Security Equipment Integration Working Group

Review of the Open Supervised Device Protocol (OSDP™) For DoD Applicability

1 August 2014

Security Classification: UNCLASSIFIED

DISTRIBUTION STATEMENT A. Approved for public release.

DOCUMENT REVISION HISTORY

Revision	Date	Description of Change	Responsible Person
1.0	2014-08-01	Final	SEIWG

Table of Contents

1 INTRODUCTION 5

2 OSDP™ SYNOPSIS 5

2.A SIA STANDARDS COMMITTEE 7
2.B VENDORS OF COTS PRODUCTS SUPPORTING OSDP™ 8
2.C OSDP™MESSAGE SUMMARY 8

3 PHYSICAL ACCESS CONTROL SYSTEMS 9

3.A PACS ARCHITECTURES 9
3.B DOD PACS 10

4 FEDERAL PACS GUIDANCE 10

4.A FISMA 10
4.B HSPD-12 10
4.C FIPS 201 11
4.D FEDERAL CIO COUNCIL 11
4.E FICAM 12
4.F IDENTITY ASSURANCE LEVELS 12
4.G APPROVED PRODUCT LISTS (APL) 13
4.H FICAM FUNCTIONAL REQUIREMENTS 14
4.I DYNAMICALLY CONFIGURABLE AUTHENTICATION MODES 15
4.J ENTRY POINTS 15
4.K NATIONAL SECURITY SYSTEMS 15

5 ANALYSIS 15

5.A PACS INTEGRATION 15
5.B LEGACY WIEGAND DEVICES 16
5.C RS-485 17
5.D ENCRYPTION 17
5.E TAMPER DETECTION 18
5.F CABLE AND WIRING 19
5.G BIOMETRICS 19
5.H OSDP™ EXTENSIBILITY 19

6 SUMMARY 20

7 REFERENCE DOCUMENTS 21

List of Tables

TABLE 1. WIEGAND VS. OSDP™ COMPARISON 7
TABLE 2. OSDP™ PLUGFEST 8
TABLE 3. OSDP™ MESSAGE SUMMARY 8

List of Figures

FIGURE 1. TYPICAL PACS ARCHITECTURE 6

1 INTRODUCTION

This White Paper is intended for distribution to the SEIWG Service Representatives and, through them, to the four Department of Defense (DOD) Services. It summarizes technical research completed by the SEIWG on a Security Industry Association (SIA) standard referred to as Open Supervised Device Protocol (OSDP™) specification, Version 2.1.5 [1][1]. OSDP™ is an interface standard used within a Physical Access Control System (PACS), which is applicable to access control system (ACS) functionality with relevance to intrusion detection system (IDS) functionality.

The purpose of this White Paper is to assist technical engineering efforts to acquire, sustain or upgrade a PACS for DOD installations. In particular, it introduces OSDP™ and discusses factors to consider when evaluating whether or not OSDP™ should be used. It discusses the relationship of OSDP™ to the Federal requirements and guidance for PACS.

Section 2 provides a brief synopsis of the OSDP™ standard with subsections about the SIA standards committee and vendor support for OSDP™. Section 3 discusses PACS with subsections covering architecture and DOD PACS. Section 4 discusses the Federal requirements and guidance related to PACS. Section 5 provides analysis. Section 6 provides a summary, and Section 7 lists numerous references which were examined during the research for this paper, some of which are also cited in the text[2].

2 OSDP™ SYNOPSIS

In the early 2000's several security-based companies began working together to develop protocols for interfacing with various peripheral devices (PD)/card reader products used in an Access Control System. The solutions were device-specific however. In 2005, several of the companies began developing an open protocol which was then assigned to the Security Industry Association (SIA) in 2012. SIA is a trade group for businesses focusing on the physical security industry. As such, SIA is involved in the development of open industry standards.

The OSDP™ is a non-proprietary specification that defines a communication protocol for interfacing components of a PACS. Specifically, the specification typically applies to the interface between a Control Panel (CP) and one or more Peripheral Devices (PD). A typical PD is a card reader used to input data from a magnetic stripe card, proximity card, or Personal Identity Verification (PIV) smartcards which support an ISO 14443 contact and/or contactless interface. Other PDs, such as a door input/output controller, support inputs from a keypad, monitoring points for sensors and door position or control outputs to activate electronic door latches, buzzers, LEDs, or text on an LCD display. OSDP™ has been developed to support the use of manufacturer-specific commands while still promoting interoperability and ease of configuration. Figure 1 provides a general representation of a PACS[3]. OSDP™ is typically used for interface {1}. OSDP™ is being positioned to replace the current "de facto" interface which

[1] Numbers within brackets (e.g., [1]) are used as a citation method to refer to a corresponding Reference entry in Section 7 of this white paper.

[2] References which are not explicitly cited within the text are included because they provide supporting detail.

[3] For discussion in this white paper, the OSDP interface points in Figure 1 are identified with {1}.

is considered to be the Wiegand standard [2]. Although Wiegand or OSDP™ may be applied to the interface between a CP and the PD {1}, there are four main differences between the specifications as summarized in Table 1 [43].

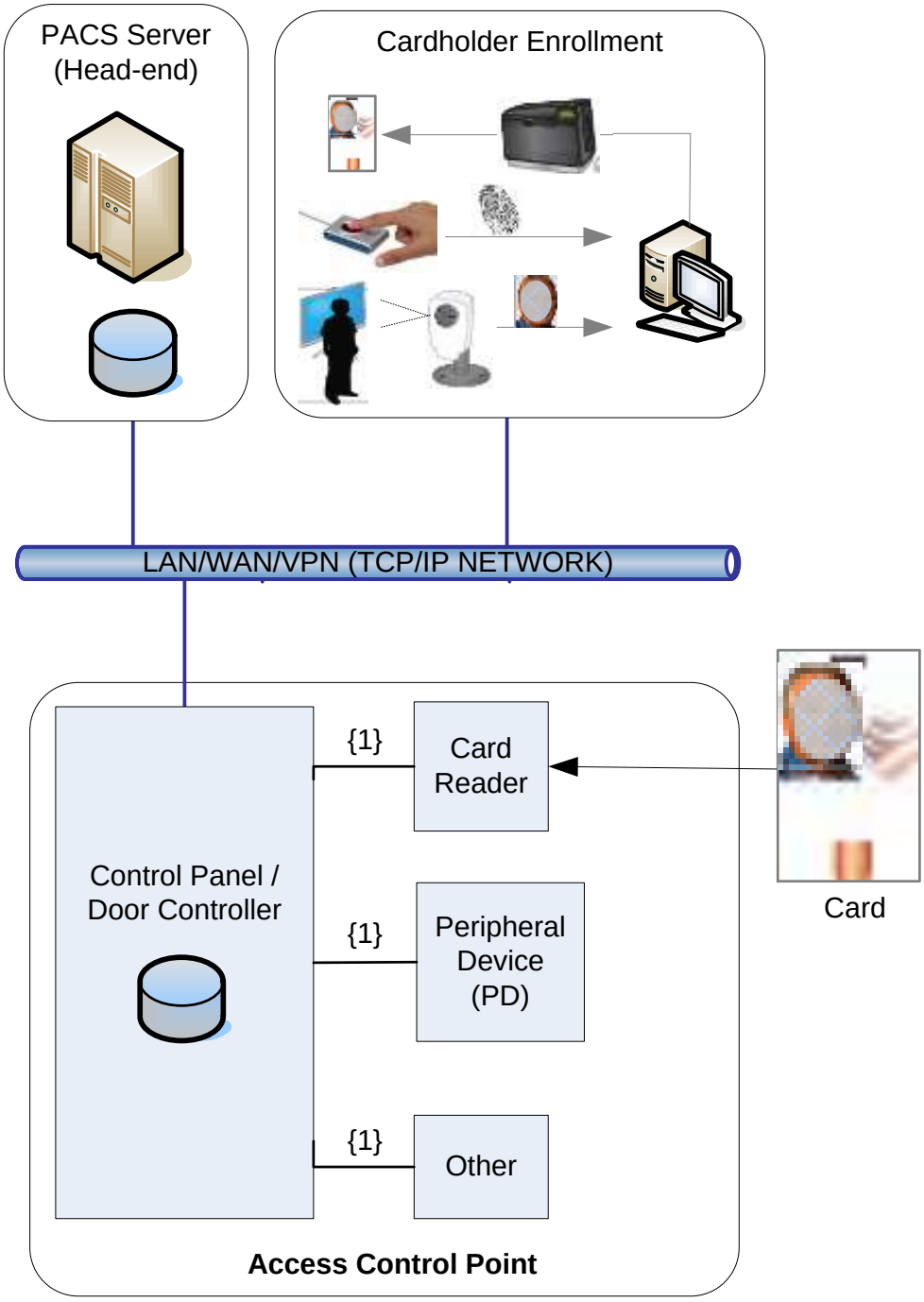

Figure 1. General Representation of a PACS

Table 1. Wiegand vs. OSDP™ Comparison

	Wiegand [2]	OSDP™ [1]
Bi-directional communication	No	Yes
Packet Size[4]	~48 bits[5] (max)	1440 Bytes (max)
Data Interface	Wiegand only	Serial
Multi-drop support	No	Yes

OSDP™ builds upon a half-duplex, serial RS-485 physical interface which supports bi-directional communication. Bi-directional communication supports continuous monitoring of the PDs by the CP which is not supported in a unidirectional implementation. Benefits of monitoring include the ability of a CP to quickly detect a problem in a PD, such as a tamper or device failure. Additionally, the bi-directional communication allows a CP to capitalize on advancing "reader" or PD technologies and capabilities, such as Smartcards and mobile devices.

OSDP™ currently supports a serial RS-485 interface but the specification is extensible and SIA plans to include support for Internet Protocol (IP) communications over Ethernet in the future. As of July 2014, there are no known commercial implementations of OSDP™ over IP (either TCP or UDP).

The amount of data exchanged in an access control system has increased significantly in recent years as the result of added encryption, the use of smartcards, and the inclusion of biometric data. OSDP™ supports a higher throughput than the Wiegand standard and can sustain the needed level of data exchange to meet performance requirements.

Rather than the "point-to-point" or "1:1" interface which the Wiegand standard supports, RS-485 supports a "multi-drop" configuration with "daisy-chained" cabling. This can reduce cabling costs.

2.A SIA STANDARDS COMMITTEE

The Access Control & Identity Subcommittee of the SIA Standards Committee led the development of the protocol detailed in the OSDP™ specification [1]. The subcommittee consists of industry representatives, manufacturers, integrators and end-users who worked to develop the protocol and produce the specification.

The specification underwent a multi-faceted review before being released. Currently Version 2.1.5 has been released by SIA but the Subcommittee is now working to prepare Version 2.1.6 of the specification which will be forwarded to be accepted as an ANSI standard. The OSDP™

[4] The IPVM paper [43] discusses throughput, but this white paper instead compares packet size. Wiegand interfaces are not usually expressed in terms of packet size, but different card formats are possible and depend on the particular reader and control panel used. 26-bit and 37-bit card formats are commonly supported over Wiegand interfaces.

[5] Wiegand communications typical for PACS are limited to 48 bits, which is insufficient to transmit the full CHUID [33].

Working Group will begin working on profiles that specify "levels" of OSDP™ conformance based on use cases. The OSDP™ Working Group will work on extending OSDP™ to work over IP networks.

2.B VENDORS OF COTS PRODUCTS SUPPORTING OSDP™

Vendor commercial-off-the-shelf (COTS) offerings for OSDP™ are currently limited. OSDP™ was demonstrated at the "OSDP™ Plugfest"[6], which was held at the ISC West conference in April 2014. OSDP™ interoperability was demonstrated by the vendors and products listed in Table 2.

Table 2. OSDP™ Plugfest

Vendor	Devices Demonstrating OSDP™
Allegion	AptiQ MT15-485 Reader
Axis Comm	A1001 Network Controller
HID Global	iCLASS SE and multiclass readers[7]
IQ Devices	INID Multismart Reader
Mercury Security	EP 1510 Control Panel
Siemens	SiPass Integrated Control Panel
Identive	(demo planning)

2.C OSDP™ MESSAGE SUMMARY

Table 3 lists the message defined in the OSDP™ specification [1]. Commands are sent from the CP to the PD, and Replies are sent from the PD to the CP. In Table 3, the Reply on the right is not necessarily a response to the Command in the same row on the left. Further explanation of these messages is beyond the scope of this white paper.

Table 3. OSDP™ Message Summary

Command (CP-PD)	Replies (PD-CP)
Poll (osdp_POLL)	Command accepted, nothing else to report (osdp_ACK)
ID Report Request (ospd_ID)	Command not processed (osdp_NAK)
PD Capabilities Request (ospd_CAP)	PD ID Report (osdp_PDID)
Diagnostic Function Control (osdp_DIAG)	PD Capabilities Report (osdp_PDCAP)
Local Status Report Request (osdp_LSTAT)	Local Status Report (osdp_LSTATR)
Input Status Report Request (osdp_ISTAT)	Input Status Report (osdp_ISTATR)

[6] A "PlugFest", aka PlugTest, is an event based on a certain standard (in this case, OSDP) where the designers of electronic equipment or software test the interoperability of their products or designs with those of other makers. http://en.wikipedia.org/wiki/Plugtest

[7] According to the HID iCLASS How to Order Guide [52], pgs 42-43, OSDP support is listed. The HID pivCLASS How to order Guide [53], which is a little older, mentions OSDP v1.

Command (CP-PD)	Replies (PD-CP)
Output Status Report Request (osdp_OSTAT)	Output Status Report (osdp_OSTATR)
Reader Status Report Request (osdp_RSTAT)	Reader Status Report (osdp_RSTATR)
Output Control Command (osdp_OUT)	Reader Data—Raw bit image of card data (osdp_RAW)
Reader Lead Control Command (osdp_LED)	Reader Data—Formatted character stream (osdp_FT)
Reader Buzzer Control Command (osdp_BUZ)	Keypad Data (osdp_KPD)
Text Output Command (osdp_TEXT)	PD Communications Configuration Report (osdp_COM)
Time and Date Command (osdp_TDSET)	Biometric Data (osdp_BIOREADER)
PD Communication Configuration Command (osdp_COMSET)	Biometric Match Result (osdp_FPMATCHR)
Data Transfer Command (osdp_DATA)	Client's ID, Random Number and Crptogram (osdp_CCRYPT)
Set Automatic Reader Prompt Strings (osdp_PROMPT)	Initial R-MAC (osdp_RMACI)
Scan and Send Biometric Data (osdp_BIOREAD)	PD is Busy reply (osdp_BUSY)
Scan and Match Biometric Template (osdp_BIOMATCH)	Manufacturer Specific Reply (osdp_MFGREP_
Encryption Key Set Command (osdp_KEYSET)	Extended Read (osdp_XRD)
Challenge and Secure Session Initialization Rq. (osdp_CHLNG)	
Server Cryptogram (osdp_SCRYPT)	
Continue Sending Multi-Part Message (osdp_CONT)	
Manufacturer Specific Command (osdp_MFG)	
Extended Write (osdp_XWR)	

3 PHYSICAL ACCESS CONTROL SYSTEMS

3.A PACS ARCHITECTURES

Figure 1 provides a general representation of a PACS[8] and identifies where OSDP™ would apply. Wikipedia [11] offers several variants on Figure 1. Although depicted in Figure 1, cardholder enrollment is out of the scope of this white paper.

The FICAM/FIPS 201 testing program uses the term "topology" for a particular combination of devices forming a PACS. Before adopting a flexible approach to topologies, the GSA's FIPS 201 approved product list (APL) was more rigid. SIA provided feedback [39], which resulted in the FICAM Testing Program Functional Requirements and Test Cases (FRTC) [31], and a process [35] to submit and approve alternative topologies which map to the FRTC. With these changes to the FICAM Testing Program, it is less likely that innovative commercial solutions would be excluded from the GSA APL if they did not align exactly to one particular topology.

[8] For discussion in this white paper, the OSDP interface points in Figure 1 are identified with {1}.

Two topologies have been defined and provisionally approved, which are known as the 13.01 Topology [49] and the 13.02 Topology [50]. Topology 13.01 includes three broad categories of devices: PACS Infrastructure, Validation System, and PIV Readers. Topology 13.02 includes two broad categories of devices: PACS Validation and Infrastructure (PVI) and PIV Readers.

3.B DOD PACS

Research for this white paper did not attempt to survey DOD installations to determine what PACS hardware and software are used. Instead, some of the vendors of PACS which are known to be used on DOD installations were studied to learn more about their approach to supporting OSDP™.

4 FEDERAL PACS GUIDANCE

A plethora of requirements and guidance from the Federal Government has been promulgated which will influence decisions about the procurement of PACS.

4.A FISMA

The Federal Information Security Management Act of 2002 (FISMA) (Title III of Public Law 107-347) was concerned more about information security than physical access to federal facilities. However, FISMA is relevant because Homeland Security Presidential Directive 12 (HSPD-12) [4], "Policy for a Common Identification Standard for Federal Employees and Contractors", conflates access to information systems and access to facilities around a single form of identification.

The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of FISMA. NIST is part of the Department of Commerce, and its publications provide a foundation for much of the federal PACS guidance.

Annual reporting of metrics for FISMA may include measures related to PACS. Office of Management and Budget (OMB) memos are issued with instructions for FISMA reporting, and DHS provides the questions which are to be answered by each agency's chief information officer (CIO) and inspectors general (IG).

4.B HSPD-12

HSPD-12 issued the policy to establish a "mandatory, Government-wide standard for secure and reliable forms of identification". HSPD-12 also directed "the use of identification by Federal employees and contractors that meets the Standard in gaining **physical access** to Federally controlled facilities and **logical access** to Federally controlled information systems".

The Secretary of Commerce was assigned the responsibility to promulgate the Standard in consultation with Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. HSPD-12 required the Secretary of Commerce to periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

According to HSPD-12, departments and agencies are required to implement HSPD-12 in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

4.C FIPS 201

The "Standard" directed by HSPD-12 is FIPS 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors", initially published by NIST in Feb 2005. OMB memorandum M-05-24 clarified several aspects of HSDP-12, such as, the definition of "Federally controlled facilities". FIPS 201 references a number of Special Publications for technical details, which further reference various other related standards from other standards development organizations. However, at this time, FIPS 201 and related publications do not prescribe a standard protocol for use between a card reader and a PACS control panel. That is, OSDP™ is not prescribed by the FIPS 201 guidance at this time.

FIPS 201 (2005) was superseded by FIPS 201-1 (2006), which was superseded by FIPS 201-2 (2013). Some of the NIST Special Publications referenced from FIPS 201-2 cite the current approved version "or as amended"; some amended specifications are available in draft.

Several DOD issuances address PACS. Directive-type Memorandum (DTM) 14-005, DOD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files [25], directs USD(I) to "develop technical and interface requirements for card issuance, revocation notification, and system interoperability with physical access control systems (PACS) and the interoperability layer service (IoLS)." DTM-14-005 also states that "the PACS will support a DOD-wide and federally interoperable physical access control capability compliant with Homeland Security Presidential Directive-12". DTM-14-005 references DTM-09-012[9] [23], which is to be incorporated into DOD 5200.08-R [22] and DODI 5200.08 [57]. With regard to PACS, DTM-09-012 states the following:

> *"When funding becomes available, installations will procure an electronic PACS that provides the capability to rapidly and electronically authenticate credentials and individuals authorization to enter an installation. The PACS must support a DOD-wide and federally interoperable access control capability that can authenticate USG[10] physical access credentials and support access enrollment, authorization processes, and securely share information."*

DOD has been making progress toward implementation of HSPD-12 as reported by the DOD Inspector General [19][20]. The DOD FY13 FISMA Report [60] references additional DODIG reports [61][62].

4.D FEDERAL CIO COUNCIL

The Federal Chief Information Officers (CIO) Council is chartered [56] to (among other things) develop recommendations for the OMB on Federal Government IT management policies and requirements. Of relevance to PACS is the Information Security and Identity Management

[9] Incorporates Change 4, 22 April 2014

[10] United States Government

Committee (ISIMC)[11] and its Identity, Credential, and Access Management Subcommittee (ICAMSC) with the charter to foster effective ICAM policies and enable trust across organizational, operational, physical, and network boundaries. One key document from ICAMSC is the PIV in E-PACS document [33].

4.E FICAM

OMB Memorandum M-11-11 [41] "outlined a plan of action to expedite the Executive Branch's full use of the PIV credentials and required each agency to develop and issue an implementation policy … through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. To support this effort, the Federal CIO Council and OMB developed a segment architecture for identity, credential, and access management (ICAM)." [12] This segment architecture[13] is part of the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance [30][14]. The "FICAM Roadmap" includes 9 initiatives, one of which is to modernize PACS infrastructure (Initiative 7, Chapter 10).

The term "FICAM" has come to be synonymous with "FIPS 201".

SIA has made presentations to the Government Smart Card Inter-agency Advisory Board (IAB) on OSDP™ [26] and on migration of PACS to PIV and PKI [55]. SIA has also provided a white paper on PACS in a FICAM Framework [39].

OSDP™ states that "the OSDP™ Specifications address a mechanism for passing messages (APDUs) between authentication software and a smartcard transparently, without reader support. This mechanism is intended to support FICAM compliant authentication ..."

APDUs (Application Protocol Data Units) are the messages sent to/from a smartcard (CAC or PIV).

4.F IDENTITY ASSURANCE LEVELS

FIPS 201-2 defines four assurance levels[15]: LITTLE or NONE, SOME, HIGH, and VERY HIGH. Table 4 shows the various authentication mechanisms which have been defined and the corresponding assurance level provided by them. The capability of the devices procured for a PACS is dictated to an extent by the assurance level required for a given installation (or protected area within an installation). Note that some authentication mechanisms, namely VIS and CHUID, were downgraded in FIPS 201-2 (LITTLE or NONE) from their assurance level in FIPS 201-1 (SOME).

---

[11] https://cio.gov/about/groups/information-security-identity-management-committee/

[12] See [58]

[13] Segement architectures are defined within the context of the Federal Enterprise Architecture, http://www.whitehouse.gov/omb/e-gov/FEA

[14] Version 1.0 was published in 2009, and Version 2.0 [30] was published in 2011. An update is in progress [47]. See also http://www.idmanagement.gov/ficam-roadmap-update

[15] Also defined in OMB M-04-04.

Table 4. Assurance Levels

Authentication Mechanism[16]	FIPS 201-1	FIPS 201-2
VIS	SOME	LITTLE or NONE
CHUID	SOME	LITTLE or NONE
PKI-CAK	-	SOME
SYM-CAK	-	SOME
BIO	HIGH	HIGH
BIO-A	VERY HIGH	VERY HIGH
OCC-AUTH	-	VERY HIGH
PKI-AUTH	-	VERY HIGH
PKI	VERY HIGH	-

"PKI-Card Authentication Key (PKI-CAK): A PIV authentication mechanism that is implemented by an asymmetric key **challenge/response protocol** using the Card Authentication key of the PIV Card and a contact or contactless reader."

"PKI-PIV Authentication Key (PKI-AUTH): A PIV authentication mechanism that is implemented by an asymmetric key **challenge/response protocol** using the PIV Authentication key of the PIV Card and a contact reader, or a contactless card reader that supports the virtual contact interface."

The challenge/response protocol may require bi-directional message exchange between the reader and control panel. Legacy Wiegand does not support bi-directional flow; it only sends from reader to control panel. But if the challenge/response is just between the card and the reader, and the reader only sends to the control panel after the reader completes the authentication, then perhaps a bi-directional interface between the reader and control panel is not needed (and the link between the reader and the control panel does not need encryption).

4.G Approved Product Lists (APL)

OMB Memorandum M-06-18 requires Federal Agencies to procure only qualified products and services listed on the GSA Approved Products List (APL) when implementing HSPD-12 into their environment. Products are added to the APL after successful compliance testing. Originally known as the FIPS 201 Testing Program, testing for FIPS 201 compliance is now part of the FICAM Testing Program. A wide variety of products are listed on the APL [66], but there is also a related APL for PACS [65]. In addition, products removed from the APL are placed on the Removed Products List (RPL)[17].

[16] Appendix B of NIST SP 800-73-3 (or draft 800-73-4) Part 1 provides sequence diagrams which help understand these authentication mechanisms.

[17] http://idmanagement.gov/removed-products-list

The card readers listed on the FIPS 201 Approved Product List (APL) include pivCLASS readers from HID Global, but these are not the class of readers which were used for the OSDP™ Plugfest.

DOD contracts may restrict procurement of security equipment to items on other APL's or Approved Equipment Lists (AELs) (e.g., [44]). These AELs may focus on other physical security systems, such as an Intrusion Detection System (IDS) or Video Management System (VMS). In some cases, PACS components are integrated into the annunciators which are listed on the IDS AEL. There may be opportunities to leverage the GSA FICAM/FIPS 201 testing program in qualifying products for DOD AELs (whose scope may not be limited to or focused on PACS).

4.H FICAM FUNCTIONAL REQUIREMENTS

A recent document titled "Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS)" [33] provides an excellent discussion of "the current PACS landscape, as well as current standards and guidance that directly or indirectly affect PACS." It states that

> *"the PACS must support bi-directional communications in order to perform challenge/response activities with PIV and PIV-I Cards. This may include updating physical cabling links between the reader and controller/panel and shifting away from the Wiegand Protocol commonly used for unidirectional communication today."*

It also talks about the need for bi-directional communications when card readers support dynamic reconfiguration of the reader's authentication mode. However, PIV in E-PACS [33] does not explicitly prescribe OSDP™ as the protocol for achieving this capability.

The PIV in E-PACS document, section 8, states that "as a federal information system, an E-PACS is subject to (SP 800-53) security controls and the NIST Risk Management Framework to ensure that it is correctly protected". PIV in E-PACS [33] augments the security controls from SP 800-53 with additional controls specific to E-PACS.

OSDP™ is mentioned briefly with the FICAM functional requirements (FRTC [31]). The FRTC defines 251 tests divided among 6 sections (numbered 2 – 7). Section 7 is PACS Design and has 76 tests across 11 subsections. Section 7.7 deals with Portal Hardware (14 tests). Test #227, section 7.7.13, verifies an optional security requirement where "the System shall protect the communications between readers and the PACS using a cryptographically secure protocol". The Pass/Fail criteria say "FICAM profile for OSDP™ to be developed in next spiral of FICAM Testing Program". Most FRTC tests are cross-referenced to specific security controls the PIV in E-PACS [33] guidance. Test #227 is cross-referenced to PSC-1, Communication between System Elements, which is a security control that protects communications and detects tampering.

In addition to the PSC-1 security control, other security controls may be applicable to OSDP™. PACS Configuration Management (PCM) Control PCM-3 is for configuring reader authentication modes. PCM-3 maps to several tests in the FRTC document, but perhaps the one most relevant to OSDP™ is test #215, section 7.7.1. It is a required security requirement stating that the "product shall support Reader to PACS communications using bi-directional technology.

This includes a minimum of one of RS-485, Ethernet, or secure wireless". However, it does not mention OSDP™ explicitly.

4.I Dynamically Configurable Authentication Modes

If a two-way interface is supported between a CP and PD, then it may be possible to change the authentication mode, for example, from single factor to double factor, using commands from the CP to the PD (reader). This may be useful if the strength of authentication needed changes based on factors like the Force Protection Condition (FPCON) level or whether an entry portal is manned (weekdays daytime) or unmanned (nights, weekends). These and other considerations are listed in DTM 09-012 [23]. OSDP™ would play a supporting role in providing such dynamic configurations in that is supports commands related to PIN entry and biometrics, but the control panel software would need to orchestrate these configuration changes by its selection of which OSDP™ commands to use for a particular configuration.

4.J Entry Points

The strength of authentication is often decided by the location of the entry point. The perimeter of a military base needs to balance the throughput required for automobile traffic entering the base at rush hours where the speed of authentication is important to avoid delays. Contrast perimeter access control to a restricted room deep within a building which has fewer entries and the delays associated with strong authentication (e.g., PIN entry and biometric readings) are tolerable.

4.K National Security Systems

The definition of a National Security System (NSS) is provided in Title 44 of the United States Code (44 U.S.C.) Chapter 35, section 3542(b)(2). Much of the Federal guidance explicitly excludes NSS. It is not clear to what extent DOD PACS could be considered a NSS. It should be noted that even if a PACS is considered to be a NSS, this would only exclude the use of PIV for the Logical Access Control System (LACS) used to authenticate and authorize users of the PACS. This same PACS could be used to control access to the installation, but the installation would not be considered an NSS. Therefore, physical access to the (non-NSS) installation would be governed by (not exempted from) the Federal guidance which applies to non-NSS. The person entering the installation is not using the PACS in the same sense as the security forces personnel who monitor and control the PACS and associated intrusion detection and assessment systems. Even if a NSS resides within a restricted area, the restricted area is not an Information Technology (IT) system. The NSS designation is usually associated with an IT system.

OMB Memorandum M-14-04 [58] provides some discussion of NSS and refer to CNSSI 1253 [59] for more guidance.

5 Analysis

5.A PACS Integration

PACS integration is examined from several points of view. First, it is often the case for DOD procurements that integration of the components which constitute a PACS is outsourced to a contractor. The choice of using OSDP™ within a particular PACS deployment is usually

decided by the organization (contractor) who is responsible for integration. The FICAM/FIPS 201 Testing Program acknowledges this by the emphasis on end-to-end PACS testing. The GSA PACS APL V2[18] lists the commercially-available products in approved configurations for procurement by federal agencies. According the FAQ [54], end-to-end system testing is beneficial for the following reasons:

- PACS products, by their nature, tend to be purchased as complete systems as opposed to individual components.
- By testing and approving entire systems, agencies will find it easier to identify and procure systems that meet their needs and be fully functional once installed.
- This testing leverages recent guidance regarding the deployment of PIV-based PACS (e.g., Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0, March 26, 2014).

On the PACS APL V2, currently there is approval for 6 different card readers (all from HID global) and 4 different PACS infrastructures (3 vendors: Tyco Software House, Brivo, and Hirsch). Products from other PACS vendors are progressing through the testing program: some have been tested (results being reviewed), testing is in progress, application for testing has been approved (but not yet scheduled), or application for testing is under review.

Secondly, PACS is often integrated with other systems to provide overall physical security. For example, a balanced magnetic switch (BMS) detects when a door has been opened. The PACS controller often unlocks the door in response to an authenticated and authorized cardholder attempting entry, and opening of the door is expected for some short amount of time. However, if the door is opened long after any authorized entry, then the BMS detection is expected to trigger the Intrusion Detection System (IDS). Likewise, video cameras may support visual authentication at entry points, but the video also feeds into a Video Management System (VMS) which supports assessment of alarms triggered by the IDS. DOD contractors are often responsible for integration of these various systems and subsystems. Again, the choice of using OSDP™ is one of many factors which are considered by the integrator.

5.B LEGACY WIEGAND DEVICES

It is important to understand that the term "Wiegand" can refer to either (1) a type of card, which uses "Wiegand wires" and the Wiegand "effect", or (2) the Wiegand "interface". The early card readers used both Wiegand cards and the Wiegand interface (from the reader to the control panel). However, today it is common to find readers that work with more modern cards (e.g., smartcards) but still use the Wiegand interface to send data from the card to the control panel. The Wiegand interface was originally based on the Wiegand card limitation of the number of physical Wiegand wires which fit on a standard size card, and this influenced the number of bits available for a card number. The "universal format", based on the original Wiegand cards and readers, is 26 bits, two of which are parity bits, leaving 24 bits for a card number. Furthermore, these 24 bits included an 8 bit "facility code" and a 16 bit identifier for the individual card (or card holder) associated with that facility.

[18] http://www.idmanagement.gov/pacs-apl-v2

The Smart Card Alliance published a document responding to requests for sample Wiegand message formats that will handle the additional fields of the Federal Agency Smart Credential Number (FASC-N) [40].

5.C RS-485

Many vendors' data sheets list support for RS-485. However, this does not necessarily mean that the device supports OSDP™ (over the RS-485 interface).

RS-485 is a physical layer signaling standard over which various (often proprietary) data link protocols are transmitted. When reading vendor data sheets, be careful to not read too much into the listing of RS-485 support. Seek additional information from the vendor to confirm that OSDP™ is supported if a data sheet mentions RS-485 but does not mention OSDP™ explicitly.

RS-485 can be used over longer lengths of wiring when compared to Wiegand interfaces and Ethernet. RS-485 can also be daisy-chained (e.g., from CP to PD to PD to PD …), which offers some additional flexibility in selecting a location for the CP. The maximum data rate supported by RS-485 will depend on wiring and other factors [9].

5.D ENCRYPTION

The need for encryption between a card reader (or other peripheral devices) and the control panel is a local decision based on the perceived threat or vulnerabilities of the environment. For example, a device known as "Gecko" has been demonstrated as a man-in-the-middle (MITM) attack, but it requires physically breaking the wires between the reader and control panel to insert the Gecko device.[3] One should consider the likelihood of an attacker gaining physical access to this cable.

There may be good reason to make sure that the card presented to the reader by the cardholder is (or contains) a valid credential. This may require cryptographic protocols to and from the card (in this case, a "smartcard"). A challenge-response protocol exchange between an "on-card" entity and an "off-card" entity can be part of this validation. The "off-card" entity could be the reader, or perhaps this entity resides in the control panel such that the challenge-response must pass across the interface between the reader and the control panel.

Smartcard standards define a Secure Channel Protocol (SCP) [45] which can be used between the card and an "off-card" entity.

OSDP™ supports optional encryption over RS-485 between the reader and the control panel. The OSDP™ defines one approach for encryption based on SCP. OSDP™ also defines a profile for a transparent mode of operation where data (an APDU) is passed between the card and the control panel. However, it’s not clear if the endpoints of the secure channel can be between the control panel and the smartcard without terminating in the reader.

Typically the Wiegand interface between a reader and control panel would not be encrypted. There may be proprietary approaches to encrypting Wiegand interfaces, but in general Wiegand interfaces are not encrypted.

5.D.1 KEY MANAGEMENT

SCP [45] specifies AES[19], which is a symmetric key encryption algorithm which uses the same (secret) key for both encryption and decryption. Thus the same key must be loaded into both the sender and receiver. Key management refers to the procedures used to generate, distribute, and load these keys. Although the SCP specification allows for AES-128, AES-192, and AES-256, the OSDP™ specification does not define values (for Function Code 009) for AES-192 and AES-256.

Using the SCP option of OSDP™ imposes requirements for loading secret (symmetric) keys into various devices. The OSDP™ specification suggests, but does not prescribe, that readers which support OSDP™ with SCP have configuration settings to enable "installation mode" whereby a default Secure Channel Base Key (SCBK-D) can be used while a control panel generates an SCBK for each reader to be used after "installation mode" is disabled.

If the intent is to use SCP with the transparent mode of OSDP™, then the AES key would need to reside within the smartcard (PIV or CAC) and the control panel. FIPS 201-2 defines a symmetric Card Authentication key (SYM-CAK) as an optional data element of the PIV data model, which has been examined for PACS applications [63].

Asymmetric cryptography involves a secret private key (which is not shared) and a public key (which can be widely available through a variety of repositories and exchange methods). A Public Key Infrastructure (PKI) is used to manage the generation of the public-private key pairs, as well as the associated X.509 certificates used to distribute the public key and related metadata. Since OSDP™ specifies SCP03, which uses symmetric keys (i.e., AES), PKI is not applicable to the encryption of OSDP™ messages.

FIPS 201-2 adds Secure Messaging, which is required for the Virtual Contact Interface (VCI) and is used for non-card-management operations. Draft SP 800-73-4 Part 2 specifies a key establishment protocol (section 4.1); secure messaging (section 4.2) uses the symmetric session keys derived using the key establishment protocol. Secure messaging uses AES as the encryption algorithm, which is the same as SCP03. OSDP™ and SCP03 do not define a key establishment protocol. The FIPS 201-2 secure messaging does not use the SYM-CAK key. Further study is needed to determine if SCP03 could be used between the CP and a PIV/CAC card and if the key establishment protocol defined in SP 800-73-4 can be used. This may provide encryption where needed without the need to manage symmetric keys for each PD.

5.E TAMPER DETECTION

Some PDs have a separate wire to signal a tamper condition to the control panel, which is sent on a different wire than the Wiegand or RS-485 signals. When the PD is a door controller, then the reader is external to the PD. OSPD supports a message (OSDP™_RSTATR) which allows the door controller to send a tamper indication over the RS-485/OSDP™ line when it detects a change in the tamper wire from the reader. In other cases, the PD may receive a tamper signal when the enclosure door is opened, in which case a different message (OSDP™_LSTATR) is used to inform the CP of the tamper.

[19] Advanced Encryption Standard is defined in FIPS 197

Other PACS standards, such as, UL294 [15], also address tampering and line supervision. OSDP™ is a half-duplex protocol with periodic polling from the CP. The PD that is polled must reply within a configurable Reply Delay setting, which is typically 3 milliseconds, but is not to exceed 20 milliseconds. If the CP does not receive a reply before the Reply Delay setting, the CP re-sends the last command. It is likely that tampering with the cabling to the PD would prevent transmission of any reply (including the OSDP™_RSTATR tamper message). The OSDP™ specification [1] says that the PD waits 8 seconds until it considers the communications off-line, after which the PD and CP reinitiate a new connection sequence. In the absence of a separate, supervised, tamper wire, the loss of the connection could implicitly indicate a possible tampering of the RS-485 wiring, but the OSDP™ specification [1] does not elaborate on this situation. Some form of line supervision may be required if the CP cannot leverage OSDP™ timers to detect tampering of the RS-485 wiring.

5.F Cable and Wiring

It is assumed that many card readers which exist in DOD installations interface to a control panel using a Wiegand interface which uses three wires: Data1 (D1), Data0 (D0), and common ground. Often additional wires are used between the reader and control panel. A cable running between the control panel and the reader is likely to have more than the three wires required for the Wiegand interface. The wires used with Wiegand readers may not be twisted pairs, which are used for RS-485 interfaces. Therefore, replacing a reader which provides a Wiegand interface with another reader which supports RS-485 and OSDP™ is likely to require new twisted pair wiring.

OSDP™ supports several messages, which are sent over the RS-485 link, which may obviate the need for separate wires between the reader and control panel. For example, wires used to activate LEDs and buzzers can be eliminated if the OSDP™ Reader LED Control Command is used instead. The previous section discussed OSDP™ messages which can report on some tamper conditions and concerns with detection of tampering on the RS-485 wiring.

5.G Biometrics

Some Wiegand-based readers support multiple inputs: a card reader, PIN keypad, and a fingerprint reader, for example. In such a reader, sometimes the number read from the card is sent over a Wiegand interface, but fingerprint data would be sent over a different interface. For example, an RS-485 interface (not using OSDP™) may be used to send fingerprint templates to a reader. A fingerprint scan at the reader is then matched to a template previously loaded into the reader. When there is a match, then a card number associated with the cardholder can be sent over the Wiegand interface.

5.H OSDP™ Extensibility

OSDP™ defines a basic set of messages, but it also allows for Extended Write Commands and Extended Read Replies, which are defined in a "Profile". One such profile is defined in the OSDP™ spec: Transparent smart card interface support.

As mentioned above, OSDP™ defines an encryption approach based on GlobalPlatform SCP [45]. However, other (as yet undefined) methods of encryption may be possible; that is, OSDP™ is extensible by providing a field within OSDP™ messages which indicates the

encryption method to use. The OSDP™ message format includes a Security Block Type (SEC_BLK_TYPE) field to signal the encryption approach to use.

Another way of extending OSDP™ is by use of the OSDP™_MFG command and OSDP™_MFGREP reply, which is a way of wrapping vendor-unique (proprietary) messages in an OSDP™ envelope. A configuration which works well with one pair of reader and control panel may not work as well if either the reader or control panel is replaced by one from another OSDP™ vendor. Care must be taken for example if OSDP™_MFG messages are needed for some capabilities.

Although it has been suggested [26] that OSDP™ supports remote firmware updates (e.g., pushing new firmware from a CP to a reader), that capability is not explicitly discussed in the OSDP™ specification.

6 SUMMARY

OSDP™ is not yet widely adopted in COTS products. At this time, OSDP™ is not explicitly prescribed for FIPS 201-2 or FICAM compliance, but there is some documentation [33] suggesting that a bi-directional interface, like that provided by OSDP™, is needed between a reader and control panel within a PACS. Vendors have been creative in extending the life of the legacy Wiegand interfaces, and it appears that a Wiegand interface from a reader to a control panel may be able to support some authentication mechanisms defined in FIPS 201-2. However, Wiegand alone, without additional interfaces, cannot support high or very high levels of assurance.

There is no evidence that OSDP™ was used within any of the end-to-end PACS which are approved on the GSA PACS APL v2, although some of those products may support OSDP™.

With the emphasis to implement HSPD-12, when funding becomes available for procurement of PACS, DOD acquisition documents will need to factor in the FICAM guidance. Adoption of OSDP™ in DOD PACS may depend on the availability of COTS products which support OSDP™ and have been approved by GSA for the PACS APL [65]. Currently, DOD procurements do not have to specify adherence to OSDP™ because it not currently specified as required within the FICAM Testing Program. The mention of OSDP™ in the FRTC is encouraging for adoption within FICAM products, and industry outreach is expected to increase. An update to the FICAM Roadmap and Implementation Guidance is in progress [49], and this may provide an opportunity to expand the references to OSDP™ within FICAM guidance.

Based on the market research conducted for preparation of this white paper, PACS vendors appear to use FICAM as a selling point more than OSDP™ (based on an informal survey of product data sheets, press releases, and related material available from web sites). SIA has been influential in the FICAM arena through its interaction with the Government Smart Card Inter-agency Advisor Board (IAB). Specifically, based on SIA feedback, the GSA FICAM/FIPS 201 Testing Program instituted a topology adoption process [35] to accommodate alternate (innovative) PACS architectures and products. Since all federal departments and agencies, including DOD, are under pressure to adopt stronger authentication through the use of FICAM/FIPS 201 technology, OSDP™ is more likely to be used if it is more clearly associated with FICAM guidance.

7 REFERENCE DOCUMENTS

[1] Security Industry Association, "Open Supervised Device Protocol", Version 2.1.5, September 2012, http://www.siaonline.org

[2] Wiegand Specification, SIA AC-01-1996.10 – Access Control - Wiegand

[3] Zac, Franken (Jan 31, 2008). "Physical Access Control Systems". Black Hat 2008 security conference. Washington DC: BlackHat.com. p. 11. Retrieved 2014-06-12. http://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/bh-dc-08-franken.pdf

[4] Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors, http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html, http://www.dhs.gov/homeland-security-presidential-directive-12

[5] Government Smart Card Interoperability Specification, Version 2.1, http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

[6] NIST Special Publication 800-96, "PIV Card to Reader Interoperability Guidelines", Spetember 2006, http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[7] NIST Special Publication 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)", November 2008, http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

[8] DMDC, Interoperability Layer Service (IoLS) System of Record Notice (SORN), http://dpclo.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/8143/dmdc-16-DOD.aspx

[9] Telecommunications Industry Association (TIA) and Electronic Industries Alliance (EIA), "Application Guidelines for TIA/EIA-485-A", Jan 2006, http://e2e.ti.com/cfs-file.ashx/__key/telligent-evolution-components-attachments/00-142-00-00-00-33-63-91/TSB_2D00_89_2D00_A.pdf

[10] Wikipedia contributors, "Wiegand interface," Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=Wiegand_interface&oldid=607599805 (accessed June 13, 2014).

[11] Wikipedia contributors, "Access control," Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=Access_control&oldid=612630885 (accessed June 13, 2014).

[12] NIST FIPS PUB 201-1, Change Notice 1, Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors", March 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[13] NIST FIPS PUB 201-2, Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors", August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[14] NIST Special Publication 800-63-2, "Electronic Authentication Guideline", August 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[15] Underwriters Labs, UL294, Scope statement for Access Control Systems Units, http://ulstandardsinfonet.ul.com/scopes/scopes.asp?fn=0294.html

[16] DMDC Card Technologies & Identity Solutions Division (CTIS), "DOD Implementation Guide for CAC Next Generation (NG)", Version 2.6, November 2006, http://www.cac.mil/docs/CAC_NG_Implementation_Guide_v2.6.pdf

[17] 110th Congress, Public Law 110–181, 28 January 2008, (Sec. 357, Sec. 1069), http://www.DOD.gov/DODgc/olc/docs/pl110-181.pdf

[18] General Council of the DOD , Legislative proposals as part of the National Defense Authorization Bill for Fiscal year 2009, 25 April 2009, http://www.DOD.mil/DODgc/olc/docs/25April2008Package.pdf

[19] DOD IG Report to Congress on Section 357 of the National Defense Authorization Act for Fiscal Year 2008, "Review of Physical Security of DOD Installations", Report No. D-2009-035, (Project No. D2008-D000LB-0159.000), January 14, 2009, http://www.DODig.mil/Audit/reports/fy09/09-035.pdf , http://www.dtic.mil/get-tr-doc/pdf?AD=ADA499348

[20] DOD IG Report No. D-2008-104, "DOD Implementation of Homeland Security Presidential Directive-12", June 23, 2008, http://www.DODig.mil/audit/reports/fy08/08-104.pdf

[21] DOD Directive, "DOD Personnel Identity Protection (PIP) Program ", http://www.dtic.mil/whs/directives/corres/pdf/100025p.pdf

[22] USD(I), DOD 5200.08-R, "Physical Security Program", 9 April 2007, Incorporating Change 1, 27 May 2009, http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf

[23] Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DOD Physical Access Control", 8 Dec 2009, Incorporating Change 4, 22 April 2014, http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-012.pdf

[24] Directive-type Memorandum (DTM) 13-005,"Deviations from the DOD Physical Security Program", 25 April 2013, Incorporating Change 1, 4 Nov 2013, http://www.dtic.mil/whs/directives/corres/pdf/DTM-13-005.pdf

[25] Directive-type Memorandum (DTM) 14-005 – "DOD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files", 22 April 2014, http://www.dtic.mil/whs/directives/corres/pdf/DTM14005_2014.pdf

[26] SIA, Rob Zivney, "OSDP™, A SIA PACS Specification with PIV Support", http://www.fips201.com/resources/audio/iab_0213/iab_022713_zivney.pdf

[27] HID Global, "iCLASS SE Configurator March 2013 Basic Models", http://www.hidglobal.com/node/15683

[28] HID Global White Paper, "Achieving a FIPS 201 Physical Access Control Solution", 2013-09-16, http://www.hidglobal.com/sites/hidglobal.com/files/resource_files/hid-ach-fips201-pac-solution-wp-en.pdf

[29] Physical Access Interagency Interoperability Working Group, "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems", (TIG SCEPACS), Version 2.3, 20 Dec 2005, http://www.idmanagement.gov/sites/default/files/documents/PACS.pdf

[30] Federal Chief Information Officers Council, "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance", Version 2.0, 2 Dec 2011, http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf

[31] GSA FICAM Testing Program, "Functional Requirements and Test Cases", Version 1.2.0, 23 October 2013, http://www.idmanagement.gov/sites/default/files/documents/Functional%20Requirements%20and%20Test%20Cases%20v1.2.0.pdf

[32] GSA FICAM Testing Program, PACS Topology Mapping Form (Based on FRTC v1.2.0), Version 1.2.0, 23 Oct 2013, http://www.idmanagement.gov/sites/default/files/documents/PACS%20Topology%20Mapping%20Form%20for%20FRTC%20v1.2.0_0.docx

[33] ICAMSC[20], "Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS)", Version 3.0, 26 March 2014, http://www.idmanagement.gov/sites/default/files/documents/Personal%20Identity%20Verification%20in%20Enterprise%20Physical%20Access%20Control%20Systems_v3_20140326.pdf

[34] PACS Topology 3-31-2014, http://idmanagement.gov/photo/pacs-topology-3-31-2014

[35] GSA FICAM Testing Program, PACS Topology Adoption Process Document, Version 1.0, 1 Aug 2013, http://idmanagement.gov/sites/default/files/documents/Topology%20Adoption%20Process%20v1.0_0.pdf

[36] Joint Base Lewis-McChord (JBLM) Automated Installation Entry (AIE), http://www.lewis-mcchord.army.mil/des/le_automated_access.htm

[37] NIST, National Strategy for Trusted Identities in Cyberspace, http://www.nist.gov/nstic/

[38] OMB Office of Information and Regulatory Affairs, Information Collection Review, Defense Biometric Identification System (DBIDS), OMB Control Number 0704-0455, http://www.reginfo.gov/public/do/PRAOMBHistory?ombControlNumber=0704-0455

[39] Security Industry Association, Physical Access Control Systems (PACS) in a Federal Identity, Credential, and Access Management (FICAM) Framework, April 2014,

[20] Identity, Credential, and Access Management Subcommittee (ICAMSC) of the Information Security and Identity Management Committee (ISIMC) under the authority of the Federal CIO Council

http://www.siaonline.org/SiteAssets/GovernmentRelations/SIA%20PACS-FICAM%20final.pdf

[40] Smart Card Alliance Physical Access Council, Wiegand message formats for Federal Agency Smart Credential Number (FASC-N), Aug 2008, http://www.smartcardalliance.org/resources/lib/PAC_Wiegand_Recommendation.pdf

[41] OMB M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors", 3 Feb 2011, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

[42] ICAMSC, PIV in E-PACS, 24 May 2012, Version 2.0.2, Earlier draft version of [33], https://max.omb.gov/community/download/attachments/609459355/DRAFT+-+PIV+in+EPACS_v2_0_2+%285-24-2012%29.pdf

[43] IPVM, "Wiegand vs OSDP™", 19 March 2014, http://ipvm.com/updates/2484

[44] HQ USAF/A7S, Non-Nuclear Intrusion Detection System (IDS) Equipment Approval, 29 Jan 2014, https://afsfmil.lackland.af.mil/sfxr-requirements.html

[45] GlobalPlatform, Secure Channel Protocol 03 – GlobalPlatform Card Specification v2.2 - Amendment D, Version 1.1, September 2009, http://www.globalplatform.org/specificationscard.asp

[46] GSA[21], "Enabling Strong Authentication with Personal Identification Verification Cards: Public Key Infrastructure (PKI) in Enterprise Physical Access Control Systems (E-PACS) Recommended Procurement Language for RFPs", Version 1.0.5, 4 Feb 2014, http://www.idmanagement.gov/sites/default/files/documents/Procurement%20Language%20v1%200%205.pdf

[47] FICAM Roadmap Update Forum, 16 June 2014, https://www.idmanagement.gov/sites/default/files/documents/FICAM%20Initiative_Roadmap%20Update%20Forum_20140616_0.pdf

[48] (deleted)

[49] GSA, Provisionally-Approved FICAM Testing Program PACS Topology Mapping Form (PACS 13.01), Version 1.3.0, 23 Oct 2013, http://www.idmanagement.gov/sites/default/files/documents/Provisionaly-Approved%20Topology%20Mapping%20Form%20%28PACS%2013.01%29%20v1.3.0.docx

[50] GSA, Provisionally-Approved FICAM Testing Program PACS Topology Mapping Form (PACS 13.02), Version 1.3.0, 16 May 2014, http://www.idmanagement.gov/sites/default/files/documents/Provisionaly-Approved%20Topology%20Mapping%20Form%20%28PACS%2013.02%29%20v0.1.0.docx

[51] (deleted)

[21] U. S. General Services Administration; Office of Government-wide Policy; Office of Information, Integrity, and Access; Identity Assurance & Trusted Access Division

[52] HID Global, iCLASS SE How to Order Guide, D00545, Release C.10, July 2014, http://www.hidglobal.com/sites/hidglobal.com/files/resource_files/d00545-c.10_iclass-se-htog-en.pdf

[53] HID Global, pivCLASS How to Order Guide, D00546, B.3, January 2014, http://www.hidglobal.com/sites/hidglobal.com/files/resource_files/d00546-b.3-pivclass-htog-en_2.pdf

[54] GSA, "FAQs FIPS 201 Evaluation Program for Physical Access Control Systems (PACS) ", 23 June 2014, https://www.idmanagement.gov/sites/default/files/documents/PACS%20Testing%20FAQ_20140623.docx

[55] SIA, Steven Van Till, "A Security Industry Association (SIA) Perspective on the Cost and Methods for Migrating PACS Systems to Use PIV and PKI as Relying Parties", 24 April 2013, http://www.fips201.com/resources/audio/iab_0413/iab_042413_till.pdf

[56] Federal Chief Information Officers (CIO) Council, Charter, Nov 2012, https://cio.gov/wp-content/uploads/downloads/2013/02/CIOCCharterNov2012Approved.pdf

[57] DODI 5200.08, "Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)", December 10, 2005, Incorporating Change 2, Effective April 8, 2014, http://www.dtic.mil/whs/directives/corres/pdf/520008_2005_ch2.pdf

[58] OMB M-14-04, "Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management", 18 Nov 2013, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

[59] Committee on National Security Systems Instruction (CNSSI) 1253, "Security Categorization And Control Selection For National Security Systems", 27 March 2014, https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[60] Deputy Secretary of Defense, "Department of Defense FISMA and Privacy Management Report Fiscal Year 2013", 2 Dec 2013, https://www.intelink.gov/go/3MLWJyD

[61] DOD IG, DODIG-2012-122, "DOD Should Procure Compliant Physical Access Control Systems to Reduce the Risk of Unauthorized Access", FOUO, 29 Aug 2012, http://www.DODig.mil/pubs/

[62] DOD IG, DODIG-2013-134, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks", FOUO, 16 Sep 2013, redacted version at http://www.DODig.mil/pubs/

[63] Gupta, Sarbari, "Cross-Agency Authentication using PIV Symmetric Keys", NIST Key Management Workshop, 9-10 June 2009, http://csrc.nist.gov/groups/ST/key_mgmt/documents/June09_Presentations/sarbari_gupta_KMWSJune09_SymmetricKeyMgmt_PIV.pdf

[64] OMB, Information Collection Review (ICR) Documents, Navy Enabler Framework, http://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201402-0703-002

[65] GSA, FICAM Testing Program, PACS Approved Products List (APL), Version 2, http://www.idmanagement.gov/pacs-apl-v2

[66] GSA, FICAM Testing Program, FICAM/FIPS 201 Approved Products List (APL), http://www.idmanagement.gov/approved-products-list

CLEARANCE REQUEST FOR PUBLIC RELEASE OF DEPARTMENT OF DEFENSE INFORMATION

(See Instructions on back.)

(This form is to be used in requesting review and clearance of DoD information proposed for public release in accordance with DoDD 5230.09.)

TO: *(See Note)* **Chief, Office of Security Review, 1155 Defense Pentagon, Washington, DC 20301-1155**

Note: Regular mail address shown above. For drop-off/next day delivery, use:
Room 12047, 1777 North Kent Street, Rosslyn, VA 22209-2133

1. DOCUMENT DESCRIPTION

a. TYPE	b. TITLE
Technical Doc	Open Supervised Device Protocol for DoD Applicability
c. PAGE COUNT	**d. SUBJECT AREA**
27	White Paper on a Security Industry Standard

2. AUTHOR/SPEAKER

a. NAME *(Last, First, Middle Initial)*	b. RANK	c. TITLE
SEIWG (acronym in block 6)	CIV	DoD Physical Security Enterprise Program working group
d. OFFICE		**e. AGENCY**
Deputy Assistant Secretary of Defense-Nuclear Matters		OSD

3. PRESENTATION/PUBLICATION DATA *(Date, Place, Event)*

Date: 60 days from date of submission

Place/Forum: http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwg.html (this is the proposed web site that is accessible by the public, where the technical document would be posted if approved for release)

CLEARED
For Open Publication

MAR 0 2 2015

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

4. POINT OF CONTACT

a. NAME *(Last, First, Middle Initial)*	b. TELEPHONE NO. *(Include Area Code)*
Rourk, Rodney, R.	843-218-4375

5. PRIOR COORDINATION

a. NAME *(Last, First, Middle Initial)*	b. OFFICE/AGENCY	c. TELEPHONE NO. *(Include Area Code)*
Gillis, Roderick E.	OASD(NCB/NM)	703 697-1124

6. REMARKS

Under the auspices of the Physical Security Enterprise & Analysis Group (PSEAG), the Security Equipment Integration Working Group (SEIWG) is a technical subcommittee comprised of joint service representatives that develop joint interoperability standards for Physical Security Equipment. The PSEAG/SEIWG sponsor, Office of Assistant Secretary of Defense for Nuclear, Chemical, and Biological Programs/Nuclear Matters (OASD-NM), seeks approval to change the distribution statement on the technical document listed in block 1b, which is a white paper that we believe can be released to the public, Distribution A.

7. RECOMMENDATION OF SUBMITTING OFFICE/AGENCY

a. THE ATTACHED MATERIAL HAS DEPARTMENT/OFFICE/AGENCY APPROVAL FOR PUBLIC RELEASE *(qualifications, if any, are indicated in Remarks section)* AND CLEARANCE FOR OPEN PUBLICATION IS RECOMMENDED UNDER PROVISIONS OF DODD 5230.09. I AM AUTHORIZED TO MAKE THIS RECOMMENDATION FOR RELEASE ON BEHALF OF:

Deputy Assistant Secretary of Defense for Nuclear Matters

b. CLEARANCE IS REQUESTED BY 20150228 *(YYYYMMDD).*

c. NAME *(Last, First, Middle Initial)*	d. TITLE
Gillis, Roderick, E.	Chairman, DoD PSEAG
e. OFFICE	**f. AGENCY**
Gillis, Roderick, E.	OSD
g. SIGNATURE	**h. DATE SIGNED** *(YYYYMMDD)*
Rodrick E Gillis	20150211

DD FORM 1910, JAN 2006 PREVIOUS EDITION MAY BE USED. Adobe Professional 8.0

IT-S-0639