Draft NISTIR 7863

Cardholder Authentication for the PIV Digital Signature Key

W. Timothy Polk
Hildegard Ferraiolo
David Cooper

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 7863

Cardholder Authentication for the PIV Digital Signature Key

W. Timothy Polk
Hildegard Ferraiolo
David Cooper
Computer Security Division
Information Technology Laboratory

December 2013



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency Report 7863
9 pages (December 2013)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *December 13, 2013* through *January 17, 2014*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: piv_comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

FIPS 201-2 requires explicit user action by the Personal Identity Verification (PIV) cardholder as a condition for use of the digital signature key stored on the card. This document clarifies the requirement for explicit user action to encourage the development of compliant applications and middleware that use the digital signature key.

Keywords

personal identification number; personal identity verification; PIN caching; PIV

Table of Contents

1. INTRODUCTION 1

2. BACKGROUND 1

3. ARCHITECTURES 2

4. MINIMUM SECURITY OBJECTIVES & CONTROLS 2

4.1 Per-Transaction PIN Entry 2

4.2 Explicit User Action with PIN Caching 2

APPENDIX A— ACRONYMS 4

APPENDIX B— REFERENCES 4

1. Introduction

FIPS 201 defines the Personal Identity Verification (PIV) Card and supporting process requirements. A private cryptographic key, the digital signature key (DSK), is specified for digitally signing messages and data. The DSK is generated on the card and is never exported; all operations with this private key are performed by the PIV Card. FIPS 201 requires authentication of the cardholder via "explicit user action" each time the DSK is used to perform a cryptographic operation.

Special Publication 800-73 specifies the "PIN ALWAYS" access condition for the DSK to ensure that the PIN is submitted to the card for each requested cryptographic operation. However, FIPS 201 does not mandate the use of card readers with integrated PIN entry pads. As a result, the PIV Card itself cannot differentiate between a freshly supplied PIN and a PIN cached by the calling application or system.

This specification clarifies the requirement for "explicit user action" and specifies a range of implementation options that satisfy this requirement, in order to ensure a consistent and reliable level of security.

2. Background

The digital signature key (DSK) is intended to sign data, such as electronic forms, documents or electronic mail. Operations using the DSK can be performed after the PIV Card has been activated. To protect the DSK against misuse after activation, each subsequent private key operation requires an explicit user action.

The PIV Card incorporates a single mechanism for both authenticating the cardholder and expressing explicit user action: entry of the user PIN.[1] The user PIN must be presented to the PIV Card to activate the card for privileged operations or to perform a signing operation with the DSK. If the user is prompted for the PIN, and that value is presented to the PIV Card for each operation, the requirement for explicit user action is clearly satisfied. This ensures that the user is present and intended to generate a signature with the DSK each time a signature generation operation is performed. However, ensuring that the PIN is re-entered by the user for each signature operation requires system level controls outside the boundaries of the PIV Card.

In addition, for some applications it is considered impractical to require the cardholder to enter the PIN for each signature. For example, users may be required by policy to sign every email message. When the user is sending a large number of email messages in a short period, repeatedly entering the PIN greatly decreases usability. In such cases, the application or middleware can be designed to retain (or cache) the smart card PIN and present it on behalf of the user. However, caching the PIN may allow the application or middleware to present the PIN without the cardholder's knowledge.

The following sections identify possible architectures for systems that use the DSK, and define the minimum security objectives and controls that constitute *explicit user action* for the PIN ALWAYS access condition of the DSK.

[1] FIPS 201-2 introduces the option for PIV Cards to implement on-card fingerprint biometric comparison, in addition to the PIN, as a mechanism to authenticate the cardholder to the card, however, the recommendations in this document only apply to the PIN.

3. Architectures

There are two basic configurations for a PIV compliant system that leverages the DSK:

(1) A computing system can be designed so that the PIN is never exposed to the operating system, middleware, or applications. The components of this system are the host computer with an external smart card reader with keypad, and the PIV Card. In this case, the PIN is submitted from the user "directly" to the PIV Card. The application or operating system cannot cache the PIN so enforcing the PIN ALWAYS requirement is sufficient to confirm explicit user action for each DSK private key operation.

(2) A computing system can be designed so that the PIN is entered via the host computer's keyboard. The components of this system are the host computer system with an internal or external smart card reader without keypad, and the PIV Card. In this case, the PIN is entered into the keyboard and is processed by the operating system, middleware, or application before submission to the PIV Card.

In configuration (1), it is the external reader's responsibility to ensure that the PIN is supplied to the PIV Card as a result of an explicit action. In configuration (2), the host system software, in combination, has the responsibility to ensure that the PIN is supplied to the PIV Card as a result of an explicit action.

The following section specifies implementation guidelines for PIV system components.

4. Minimum Security Objectives & Controls

This section specifies minimum security controls and objectives for system implementations that leverage the DSK to ensure that each presentation of the PIN represents an explicit user action. Section 4.1 describes functional requirements for systems that prohibit PIN caching. Section 4.2 specifies the minimum security objectives and controls for system implementations that support DSK PIN caching.

4.1 Per-Transaction PIN Entry

Entering the PIN each time is the most direct and strongest mechanism to achieve *explicit user action* for the PIN ALWAYS access condition of the DSK. This can be achieved by any of the following methods:

(1) PIN entry is performed exclusively using an external card reader with key pad,[2] and the card reader itself does not cache the PIN; or

(2) PIN entry is performed using the host system, and the operating system, middleware, and all applications are configured so that the PIN is never cached.

In combination with the PIV Card's native controls, both solutions confirm user action for each DSK private key operation simply by enforcing the PIN ALWAYS requirement.

4.2 Explicit User Action with PIN Caching

If the PIN is cached by any component of the system, it is the system's responsibility to ensure an *explicit user action* occurs before the PIN is presented to the PIV Card. Examples of affirmative action could include clicking "OK" in a pop-up box or by user selection of an appropriate menu option or commit button within the application.

[2] Note that the card reader needs to intercept and discard any APDUs that contain the PIN originating from the host system.

PIN caching implementations for the DSK should ensure that the following are satisfied:

1. The PIN cache is limited to a single process or application instance. That is, a PIN presented by an email application to digitally sign email is not accessible to other applications resident on the host system, such as workflow or document signing applications.
2. The cached PIN is not presented to the smart card without an associated *explicit user action*. The explicit user action may be handled by either of the following methods:
    a. The component that confirms the *explicit user action* is the component that caches the PIN (e.g., the application or the middleware); or
    b. The programming interface between the component that confirms the *explicit user action* and the component that caches the PIN can convey the difference between a request associated with *explicit user action* and a request that was not associated with an *explicit user action*.
3. The PIN cache is cleared if any of the following conditions apply:
    a. The system is shut down or rebooted;
    b. The PIV Card is removed from the system;
    c. The associated process or application instance is terminated; or
    d. The PIN has not been presented to the PIV Card for more than *N* minutes. (In other words, no more than *N* minutes have passed since the user performed an explicit action authorizing a signature.) The value of *N* is an agency (or ICAMSC) decision but should not exceed thirty minutes.

Appendix A—Acronyms

APDU	Application Protocol Data Unit
DSK	Digital Signature Key
FIPS	Federal Information Processing Standard
ICAMSC	Identity, Credential, and Access Management Subcommittee
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
PIN	Personal Identification Number
PIV	Personal Identity Verification
SP	Special Publication

Appendix B—References

[FIPS201] Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) Federal Employees and Contractors*, August 2013.

[SP800-73] Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*.