IDEMIA PUBLIC SECURITY

The Power of PIV: Understanding FIPS 201 for Secure Credential Verification in Government and Beyond

Roland Fournier

About the Standards

1. FIPS 201 and PIV

Federal Information Processing Standard (FIPS) 201 is a standard for Personal Identity Verification (PIV) systems used by the U.S. federal government that was developed to secure access to government facilities and information systems. It provides a standard for PIV systems to meet the security requirements of Homeland Security Presidential Directive-12 (HSPD-12), provides a common identification standard for federal employees and contractors, and ensures interoperability between PIV systems of different federal agencies.

FIPS 201 defines the technical and operational requirements for PIV systems, ensuring robust authentication for varying security access levels, digital signatures, and data encryption.

Key areas covered by the standard include:

- **Identity Proofing and Issuance:** Specifies processes for verifying and issuing credentials.
- **System and Security Controls:** Details card elements, interfaces, and security measures.
- **Authentication Mechanisms:** Supports multiple levels of identity assurance.
- **Digital Signatures:** Enables signing of emails and documents to ensure authenticity and integrity, using a private key stored on the card.
- **Encryption:** Supports data encryption to protect sensitive information, typically through public-key cryptography.
- **Multi-Factor Authentication:** Combines something the user has (the card), knows (a PIN), and, optionally, is (biometrics) for enhanced security.
- **Interoperability:** Ensures compatibility across federal agencies and systems, adhering to standardized protocols like NIST SP 800-73.

U.S. federal departments and agencies are required to implement FIPS 201, and the National Institute of Standards and Technology (NIST) publishes FIPS standards after approval by the Secretary of Commerce, with the standards enforced through the FIPS 201 Evaluation Program, which tests and certifies products used in PIV credentialing systems.

FIPS 201 Evaluation Program

The Federal Information Processing Standard 201 (FIPS 201) Evaluation Program (also known as the FICAM Testing Program) tests and certifies services and commercial products used in PIV credentialing systems, physical access control systems (PACS), and public key infrastructures (PKIs).

The program evaluates products such as smart cards (secure elements) that are used in Personal Identity Verification (PIV), Personal Identity Verification – Interoperable (PIV-I), and Common Access Card (CAC) credentials. A validation certificate from the NIST Personal Identity Verification Program (NPIVP) details that the product being tested is listed in the PIV Card Application Validation list and is conformant as defined in NIST Special Publication 800-73.

2. FIPS 140-3

"FIPS 140-3" refers to the Federal Information Processing Standard Publication 140-3, a U.S. government standard outlining security requirements for cryptographic modules, essentially setting the bar for the design and implementation of secure encryption technologies used in federal systems. Compliance with FIPS 140-3 is a prerequisite for FIPS 201 ("PIV") certification.

This latest version of the standard, published March 22, 2019, primarily references the ISO/IEC 19790:2012 standard for its technical requirements, which means compliance requires adhering to the requirements outlined in that document.

FIPS 140-3 covers aspects like key management, physical security, and cryptographic algorithms. It defines different security levels (typically 1 to 4), with security requirements increasing depending on the sensitivity of the data being protected.

To be FIPS 140-3 compliant, cryptographic modules must undergo testing and validation by a Cryptographic and Security Testing Laboratory (CSTL) under the Cryptographic Module Validation Program (CMVP), a joint initiative between NIST and the Canadian Centre for Cyber Security. The CMVP reviews and validates submissions. Certified modules are essential for PIV-compliant smart cards and USB security keys.

A True PIV Product Is About Achieving PIV Certification

After all this rigorous security testing, the resulting smart card or USB security key authenticator products can legitimately claim to be "PIV certified."

In order to meet FIPS 201 standards and claim that your product is PIV certified, the following are therefore required:

1. The application/applet on the token needs to pass FIPS 201 validation and meet the standards laid out in HSPD-12, resulting in a validation certificate from the NIST Personal Identity Verification Program (NPIVP) detailing that the product being tested is listed in the PIV Card Application Validation list.
2. A validation certificate from the NIST Cryptographic Module Validation Program (CMVP) which validates cryptographic modules to the Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules: Cryptographic Module Validation Program | CSRC
3. Submission of the NPIVP Certificate plus the FIPS 140-3 CMVP Validation Certificate to the FIPS 201 Evaluation Program for review, resulting in a certification letter and the product being placed on the Approved Products List (APL).

Adoption of USB Security Keys

While the bedrock of FIPS 201-compliant (PIV) authenticators remains the PIV card, there is an increasing demand for USB security keys because of their versatility for logical access.

Moreover, as not all applications support PIV authentication, a browser-based authentication method like FIDO passkeys offers an appealing additional option. Any USB key authenticator would therefore do well to carry both types of credentials for maximum versatility.

Conclusion

Given the robustness of the PIV/FIPS 201 standard, it is understandable that government agencies and security-conscious large enterprises would seek out products that meet the PIV standards—and that vendors would be eager to meet the demand, claiming "PIV compliance." However, absent robust investment in research and development and the time and expense involved in achieving certification from NIST, buyers have no guarantee that the hardware tokens they are buying do, in fact, meet the standard, which may represent an unwanted risk.

Multiple vendors claim to support the FIPS 201 standard, but **only two have secure modules listed with active certification on the Approved Products List**, and IDEMIA is one of them. Its ID-One Key® product combines the security of a certified PIV authenticator with the convenience of the USB form factor, and, backed by IDEMIA's strong track record in government credentialing, offers a robust solution for authentication, encryption, and email signing.

In conclusion, when looking for a USB-based PIV solution, it is therefore important to look for the following:

- **Security Certifications:** Ensure that the selected smart card or USB security key is **FIPS 201-certified** for PIV applications, **NIST FIPS 140-3 certified**, and **FIDO2**

certified, ensuring it meets the rigorous security and compliance requirements necessary for government and high-security enterprise systems.

- **End-to-End FIPS 140-3 Compliance:** Unlike competitors that rely solely on third-party cryptographic modules, the IDEMIA ID-One Key® undergoes full evaluation of its cryptographic module, OS, and application together to meet FIPS 140-3 certification.
- **Multi-Modal Authentication:** The key supports both PIV *and* FIDO2 authentications, addressing the growing demand for versatile, high-assurance security solutions.
- **A Proven Track Record Providing Secure Credentials to Government:** With 25 years of leadership in the U.S. government market, IDEMIA also offers unparalleled expertise in secure credentialing to commercial enterprises.

Contact IDEMIA if you have any questions or would like to further explore this topic.