ITL BULLETIN FOR AUGUST 2016

NIST UPDATES PERSONAL IDENTITY VERIFICATION (PIV) GUIDELINES

Hildegard Ferraiolo, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

NIST has recently expanded the flexibility and enhanced the security of Personal Identity Verification (PIV) credentials by updating the following guidelines:

- Special Publication (SP) 800-156, *Representation of PIV Chain-of-Trust for Import and Export*, provides details regarding the use of chain-of-trust for import and export among PIV Card issuers.
- SP 800-166, *Derived PIV Application and Data Model Test Guidelines*, supports the expanded use of Derived PIV Credentials, as described below.

These documents support Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which specifies the model for identity credentials that are hosted on a smart card (i.e., the PIV card) and/or on mobile devices (i.e., Derived PIV Credentials). FIPS 201 is an important standard since it defines the identity proofing, registration, and issuance requirements for issuing PIV credentials to federal government employees and contractors. It was established to fulfill Homeland Security Presidential Directive 12 (HSPD-12),[2] which called for a common identification standard to be adopted regarding the interoperable use of identity credentials for physical and logical access to federal government locations and systems.

Chain-of-Trust

When data is collected as part of PIV processes, such as during identity proofing, registration, and issuance, that data may be maintained in a chain-of-trust record. FIPS 201 explains that a PIV cardholder's "chain-of-trust is a sequence of related enrollment data records that are created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records." The chain-of-trust offers process efficiencies because, for example, it enables a PIV Card to be reissued (e.g., to replace a lost or

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.
[2] See HSPD-12.

damaged card) based on the most current chain-of-trust record of the cardholder. The ability to access and trust the previous records enables issuers to avoid having to repeat the registration process. Departments and agencies that implement a chain-of-trust will also be able to transfer the record to another agency or to a service provider, so that the receiving agency or service provider can use the record to issue a PIV Card rather than re-enroll an applicant. NIST SP 800-156 provides details regarding the use of chain-of-trust for import and export among PIV Card issuers.

Purpose and Scope

FIPS 201 describes three use cases for a chain-of-trust: 1) to extend enrollment; 2) to reissue a PIV Card; and 3) to transfer PIV Card enrollment records to another federal issuer or to a service provider. The purpose of NIST SP 800-156 is to provide the data representation of a chain-of-trust record for the transferal use case. To facilitate interoperable information sharing and data exchange, the data representation is based on an XML (Extensible Markup Language) schema. The sending and receiving federal agencies will be able to exchange the chain-of-trust data according to the specifications provided in this document. Similarly, a service provider will be able to receive chain-of-trust records from various client agencies, using the XML schema specified in NIST SP 800-156. NIST SP 800-156 also supports record data integrity through the use of digital signatures, and confidentiality through encryption of chain-of-trust data in transit and at rest.

There are two use cases within the transferal scenario which NIST SP 800-156 supports:

- **Agency to agency**: In this use case, an existing PIV cardholder from agency A is transferring to agency B, where they will require a new PIV Card issued by agency B. Rather than re-enrolling the user, the chain-of-trust record is sent, (upon Agency B's request) from agency A to agency B such that agency B is able to reuse the enrollment data to issue a PIV card, thus reducing the time and effort required for agency B to re-enroll the user.
- **Agency to service provider**: In this use case, an agency does not directly issue PIV Cards to their employees and contractors, but instead utilizes a separate service provider for issuance of PIV Cards. The agency can use the chain-of-trust to send PIV Card enrollment data collected by the agency to the service provider.

In each use case, the goal is to provide a common chain-of-trust schema that facilitates information sharing and data exchange between different issuers.

Chain-of-Trust Data Requirements and Namespaces

FIPS 201 recommends that the following data be included in the chain-of-trust:

- A log of activities that documents who took an action, what action was taken, when and where the action took place, and what identification data was collected;

- An enrollment data record that contains the most recent collection of each of the biometric data collected. The enrollment data record describes the circumstances of biometric acquisition including the name and role of the acquiring agent, the office and organization, time, place, and acquisition method. The enrollment data record may also document unavailable biometric data or failed attempts to collect biometric data. The enrollment data record may contain historical biometric data;
- The most recent unique identifiers (i.e., Federal Agency Smart Credential Number [FASC-N] and Universally Unique Identifier [UUID]) issued to the individual's card. The record may contain historical unique identifiers;
- Information about the authorizing entity who has approved the issuance of a credential;
- Current status of the background investigation, including the results of the investigation once completed;
- The evidence of authorization if the credential is issued under a pseudonym; and
- Data or any subsequent changes in the data about the cardholder. If the changed data is the cardholder's name, then the issuer should include the evidence of a formal name change.

NIST SP 800-156 provides an XML schema representation of the baseline data included in the chain-of-trust. This schema has been authored to address the broadest envisioned range of chain-of-trust data to be able to transfer PIV Card enrollment records across federal agencies and to a service provider. Users of this XML schema may extend the schema as needed, such as to allow the exchange of additional elements to meet specialized requirements for the exchange of chain-of-trust data. However, extending the XML schema will also result in custom exchange that is less interoperable.

Chain-of-Trust Schema

The chain-of-trust data is encoded in the XML format specified in NIST SP 800-156. The chain-of-trust XML records are intended to be used in a direct exchange. NIST SP 800-156 contains an overview of all elements that may appear in a chain-of-trust XML file.

The confidentiality of the chain-of-trust record is to be protected at all times by both the producing and consuming organizations. In addition to encrypting the chain-of-trust record in accordance with XML encryption, the chain-of-trust records should be encrypted in transit between the chain-of-trust producer and the chain-of-trust consumer. Some example mechanisms for chain-of-trust transmission include but are not limited to: FTPS, HTTPS secured web services, and out-of-band mechanisms such as S/MIME secure email. The encryption used shall be compliant with the FIPS 140[3] standard.

While log and historical data are not included in the XML chain-of-trust record, the issuer of the chain-of-trust record should be able to correlate the chain-of-trust record to the associated log and historic data, if requested to do so by the recipient of the chain-of-trust record. Logs and historical data are

[3] See FIPS 140-2.

maintained by the original issuer and are not transferred when exchanging PIV Card enrollment records. These log and historical data were created by the original issuer and are part of the chain-of-trust record. Log and historical data contain information that correlates the subject of a chain-of-trust record to logs of identity proofing, registration (enrollment) and maintenance activities of a cardholder. This includes information about the officer who took the action, what action was taken, and when and where the action occurred. Some examples of log activities maintained in the chain-of-trust record log are initial PIV Cardholder registration, enrollment, and issuance, change of name and subsequent reissuance, and loss of card and subsequent reissuance.

Derived PIV Applications and Data Model Test Guidelines

Originally, FIPS 201 required that all PIV credentials and associated keys be stored on the PIV Card. However, although using a PIV Card for electronic authentication works well with traditional desktop and laptop computers, it is not optimized for mobile devices.

In response to the growing use of mobile devices within the federal government, FIPS 201 was revised to permit the issuance of additional PIV credentials specifically for mobile devices. This PIV credential is called a Derived PIV Credential, for which the corresponding private key is stored in a cryptographic module within a mobile device. The use of this Derived PIV Credential is restricted to provide PIV-enabled authentication services on mobile devices in order to authenticate the credential holder to remote systems.

To support this expanded use of Derived PIV Credentials, NIST has published SP 800-166, *Derived PIV Application and Data Model Test Guidelines.* It provides test requirements and test assertions that can be used to validate conformance of the Derived PIV Application and the Derived PIV data model.

Because NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, was developed for meeting the interoperability goals of FIPS 201, the conformance test cases in NIST SP 800-166 increase assurance that the Derived PIV Application and associated derived PIV data objects that have passed these tests interoperate in federal applications.

Conclusion

Special Publications 800-156 and 800-166 support the HSPD-12 requirement for enhanced security, increased government efficiency, reduced identity fraud, and protection of personal privacy for federal employees and contractors. These documents also support the U.S. Digital Government Strategy[4] mandate to deliver better services to customers at a lower cost. Through improved efficiencies (e.g., the reduction of redundant background checks and identity proofing, secure exchange of interoperable

[4] See the U.S. Digital Government Strategy.

credential records, improved access to mobile derived PIV credentials), NIST helps to securely enable an increasingly mobile workforce.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov