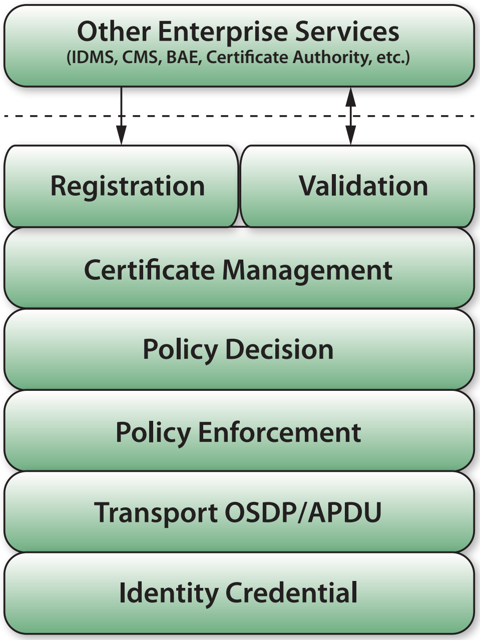


Figure 4 - Manual Registration

Provisioning identities from an IDMS may bypass the "Validation" functional block if there is a trusted relationship with the certificate authority. Registration of credential holder data into the "Certificate Management" key store and PACS database can occur directly from the trusted source.

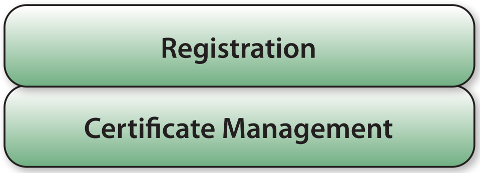


Figure 5 - IDMS Provisioning

Caching Status Proxy (CSP)

CSP capabilities are built from the "Credential Management" functional building block, in addition to the "Validation" building block. The "Validation" functional block would perform the appropriate functions for each certificate stored in the "Certificate Management" key store database. The results are returned to the "CM" database for use at a later time within the PACS infrastructure. This functionality exists in many modern server operating systems.

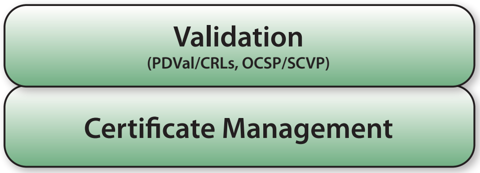


Figure 6 - Caching Status Proxy

PACS Central Server

The PACS central server in this scenario combines Registration, Caching Status Proxy and Policy Management capabilities into a single platform. The system accommodates manual and automatic registration with the option to utilize existing IDMS/CMS infrastructure, as recommended by FICAM requirements.

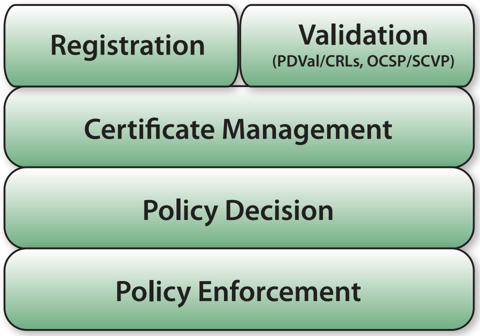


Figure 7 - PACS Central Server

PACS Distributed Intelligent Controller

The distributed processing capabilities of a PACS field controller leverages the PACS central server to manage the registered credentials. The PACS central server can distribute public key certificates and certificate statuses,, authorization logic and necessary attributes of a credential holder to each field controller, or it can reset the enable status based on information at the central server. In one example, policy decision and enforcement might be based on some external condition directly interfaced to the field control, resulting in a change to the multi-factor authentication.

A PACS distributed field controller might include functions similar to the following:

- Policy Decision
- Policy Enforcement
- OSDP/APDU

Distributed controllers in this example have the ability to challenge the identity credential using pass-through readers along with the OSDP protocol to pass APDU commands directly to the credential. Policy decision and enforcement could function in various ways, including enforcing authentication methods based on central server policy decisions or external factors connected to and monitored by the control panel.

The following functional building blocks enable the capabilities needed to perform as expected.

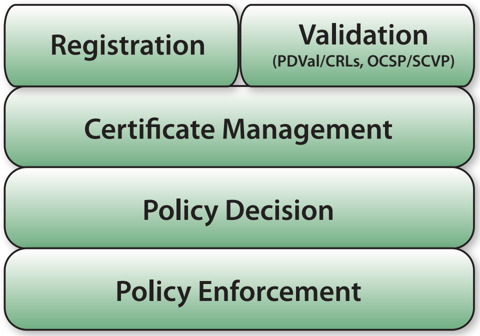


Figure 8 - PACS Field Controller

Reader

The term “reader” is a catchall for a variety of devices that can be used for credential authentication. The extent to which it performs the authentication function depends on the particular solution deployed. A reader used to interface with an identity credential may consist of the following functional building blocks:

- OSDP/APDU
- Identity Credential

The reader performs the appropriate authentication based on the device’s capability and the policy enforcement initiated by the relying system. OSDP can be used to provide a protocol to pass APDU commands from the relying system to the identity credential and back. The following functional building blocks would be used to implement the intended capability.

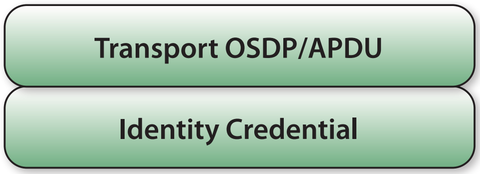


Figure 9 –Reader

Traditional PACS Architecture Supporting PKI

Products are now on the market that achieve FICAM goals in a traditional architecture and which can make selective Rip and Replace a cost-effective approach. Implementing PKI (whether for PKI-CAK, BIO signature checking or PKI-AUTH) will impact system design and functionality but may not affect the traditional architecture, though components might need to be upgraded or replaced. An example of a traditional architecture that accommodates PKI follows:

- Reader will typically be connected to control panel using bidirectional communications such as RS-485. Wiring considerations include the ability to use CAT-5 or CAT-6 for shorter distances (less than 350 feet) to allow flexibility for IP-based reader, PoE and RS-485.
- Reader-to-controller communications can be based on SIA specification OSDP 2.1.5 or later for commercial uses cases, as well as to support PIV.
- Communications between reader and controller (including any intermediate modules) should be encrypted (again, OSDP provides a specification for achieving this goal, and further guidance is expected in FIPS 201-2).
- FIPS 140-2 can be implemented in the reader, the controller, or both, per manufacturer design. If implemented in the controller, the reader can be truly "transparent," as with a LACS reader. Similarly, the reader and the authentication mechanisms can exist in one component and provide information to a controller for authorization.
- Controller will include a database for the unique identifiers of the credential, whether partial or full FASC-N, UUID, etc.
- The credential database in the controller will have an enable/disable field that is reset (downloaded) from the host based on a verity of parameters, including expiration dates, credential revocation status, local authorization policies, etc.
- Caching Status Proxy function, if integrated loosely or tightly with the PACS host, can be a source for the enable/disable status of the credential for near real-time operation at the edge.
- A traditional PACS architecture can support distributed processing, cloud implementations, survivability, and performance optimization as compared to architectures dependent on real-time communication to centralized components.

Transparent, CHUID and FICAM Readers and the Impact on PACS Applications

Transparent Readers

The term “transparent reader” is often misused and misunderstood, perhaps because of how it was applied to PACS applications in the original GSA APL. A truly transparent reader makes no interpretation of the commands being sent to the smart card, nor does it make any decision or take any action based on the content of the response from the card. A transparent reader is, in many ways, similar to a disk drive’s read/write head. It passes data between a control application and the media. In this case, the media is a smart card.

One example of a transparent reader is the LACS reader that can be found in many of today’s company laptops. Another transparent reader example is a USB reader that plugs into a computer. This is actually a LACS reader. Computers generally use PC/SC over USB to communicate with the smart card, though neither PC/SC nor USB define the transparent reader. The reader must simply serve as a conduit to enable an application to communicate with the smart card. It should do nothing more.

Perhaps the most important implementation for a transparent reader is as a door reader that only understands how to exchange smart card commands and responses with an application located in the secured space.

In 2006, the original APL included only one reader category we know as the CHUID Reader. Unfortunately, EP management determined that to qualify under the CHUID Reader category, a CHUID reader would have to include an onboard clock that could be synchronized. During implementation of the APL, EP management realized that there were few, if any, PACS readers (or LACS readers, for that matter) that met the CHUID Reader requirements, so EP management created a new reader category called the Transparent Reader that was totally inconsistent with the truly transparent aspects of a LACS reader. From that point on, all PACS readers that did not have an onboard clock were tested and included in the Transparent Reader category.

Because of the original misclassification of transparent readers for PACS in the GSA APL and a strategy to exclude PACS, itself. from the scope, the approval procedures for that category included a test for a GSA-conceived 75-bit output from a reader to be connected to a PACS: 48 bits were for the first three fields of the FASC-N, 25 bits were for the date, and the remaining two bits were for parity, which was commonly used with Wiegand pulse streams. The 75-bit format output implies that the reader makes security-related decisions and takes an action to output an identifier and expiration date to a PACS, which all PACS can utilize forever.

The GSA APL today contains more than 200 readers in the “Transparent Reader” category. It has become the low-cost catchall for any manufacturer to get its product on the APL to meet procurement requirements. A closer look reveals that more than half of the readers listed in that category are not behaving “transparently” at all.

The SIA specification, Open Supervised Device Protocol (OSDP) provides for truly transparent communication between the reader and the controller and is an appropriate alternative to the GSA 75-bit data format.

CHUID Readers

One would expect the CHUID Reader category to list readers that verify a CHUID signature and build a trusted path to the signer's root certificate before outputting 75 bits of identifier and expiration data. There is more trouble here, however. It does not appear that all 21 readers listed in this category are building paths to trusted root certificates. Few of these readers can, without help, perform all of the processing needed to correctly verify a CHUID signature, including building a trusted path back to a root certification authority. The logistics alone make it impractical and impossible.

Let us assume for a moment, though, that a reader verifies a CHUID signature and the signer's certificate can be validated back to a trusted root certificate. Does that prove that the credential is not a clone or a forgery? No, because the entire CHUID, signature and all, can be copied to another credential. Comparing a computed hash of the CHUID to the originally registered hash is not effective in detecting cloning, only tampering. This is why CHUID signature verification is not an authentication factor at all. It is also a strong rationale for deprecating the CHUID reader to "little or no assurance," as is expected in the forthcoming FIPS 201-2. The GSA APL should follow accordingly and discontinue this category without grandfathering listed readers.

Transitional Readers

There has been some discussion of creating a Transitional Reader category. If and when the combination of CHUID signature verification plus visual inspection as a single authentication factor is deprecated (and almost no readers are even doing what is required to be a true CHUID reader), then, for the reasons stated above, a category that actually does less to authenticate the credential and identify the user would simply add to the cost of the program and increase development costs for manufacturers. This category would serve no beneficial purpose.

Registration Readers

The registration process can be confirmed by establishing a Registration System category that includes the necessary components to authenticate the credential, including building a trusted path back to a root certificate for PIV Authentication, Card Authentication, and all content signer certificates. This category should not limit the technology of the reader used to verify the smart card. This means that registration can be performed using PCs with transparent LACS readers as well as other equipment (e.g., biometrics scanners and matchers). Biometric verification prior to registration can help to ensure that the biometrics will work properly if biometrics are implemented in a future phase of a security deployment. Again, note that the Registration System category should not limit the type of smart card reader used to verify the smart card and extract the data from it, as long as the reader is able to demonstrate interoperability and conformance to ISO 7816 standards.

The key element for registration is that the credential is authentic and valid and implements the FIPS 201 data model as specified in SP 800-73-x Part 1 at the time of registration. Ideally, the Registration System should implement the authentication mechanisms to the highest level used at any door in the PACS enterprise, with three-factor authentication being addressed (though FIPS 201-2 is silent on this configuration). A Registration System can optionally verify the identity of the cardholder using on- or off-card matching of a scanned sample with the card's reference biometric.

FICAM Readers

Since transparent readers for LACS, PACS and even PACS Registration (see below) might not be identical, and since the old transparent reader for PACS needs to be discontinued, the concept of the "faux" transparent reader for PACS is assimilated into the new FICAM reader.

From a reader perspective, the FICAM Reader System category should describe a reader that implements one or more authentication factors. Since all physical access control readers in the current Transparent Reader category will be recognized as "little or no assurance" (zero factor) readers by FIPS 201-2, they should eventually be replaced with readers that meet the requirements of a FICAM reader. They should initially be included in this category in order to differentiate them from LACS transparent readers.

The FICAM Reader System category should also include tests for interoperability at the ISO 7816 and 14443 layers, as well as levels of support for protocols T=0, T=1 and T=CL. The FICAM reader should be tested for protection of authenticators, FIPS 140-2 Level 2 (when applicable), and privacy for each authentication configuration. A FICAM reader could behave as a transparent reader. Accordingly, a FICAM Reader System category could add additional infrastructure that utilizes the reader.

Instead of specifying that a certain topology be followed, a FICAM Reader System category should describe the desired authentication functionality and the associated security objectives, such as the protection of authenticators, FIPS 140-2 Level 2 (when applicable), and privacy for each authentication mode. An instance of a FICAM Reader System might include a dual interface "transparent" reader that does PKI-AUTH or a reader that is capable of operating as one of the deprecated reader types until the end-user has the necessary funding and infrastructure to support one, two or three authentication factors. The same physical reader could provide one, two or three authentication factors depending on how the reader system is deployed and configured.

A FICAM Reader System implementation may work with legacy PACS or with future PACS. It is up to the vendor to decide whether they wish to offer one configuration or the other, or both, in accordance with their business objectives. It is up to the end-user to decide whether they wish to implement one configuration or the other, or both. The GSA EP test lab's goal should be to test and document functionality, security and interoperability in each authentication mode, end-to-end, and not to test for any particular intermediate configuration or topology. Leveraging and building upon industry standards such as OSDP can lower the overall costs for implementing and testing FICAM PACS solutions.

Bottom line: It is not about testing readers but rather about confirming that a reader system can perform PKI-CAK, BIO, PKI-AUTH, or combinations thereof.

Some readers (transparent) will rely on the PACS controller for these PIV authentication modes. Other readers (transparent) will rely on a separate component for PIV authentication mode and pass a Wiegand or other identifier to the PACS controller for authorization. Yet other readers will perform the PIV authentication modes integral to the reader and pass a Wiegand or other signal and identifier to the PACS controller for authorization. All are valid solutions to functionally achieve PKI-CAK, BIO, and/or PKI-AUTH.

So Just What Is a FICAM Reader Anyway?

During the March 26 meeting with GSA personnel, SIA representatives pointed out that PKI-CAK is critical to PACS but will not be usable until the CAK certificate is not only mandatory but also populated throughout the card population. GSA personnel responded, "Can't you just include a PIN pad and contact slot as a fallback and use PKI-AUTH as a fallback?"

Good question! This will also address broken antenna issues as well. And it raises some interesting new questions. First, how will a PACS controller know what authentication mechanisms are being used if the reader only passes along a resulting payload such as the UUID or FASC-N?

Ever since the introduction of multi-factor authentication, PACS have developed authorization algorithms to utilize the additional assurance available with the different factors. To be generic, let's say there is an information vector associated with each factor implemented and that vector might actually use a different unique identifier for each factory, though that is not done in PIV. This allows for card access during the day and card-plus-PIN access after hours, or single-factor assurance at lower threat levels and three-factor assurance (card, PIN and BIO) at high threat levels. If the necessary parameters are not established in the card and available to the reader, and the reader cannot send authentication factor vectors to the controller, many important and expected authorization mechanisms will be lost.

A PKI-CAK reader and a PKI-AUTH reader (or reader system) will perform all the same challenge/response, certificate checking, and path validation checks, and will produce the very same output for the same card (if the CAK is populated). There is currently no specification for how to communicate to the authorization process that the PIN was presented. Similarly, CAK-plus-BIO (three-factor) does not know any more than the UUID or FASC-N payload it receives.

In addition to authentication factors, should information be sent to the PACS controller regarding whether the card is a PIV-PIV-I, CIV, FRAC, TWIC, CAC or other credential? Conventional PACS have the ability to implement sophisticated authorization algorithms based on content and the formatting of the content in the card, but PIV does not. At present, there is not even a required discovery mechanism available in the card to determine which version of PIV the card is, or whether it is PIV-I, in order to execute expected authorization algorithms.

So a FICAM reader must be able to provide not only an authentication process, but also provide information necessary for the PACS to determine what authentication mechanisms were used and what type of credential was presented.

Contactless Card to Reader Operation at Distance

Effective interaction between a card and a reader is a function of both components. In fact, there may not be sufficient specifications in place today for the card. There should be a requirement to test the card for proper operation with a reader. This cannot be offset with more stringent testing of the reader or by putting additional constraints on the reader.

Where there is a need for a suite of test cards to test a reader for its ability to operate on the cards data model, there may well need to be a suite of readers to test cards for their ability to perform effective radio frequency (RF) communications, especially as related to distance, metallic environment and operating frequency of the card. The EP establishes minimum and maximum operating distances that dictate the need for additional testing for the cards prior to finalizing test procedures for the readers. Of particular concern is the unreasonable and conflicting requirement for operation at 7 cm and non-operation at 10 cm.

It is typical for an ISO 14443-4 card and reader interaction to work in the 1-inch (2-3 cm) range. 125 kHz proximity cards and readers, which were used by government prior to PIV, set an expectation for longer read ranges (sometimes up to 6 inches away) and instant results, but they did not have crypto operations, large payloads or the challenges of a metallic environment that are encountered at 13.56MHz. Read range is a card issue just as much as a reader issue, and it is critical to understand the science if there is ever to be success with PIV cards or smart phones, derived credentials, and NFC card emulation modes, especially since phones likely will have a smaller antenna than cards. Further, use of phones will be driven by EMV (contactless credit card) standards that limit the maximum distance to 4 cm.

Cards are passive, not active. They have no batteries and no internal source of power. They get their power from the RF energy being emitted by the reader. Available RF power is a function of both distance from the reader and the effectiveness of the coupling in the card's antenna design. Once powered, the card must transmit back to the reader and there may not be enough signal coming from the card for the reader to detect it at a given distance. Pumping more power out of the reader can be counter-productive since it can make it more difficult to detect a small data return signal from the card.

Readers are held to a fixed operation of 13.56 MHz by ISO standards, FCC, CE, etc., but cards are not. Card tuning can vary from 15 MHz to 20 MHz and some can range from the reader resonance frequency (not a good thing) to 24 MHz. Some power-hungry cards also contribute to a loss of data integrity. Many cards falsely tout higher frequency operation as a benefit, as well as higher communication speeds that can actually lead to a reduction in distance (106 kbps is probably optimum). Metallic environments, whether where the reader is mounted or integral to the card, have a significant impact on operation. Card antenna designs developed for contactless memory cards with no contact chip will not be as efficient when a metallic contact chip exists on the card. Adding a large copper 125 kHz Prox antenna ("tri-interface" for legacy) will further affect card operation.

Therefore, while SP800-73-3 and ISO 14443 clearly state a maximum read range for safety of information transfer, there is no support for the requirement of a minimum read range in the EP testing.

Criteria for determining operation at a given distance can be subjective. It will take about 0.6 seconds for a card to provide any feedback because of the crypto boot-up requirements, and the card cannot be moved during such tests, though a typical user will just keep moving the card closer or wave it back out of the RF field in this time. Then, when a reader gives its first indication of a response (LED and/or beeper), a user will often think the job is done, but for PIV, it has only begun. It might take another second or so to complete the read and then the authentication and authorization, resulting in a lock click, different color LED flash or another beep. So tests must be performed by moving a card quickly to the target distance, and then waiting, and waiting, and waiting – without moving the card.

Cards must be tested with readers of various sizes which have different sizes and shapes of antennae. Reader size is a result of where it will be mounted, with thin readers commonly used on aluminum mullions, switch-plate size readers on walls, and sometimes larger readers where greater range and performance is desired.

Consideration should be given to card-to-reader interoperability testing, such as ICAO performs (ISO 10373-6). This approach places responsibility for operation on both the card and the reader.

With all of this said, it is SIA's recommendation that there be no stated requirement for read distances at this time.

Why OSDP Can Play an Important Role in Implementing the FICAM Roadmap

OSDP is a vendor-agnostic protocol designed to enable devices to exchange security information. OSDP is functionally similar to other device interface protocols such as SCSI and USB. Originally designed by HID Global and Mercury Security (subsequently joined by Codebench), OSDP had as an objective to enable control panels to provide control and supervision of readers, door controllers and other attached security components (referred to as peripheral devices). Its bidirectional qualities enable it to be leveraged by identity and credential authentication applications and make it an obvious successor to unidirectional Wiegand.

To improve security, OSDP defines an implementation that provides encryption between control panels and peripheral devices using AES-128 encryption. OSDP supports extensions to the protocol for use with truly transparent readers to authenticate FIPS 201 credentials, thereby eliminating the risks associated with attack-side decision-making. Readers that do not make security-related decisions are inherently less expensive because they do not require the processing power needed to perform cryptographic operations that can be performed by another system component, such as the controller.

PACS manufacturers can use OSDP to configure and use readers of various assurance levels with their own applications, and the detailed result of each transaction can be sent to the PACS through its standard peripheral device interfaces. OSDP allows reader and panel manufacturers to independently develop high-assurance applications around a robust, extensible standard geared to the best practices of the physical security industry.

In 2012, OSDP's three main contributors assigned the rights to the OSDP specification to SIA in order to promote greater adoption of the protocol and, therefore, more interoperability between disparate vendor components. SIA published OSDP as an official SIA specification and has initiated the process for it to become an ANSI standard.

A test suite can be used to demonstrate compliance with OSDP. GSA EP test labs could then refer to a standard protocol to verify security and interoperability.

HSPD-12 PACS Cost Considerations

Modernizing existing PACS components can be achieved by selecting equipment capable of authentication techniques as defined by the various HSPD-12 family of standards and publications. The field controllers, readers, door hardware, cabling, associated systems, programming and maintenance may or may not be expensive to procure, configure and continuously manage. It depends on a local site survey and the choice of vendor, equipment and configuration.

Costs for components have previously been published in the GSA handbook for LACS, but the costs of the legacy or currently available PACS components have not been established. It is not possible to determine whether one topology is "better" than another without comparison of the respective costs to implement and maintain the two approaches. Costs vary, and no two manufacturers do everything the same. However, budgetary discussions in public forums (such as the IAB) indicate that current generation PACS controllers with integral PIV authentication modes, or current generation PACS readers with integral PIV authentication modes, are less expensive than the "bolt-on" replacement approach that requires a reader replacement, a new authentication controller (called a "secure controller" in the EP Spiral 1 test and approval procedures) and possibly two additional servers, each with its own software.

Modernizing (a.k.a., Rip and Replace)

Most federal agencies have been installing PACS components for decades. Many existing systems are installed with dedicated communication paths that have not yet been moved to the agency's IT infrastructure. The PIV card deployment caused a pause in the natural system lifecycle updates. Some of the cost burden being attributed to HSPD-12/PIV is actually normal operating cost and capital investment that is part of agency operations and maintenance.

As PIV-enabled, IT-based products, PACS have many ways to engineer a solution that meets the spirit of HSPD-12. The PIV card is the trusted credential, and authentication of that credential is a must, although most of the current solutions to validate that trust are hardware- and software-heavy. PACS reader transactions rely on fast throughput while still meeting the authentication and authorization priorities of the PIV market.

Depending on how a PACS is implemented, there could be some cost savings by identifying the methods used in the existing PACS installation and determining what is reusable. Field questionnaires from agencies could include questions such as:

- Where is the existing cabling and what are the types of conductors?
- Do the field controllers currently support both authentication and authorization?
- Are the card readers capable of identifying a PIV and PIV-I card?
- Does the current head-end support PIV and PIV-I? If not, can it be upgraded?
- How many power supplies are available and what is their current condition?
- Does the customer require everything to be in racks or wall-mounted?
- How far is the security closet from the closest telecommunications or networking closet?
- What are the distances from the entry controlled doors to the network switch or field controller?

- Are the current field controllers located above the door on the secure side or clustered in a closet?
- Do the current PACS components support Ethernet connections?
- Is the existing door hardware (e.g., DPS, REX, electronic lock) currently functional?
- Does the agency's IT policy allow PACS, field controllers, readers, etc. on the network?
- What is the status of the PACS with regard to certification and accreditation?

This information will allow the agency to develop cost estimates for modernizing an existing PACS or installing a new PIV-enabled PACS. There are approximately 45 qualified HSPD-12 service providers listed on the GSA idmanagement.gov website. The systems integration specialists on the Schedule 70 SIN 132-62 schedule should be able to provide consultation services to assist agencies with enhancing their existing PACS to meet PIV-related standards. In any case, an agency, its integrator and its solution supplier need to fully understand the requirements and context in order to be successful and provide maximum value to all stakeholders.

Service, Support and Reuse

Other variables to consider regarding cost are the specialists assigned to engineer, implement, train and maintain the current or new system(s). The lifecycle management and continuous monitoring aspects of the system deployed by the agency can be expensive. Depending on size, a system could require from one full-time support specialist to 50 or more.

With new programs such as FedRAMP, which accredits cloud solutions, software costs may be decreased, but there is still a field service and preventative maintenance aspect to consider. Mechanical hardware on entry-controlled doors, turnstiles and other components such as cameras and intrusion detection devices may need to be repaired, replaced or updated fairly often depending on usage.

Much of the existing cabling, along with the door hardware related to the existing PACS, could most likely be reused. The agency and a qualified service provider can review the current architecture, cabling and door hardware to capture savings in labor and equipment costs. For example, an existing door position switch (DPS) and request to exit button or device (REX) may use a 2-wire, 4-wire or 6-wire cable (if tamper is also required), and a new field controller will most likely accept that same cabling, but this should be confirmed during the planning process.

Another cost savings consideration with larger campuses and buildings is sharing the fiber optic infrastructure available through an agency's OCIO. Fiber is fast and can be converted to transmit and receive just about any signal to and from a field controller (e.g., RS-232, RS-485 and Ethernet).

Generational upgrades of a field controller to one with integral PIV authentication mode support may be less expensive than adding a parallel or bolt-on system.

Simpler is usually better. It can reduce both costs and support challenges.

End-User Responsibilities

The end-user is ultimately responsible for the security of a site. As PACS get more complicated, end-users will require more knowledge, which they can obtain either through education and training or by engaging specialized professionals.

PACS installations in federal facilities must comply with life safety codes, the Federal Information Security Management Act, Section 508, and the Americans with Disabilities Act (ADA), as well as address personally identifiable information (PII) issues and have a system of record notice (SORN) in the Federal Register, all in addition to meeting HSPD-12 and FICAM requirements. These requirements are unique for each site and are based on specific testing and accreditation criteria.

HSPD-12 and FICAM add requirements to address the threat of identity theft. Each site needs to address this threat in a manner that is appropriate for the given environment. Some baseline lab testing will aid in the selection of a system, but a shared test lab cannot account for every environment in which the federal government installs systems.

Scalable and Interchangeable Systems

Systems have to be able to be upgraded, expanded and adapted, without the need to replace existing wiring, while minimizing the need for replacing previously installed equipment. Attention must be given to preventing single-source situations in which vendor decisions regarding “end-of-life” or survivability may compromise the security and lifespan of an installed system. More importantly, COTS products and systems incorporate federal government requirements and are more competitive and more sustainable than products designed specifically for narrow requirements. Market competitive offerings, designed to meet standards such as those promulgated by SIA or traditional testing bodies, will have their development and support costs amortized over a much larger base.

Barriers and Speed Bumps

Even if the issues of architecture, topology, functional testing and configuration are resolved, there remain significant obstacles in current specifications and publications that do not allow for economical or practical implementation of a PIV-centric PACS in accordance with best practices. They are listed here in the hope that they will be on a checklist to move forward, and to remind us that we cannot test quality into an installation.

1. PACS environmental issues require contactless; contact not suitable.
2. Contactless not allowed for high- or very-high-assurance applications.
3. Contactless not allowed for BIO; PACS therefore cannot use BIO.
4. CAK created for PACS but is "optional" and not always present in PIV cards.
5. Cannot use CAK across government until "mandatory" for six years, when it will be in total card population.
6. SP800-116 permits very high assurance on inner sanctum, not perimeter.
7. FIPS 201-2 does not recognize three-factor authentication.
8. Contactless BIO-plus-CAK is not allowed, even with PIN.
9. SP800-116 says number of factors equals assurance level, in conflict with FIPS 201.
10. HSPD-12 "graduated criteria from least secure to most secure" not met.
11. RFID field is too small, sensitive to metal; cards don't finish transactions.
12. Touch and hold requires audible/visual feedback and retraining of users.
13. Broken antennae result from PIV specifications, or lack thereof.
14. No "discovery" support for version or type of PIV, PIV-I, CAC, etc.
15. Cards have many "options," but there is no guidance for "options" with PACS.
16. Card options not consistent with interoperability goals.
17. NIST states it will introduce new features as options then make mandatory.
18. 15-year delay to beneficial use.
19. 75-bit GSA string equals 153-bit UUID string (with date).
20. Secure messaging should be equally applied to contact and contactless.
21. Secure messaging will likely require a third round of reader replacements.
22. Virtual contact interface needs to become mandatory ASAP, not in 15 years.

Conclusion and Summary

The natural evolution of Physical Access Control Systems (PACS) has led to manufacturers incorporating more sophisticated technologies to meet end-user demand for better risk management solutions in today's cyber and physical threat environment. Cryptographic techniques, such as the use of a Public Key Infrastructure (PKI) and biometrics, often in combination, have been used for well over a decade. Eight years after the government first published FIPS 201 to define the Personal Identification Verification (PIV) card to comply with HSPD-12, generational upgrades to contemporary PACS have assimilated these newer technologies into competitive offerings to meet government and commercial access control market needs.

The Security Industry Association (SIA), an ANSI Standards Developing Organization, strongly believes in industry standards and has published a specification for communication between a reader and a controller called the Open Supervised Device Protocol (OSDP). We believe in industry development of standards that allow flexibility for innovation and value. There is great concern that the new testing approval procedures for Spiral 1 of GSA Approved Product List 2.0 defines a restrictive, singularly-focused approach with a specific topology that is not in the best interests of the customer or the advancement of the market. As it embraces a "proof-of-concept" topology developed years ago, the APL constrains and unduly influences industry pursuit of competitive, scalable products for government applications and does not offer an economically sound or performance-oriented approach.

Accordingly, we recommend a more functional approach to GSA APL testing that determines the processes that a PIV or PIV-I card can implement when used with a PACS and related services, regardless of topology. Topology flexibility is critical since no two enterprises, facilities, buildings or even doors and related environments are identical. The testing and approval procedures should focus on confirming that specific, desired processes can be achieved, and not focused, explicitly or implicitly, on how a system is built.