

Access Control and FIPS 201 regulations

A white paper for Security professionals



On August 27, 2004, the White House issued a directive for the creation of a new Federal standard for secure and reliable identification credentials to be issued by Federal agencies for their employees and contractors.

FIPS 201 is one result of this directive and Software House is committed to continuing support of our government customers in meeting these requirements.

From encryption standards to Cardholder Unique Identification, Software House understands the government's security criteria.

Enclosed is a summary of the FIPS-201 requirement and Software House's plans to meet them in its Fall release of C·CURE 800, a full year before the government's deadline.

SOFTWARE HOUSE

Table of Contents

Software House Overview	3
FIPS 201 Background	4
The Software House Answer to FIPS 201	7
Frequently Asked Questions	10

Software House Overview

Software House is a leading access control brand of Tyco International's Fire & Security Division. Since 1981, Software House has established itself in the security industry as an innovator by being the first company to apply sophisticated database management software to access control and security management systems. At a time when most security companies focused on selling hardware, Software House identified and developed a market niche for sophisticated software-based computerized solutions to manage and integrate diverse security hardware devices.

Today, Software House designs, markets and supports integrated security management systems, including its flagship products C·CURE® 800/8000 and the iSTAR™ Pro controller. Software House security solutions are currently installed in more than 5,500 installations worldwide, touching all vertical markets, including PetroChemical, Financial, Bio-Tech, Education, Communications, Homeland Security, Healthcare, and more.

Security-critical applications such as the U.S. Capitol, the Department of State, and the Smithsonian Institute have chosen the C·CURE 800 to address their security needs.

KEY SOFTWARE HOUSE STATISTICS

- Over 170 of the Fortune 500 Companies use C·CURE
- Leading provider of Enterprise Class access control systems
- Leading Access Control Brand Name per Freeman Reports
- C·CURE 800/8000 is the flagship platform
- Over 10,000 systems sold: 100,000 doors annually
- Over 5,000 customers, many with multiple systems

FIPS 201 Background

In August 27, 2004, the White House issued a Homeland Security Presidential Directive titled HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors". This directive called for the creation of a new Federal standard for secure and reliable identification credentials to be issued by Federal agencies for their employees and contractors. The National Institute of Standards (NIST) was assigned the lead role of creating and publishing this new standard.

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 and its associated Special Publications (still in draft mode) define specific requirements for the PIV card as well as for its issuance.

FIPS 201 consists of two parts which can be phased in sequentially:

- PIV-I describes the minimum requirements to meet the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. PIV-I does not call for interoperability of PIV credentials and systems nor does it compel the use of a particular credential technology. Each organization's credential issuing process must be accredited.
- PIV-II details the technical specs required to support PIV-I as well as interoperability among the Federal Agencies. It includes the policies and minimal requirements for interoperable PIV credentials for physical and logical access. The PIV-II credential will contain both a contactless chip and a contact chip containing the Cardholder Unique Identification (CHUID), PIN, biometric data, and encrypted keys required for Logical Access.

The Office of Management and Budget (OMB) is tasked with providing guidance to the Agencies on the implementation of HSPD-12. The OMB draft proposal calls for Agency implementation of PIV-I by October 27, 2005, and PIV-II by October 27, 2006.

PIV Card Issuance and Management

The requirements start with a PIV Card Issuance and Management System consisting of two major components, Identity Proofing & Registration, and Card Issuance & Maintenance. FIPS 201 mandates a separation of roles: the PIV Registrar and the PIV Issuer cannot be the same individual.

A Sponsor, usually the hiring party, will submit a request for credential. The Applicant then submits personal information, two photo ID's (source documents), photograph, and fingerprint biometrics. The Registrar verifies the individual matches the ID photos, submits the ID's for electronic verification if the issuer offers that capability, and submits a request for National Security Check. If all is satisfactory, the Registrar approves issuance.

Once the Issuer has received authorization, the Issuer verifies the National Security Check, requests a CHUID from the appropriate agency, requests the appropriate encryption keys from the PKI Certificate Authority and prints and programs the PIV card. In order for the Applicant to receive the card, the Applicant must present himself in person, submit picture ID and be further verified by checking that their fingerprint matches the biometric stored on the card.

Certification

FIPS 201 mandates that the PIV Service Providers be officially certified, but funding for defining and implementing the processes has not yet been procured. Until such time as NIST provides the certification framework, government agencies must self-certify their implementations. The framework defined in this document meets the certification criteria. However, it is up to each agency to certify each specific implementation.

PIV Card

The PIV card is described in great detail in FIPS 201 and its accompanying reference documents, but it is essentially a dual technology, contact and contactless, smart card. The critical data components required for Physical Access Control are the CHUID, the biometric template, PIN, and expiration date.

The Federal Agency Smart Credential Number, FASC-N, is a data record which is part of the CHUID structure. FASC-N consists of nine data fields, five of which, in combination, uniquely identify the cardholder. Those fields are listed below:

FASC-N Field Name	Length (Digits)
Agency Code	4
System Code	4
Credential Number	6
Credential Series	1
Individual Credential Issue	1

The Software House Answer to FIPS 201

C-CURE 800 v9.0 and iSTAR v.4.0 are on track to meet the PIV-II requirements of FIPS-201 in Fall of 2005, one year ahead of the deployment deadline.

Existing C-CURE and iSTAR installations covered by Software Support Agreements will be field upgradeable at no additional cost.

The attached diagram outlines the typical Software House PIV-II application which is briefly summarized in the following paragraphs.

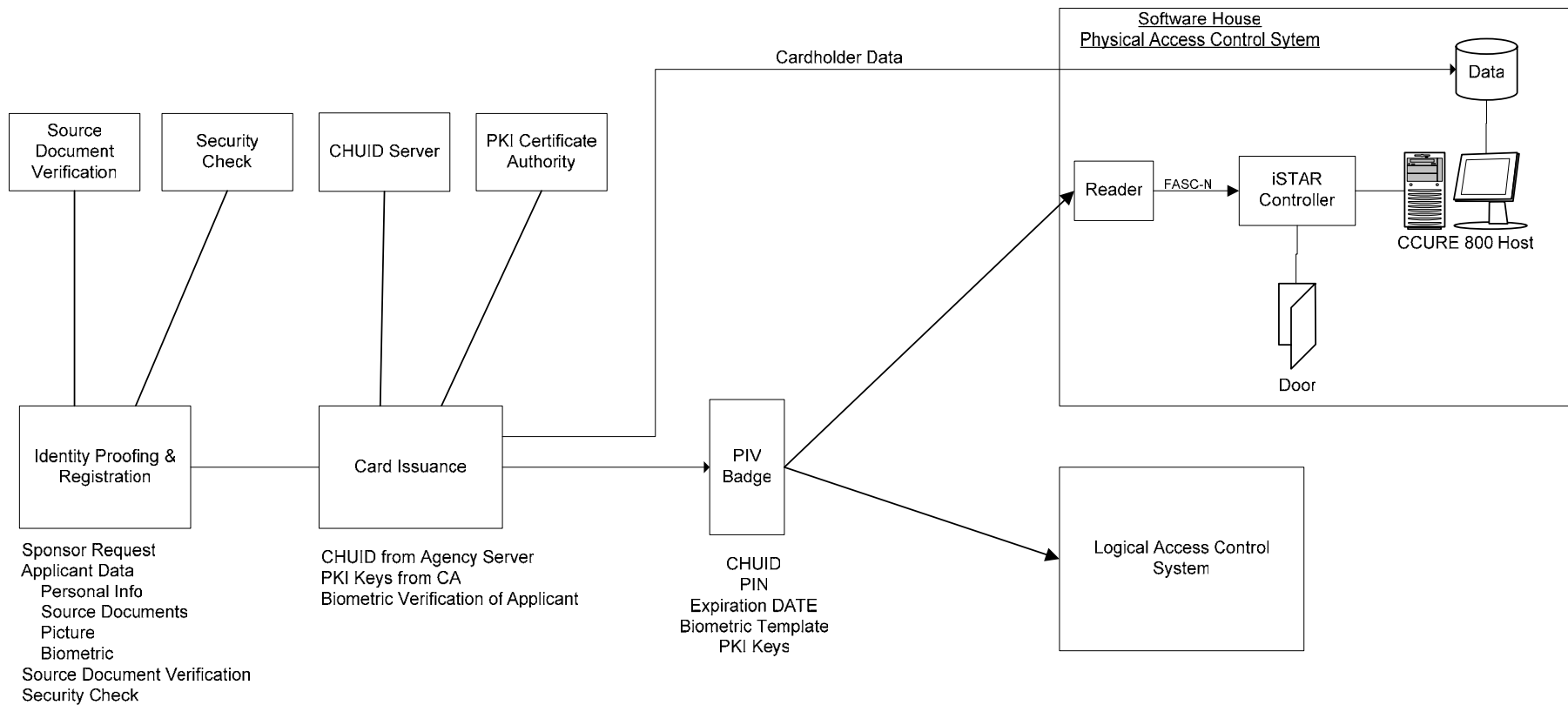
C-CURE 800 and iSTAR will support the FASC-N card format as noted below:

- Cardholder records will include the various FASC-N data elements
 - Cardholder records, including the FASC-N data, can be imported from PIV Card Issuance and Management System using the Auto Import feature.
- The cardholder record downloaded to the iSTAR controller will include specified FASC-N data elements.
- The iSTAR controller will be able to receive the FASC-N data via Wiegand interface from the reader.
- The data from the reader will be matched against the FASC-N data in the cardholder records in iSTAR.
- Cardholder FASC-N data elements will be included in the transaction record in the journal.
- The Hashed Message Authentication Code (HMAC) feature required in some Medium Security Profile applications will be supported.

A number of companies are providing readers that can read the PIV-II card and output FASC-N data via the Wiegand interface. Software House will include support for HID's FIPS-201 Readers, Integrated Engineering's ISO 14443-4 DESFire PIV-2 Readers, and compliant biometric readers. Additionally, we plan to evaluate and qualify, as required, additional readers from other vendors.

Integration to Software House's C-CURE System

C-CURE System's Cardholder Import functionality supports integration with third party PIV Card Issuance and Management Systems, including those provided by Goddard Technology and BearingPoint. Software House has a proven track record of Government and Transportation provisioning system integration with established providers in University, Transportation, and Government applications.



Software House FIPS-201 PIV-II System Model

Frequently Asked Questions

1. Are Software House solutions FIPS 201 compliant?

C-CURE 800 v9.0, coupled with iSTAR Pro v4.0 and badge readers from our partners is part of a FIPS 201 solution that includes a compliant Credentialing System which exports cardholder data to the C-CURE 800 system.

2. Do Software House solutions read FIPS 201 cards?

C-CURE 800 v9.0, coupled with iSTAR Pro v4.0 reads FASC-N and HMAC data from PIV readers, using the Wiegand interface.

3. Does Software House's existing C-CURE access control software support FIPS 201?

C-CURE 800's Auto Import utility imports cardholder records from the FIPS 201 Credentialing System. The FASC-N data in these records is matched to the FASC-N data from the readers to identify the cardholder and grant or reject access based on the cardholder's privileges.

4. Which readers do Software House support?

iSTAR Pro 4.0 will support FASC-N and HMAC data from PIV cards via the Wiegand interface. A number of companies are providing readers that can read the PIV-II card and output FASC-N data via the Wiegand interface. Software House will include support for HID's FIPS-201 Readers, Integrated Engineering's ISO 14443-4 DESFire PIV-2 Readers, and compliant biometric readers. Additionally, we plan to evaluate and qualify, as required, additional readers from other vendors.

5. Does Software House support the FASC-N Card Format

C-CURE 800 v9.0 and iSTAR v4.0 will support FASC-N. Cardholder data will include the FASC-N data fields and FASC-N data from the readers will be used to match the cardholder FASC-N as a means to identify the cardholder.

6. Which Credentialing Systems can Software House's C-CURE 800 interface to?

C-CURE 800 v9.0's Auto Import utility supports importing cardholder data, including FASC-N, from third party Card Issuance and Management System. BearingPoint and Goddard Technology are such system providers.

7. Is Software House meeting deadlines and commitments?

C-CURE 800 v9.0 and iSTAR Pro 4.0 will be available one year prior to the Oct 27, 2006 implementation deadline for PIV-II. C-CURE 800 v8.3, integrated with an approved Credentialing system, is compatible with the requirements of PIV-I and is currently available.

8. Does FIPS 201 compliance detract from other integration features?

C-CURE 800 v9.0 and iSTAR Pro 4.0 support for FIPS 201 builds on, and retains, existing capabilities. The only limitation will be that the apC controller will not support the FASC-N data format.

9. Can I migrate my existing Software House system to C-CURE 800 v9.0?

Existing C-CURE 800 and iSTAR customers under Service Support Agreement can upgrade their software at no additional cost.