



GE  
Security

# PACS FIPS 201 Compliance

A document summarizing FIPS 201 requirements and guidelines for physical access control systems and GE Security compliance status

December 2006





**Table of Contents**

1	Overview.....	3
2	GSA PIV Card Reader compliance.....	6
3	GE Security PACS Compliance.....	7



## 1 Overview

### 1.1 HSPD-12

On August 27, 2004 the President signed Homeland Security Presidential Directive 12 (HSPD-12), titled "Policy for a Common Identification Standard for Federal Employees and Contractors". This directive set requirements not only aimed at assuring physical security at federally controlled facilities, but also at securing electronic access to the Government's information systems. The requirements call for the creation of a new federal standard for electronic identity cards to be issued to all federal employees and contractors.

The National Institute of Standards and Technology (NIST) was assigned the lead role in developing and publishing this new standard for facilitating the envisioned goal of federal enterprise-wide credentialing with cross-agency interoperability.

### 1.2 FIPS 201 PIV

On February 25, 2005 NIST issued Federal Information Processing Standard 201 (FIPS 201), titled "Personal Identity Verification (PIV) of Federal Employees and Contractors". FIPS 201 has resulted in a two-stage PIV deployment with a series of currently evolving standards, technical specifications, and process guidelines that are directly aimed at PIV credentialing for both logical access control systems and physical access control systems (PACS).

FIPS 201 PIV-I (Proposed agency implementation by October 27, 2005) defines minimum process related requirements for personal identity proofing, registration, and credential issuance. PIV-I mandates separation of process roles: The PIV Registrar (Identity Proofing & Registration) and the PIV Issuer (Card Issuance & Maintenance). FIPS 201 mandates that PIV service providers be officially certified, although government funding for defining and implementing a certification process is not yet available. It is up to each government agency to self certify their specific implementation to NIST published criteria in FIPS 201 PIV-I.

FIPS 201 PIV-II (Proposed agency implementation by October 27, 2006) defines technical implementation guidance for proper support of PIV-I as well as completing federal enterprise-wide credentialing with cross-agency interoperability.

Technical implementation guidance for FIPS 201 PIV-II initially referenced The Government Smart Card Interoperability Specification v2.1 (NIST Interagency Report 6887-July 16,2003); later superseded by Technical Implementation Guidance for Smart Card Enabled Physical Access Control Systems v2.2 (Approved by the Government Smart Card Interagency Advisory Board, published-July 30, 2004).

In essence, the guidance stipulates that identity must be verified by rapid, two-factor electronic authentication – specifically, the infrastructure used must support credentials that contain both public key certificates and a PIN or password. To ensure interoperability amongst conforming agencies for both logical and physical access control applications, the Federal Agency Smart Credential (FASC) will be a single multi-technology credential compliant with contactless smart card (ISO 14443), contact smart card (ISO 7816) and magnetic stripe (ISO 7811) standards.



### 1.3 PACS Technical Implementation Guidance

The purpose of this guidance is to define specifications and standards required to enable agencies to procure and implement hardware and software for physical access control systems (PACS), with centralized guidelines that promote conformance to U.S. Government requirements such that these systems will:

1. Operate with the Federal Agency Smart Credential (FASC)
2. Facilitate cross-agency, federal enterprise interoperability
3. Allow existing legacy PACS to operate with FASC compatible card readers

Technical Implementation Guidance for Smart Card Enabled Physical Access Control Systems v2.2 states:

“ A range of assurance profiles – low, medium, and high – are associated with an extensible data model on FASC cards. These assurance profiles provide for increasing integrity of the transaction between the card and the reader, enabling assurance that a genuine card is present for the access request. Using the methods prescribed for each assurance profile a PACS can function for the intended purpose, at the adequate level of integrity and security warranted by the specific environment, and facilitate cross-agency interoperability across the population of FASC cardholders. Currently this guidance does not require nor preclude the use of additional authentication factors such as PIN and/or biometric input in conjunction with the FASC card applications. When the use of additional authentication factors is warranted by an application, this guidance recommends including these factors in the cryptographic operations. It should be noted that this guidance is not intended to stipulate or exclude any specific method of communication from the reader to the panel. This guidance recommends a minimum level of security and interoperability between a token, typically a FASC card, and reader. A principal consideration in this guidance is to permit the continued use of existing PACS infrastructure with minimal change, typically reader replacement. This guidance allows partial credential data to be transmitted from the reader to the panel in legacy system upgrades to simplify migration for using FASC cards.”

In this guidance, the FASC conforms to a standardized numbering scheme called the Federal Agency Smart Credential Number (FASC-N) to be used as the individual identifier for PACS applications and is the primary identification string on all government issued credentials.

PACS applications will receive and compare the output from a reader to determine if access will be granted. Access is granted based on both the successful authentication of the FASC (valid card to reader transaction) and authorization to enter the requested area (valid reader to PACS panel transaction). A reader to PACS panel transaction will consist of a FASC-N.



Although a complete FASC-N (card to reader transaction) is fully represented by 40 characters encoded as 200 bits (25 byte) and transmitted in Binary Coded Decimal (BCD); the FASC-N specific data components for PACS applications are extracted and processed (reader to PACS panel transaction) as a 16-digit physical access control unique identification number consisting of the following elements:

<u>FASC-N Field Name</u>	<u>Length BCD</u>
1. Agency Code	4 Digit
2. System Code	4 Digit
3. Credential number	6 Digit
4. Credential Series	1 Digit
5. Individual Credential issue	1 Digit

The stated compliance guidance for full PACS interoperability requires a minimum of fourteen digits consisting of Agency Code, System Code, and Credential Number when matching FASC-N to PACS enrolled cardholders. The combination of an Agency Code, System Code and Credential Number is a fully qualified number that is uniquely assigned to a single individual. This minimum is to insure uniqueness among all federally issued FASC cards. A fewer number of digits may be matched but uniqueness will not be guaranteed across all FASC cardholders.



## 2 GSA PIV Card Reader Compliance

In September 2006 NIST released SP 800-78, which set standards for PIV compliant access control card readers in accordance with GSA selecting to standardize on a 75-bit Wiegand output format. GSA updates its FIPS 201 Evaluation Program by documenting PIV Card Reader-CHUID specifications and test procedures for submission of product evaluation and approvals. GSA approved readers are listed on the approved products list.

### 2.1 PIV Card Reader Output Structure

The data format shall consist of two parity bits, Agency Code, System Code, and Credential Code elements of the FASC-N along with the Expiration Date (YYYYMMDD) from the CHUID. Each element shall be individually formatted as binary numbers and combined to form a 75-bit string.

<u>Data Element</u>	<u>Position</u>	<u>Length</u>
1. (P1) Even Parity	1	1
2. Agency Code	2-15	14
3. System Code	16-29	14
3. Credential Code	30-49	20
4. Expire Date	50-74	25
5. (P2) Odd Parity	75	1

The first parity bit (P1) is even and shall be calculated over the first 37 bits. The second parity bit (P2) is odd and shall be calculated over the last 36 bits.



## 3 GE Security PACS Compliance

### 3.1 FIPS 201 PIV-I Compliance

The following GE Security PACS platforms currently provide database integration capabilities to facilitate provisioning system integration with PIV card issuance and management systems or PIV service providers:

1. Diamond II v2.3 or later
2. SapphirePro v4.75 or later
3. Secure Perfect v6.11 or later
4. Picture Perfect 2.0 or later
5. Facility Commander Wnx

### 3.2 FIPS 201 PIV-II Compliance

#### 3.2.1 Diamond II

Software Requirements: Diamond II v2.3 or higher

Hardware Requirements: ACURS, ACU2X, ACU2XL, ACUVision, IKE, RREs currently support GSA Wiegand data format for FASC-N

Configuration Details: Wiegand data format set to read "System Code" and "Credential Number" as badge ID; Badge ID will be [System Code][Credential Number]

#### 3.2.2 SapphirePro

Software Requirements: SapphirePro v4.75 or higher

Hardware Requirements: ACURS, ACU2X, ACU2XL, ACUVision, IKE, RREs currently support GSA Wiegand data format for FASC-N

Configuration Details: Wiegand data format set to read "System Code" and "Credential Number" as badge ID; Badge ID will be [System Code][Credential Number]

#### 3.2.3 Secure Perfect

Software Requirements: Secure Perfect v6.1.1 or higher

Hardware Requirements: PXNplus CPU based M5, M2000 or M3000 controllers; If 8RP or M2000 are in use, then the Wiegand output from the reader needs to be formatted by a WIU-4, WIU-4 firmware version 1.07 or higher is required; If 2RP or 2SRP is in use then a switch setting can be used to identify 75-bit Wiegand data format is in use



Configuration Details: PXNplus badge formatting, Wiegand data format set to read "Agency Code", "System Code" and "Credential Number" as badge ID; Badge ID will be [Agency Code][System Code][Credential Number]

### 3.2.4 Picture Perfect

Software Requirements: Picture Perfect v2.0 or higher

Hardware Requirements: PXNplus CPU based M5, M2000 or M3000 controllers; If 8RP or M2000 are in use, then the Wiegand output from the reader needs to be formatted by a WIU-4, WIU-4 firmware version 1.07 or higher is required; If 2RP or 2SRP is in use then a switch setting can be used to identify 75-bit Wiegand data format is in use

Configuration Details: PXNplus badge formatting, Wiegand data format set to read "Agency Code", "System Code" and "Credential Number" as badge ID. Badge ID will be [Agency Code][System Code][Credential Number]

### 3.2.5 Facility Commander Wnx

Software Requirements: All Versions

Hardware Requirements: PXNplus CPU based M5, M2000 or M3000 controllers; If 8RP or M2000 are in use, then the Wiegand output from the reader needs to be formatted by a WIU-4, WIU-4 firmware version 1.07 or higher is required; If 2RP or 2SRP is in use then a switch setting can be used to identify 75-bit Wiegand data format is in use

Configuration details: PXNplus badge formatting, Wiegand data format set to read "Agency Code", "System Code" and "Credential Number" as badge ID. Badge ID will be [Agency Code][System Code][Credential Number]

### 3.2.6 GE Transition Series Readers

GE will release Model 600 Transition Series readers in Q1 2007. These readers will be able to read government issued FIPS 201 credentials and will be submitted to GSA for inclusion on the Approved Products List. The Model 600 readers will also read 125 kHz GE Proximity and HID Proximity credentials.