NIST Special Publication 800-156

Representation of PIV Chain-of-Trust for Import and Export

Hildegard Ferraiolo
Ramaswamy Chandramouli
Ketan Mehta
Jason Mohler
Stephen Skordinski
Steven Brady

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-156

C O M P U T E R S E C U R I T Y

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

NIST Special Publication 800-156

Representation of PIV Chain-of-Trust for Import and Export

Hildegard Ferraiolo
Ramaswamy Chandramouli
Ketan Mehta
Computer Security Division
Information Technology Laboratory

Jason Mohler
Stephen Skordinski
Steven Brady
Electrosoft Services Inc.
Reston, VA

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-156

May 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-156
Natl. Inst. Stand. Technol. Spec. Publ. 800-156, 48pages (May 2016)
CODEN: NSPUE2

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-156

Comments on this publication may be submitted to:

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. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This document provides a common XML-based data representation of a chain-of-trust record to facilitate the exchange of Personal Identity Verification (PIV) Card enrollment data. The exchanged record is the basis to personalize a PIV Card for a transferred employee and also for service providers to personalize a PIV Card on behave of client federal agencies.

Keywords

enrollment record; Federal Information Processing Standards (FIPS) 201; HSPD-12; identification; identity infrastructure; Personal Identity Verification (PIV); PIV Architecture; PIV Card; PIV chain-of-trust; XML information sharing

Acknowledgement

The authors of SP 800-156 gratefully acknowledge and appreciate the support and contributions by many in the public and private sectors whose helpful and beneficial comments greatly enhance the utility of this publication. Special thanks to Stephen Sill and Matthew Arnold from the GSA HSPD-12 Managed Service Office (MSO) for their review and contributions to this document.

Table of Contents

List of Appendices

List of Tables

1 Introduction

1.1 Background

The Homeland Security Presidential Directive 12 [HSPD12] called for a common identification standard to be adopted governing the interoperable use of identity credentials to allow physical and logical access to federal government locations and systems. The Federal Information Processing Standard (FIPS) 201 [FIPS201], "Personal Identity Verification (PIV) of Federal Employees and Contractors," was developed as the standard for the identity credentials hosted on a smart card called the PIV Card. [FIPS201] defines the identity proofing, registration, and issuance requirements for issuing PIV Cards to Federal Government employees and contractors.

Data collected during identity proofing, registration, and issuance may be maintained in a chain-of-trust record. As per FIPS 201-2, "a card issuer may optionally maintain, for each PIV Card issued, a documentary chain-of-trust for the identification data it collects. The 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 a PIV Card can be re-issued based on the most current chain-of-trust record, and more importantly, can avoid having to repeat the identity proofing and re-registration (re-enrollment) 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. This Special Publication provides the representation of a chain-of-trust for import and export between PIV Card issuers.

1.2 Purpose and Scope

[FIPS201] describes three use cases for a chain-of-trust: 1) to extend enrollment, 2) to re-issue a PIV Card, and 3) to transfer PIV Card enrollment records to another federal issuer or to a service provider. The purpose of this document is to provide the data representation of a chain-of-trust record for the transferal use case. The data representation is based on a common XML (Extensible Markup Language) schema to facilitate interoperable information sharing and data exchange. 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 different client agencies that are based on a common XML schema specified in this document. This document also provides support for data integrity through digital signatures and for confidentiality through encryption of chain-of-trust data, in transit and at rest.

There are two use cases within the transferal scenario which this document supports:

Agency to agency: In this use case, an existing PIV cardholder from agency A is transferring to agency B, where he/she 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, thus reducing the time and effort required for agency B to issue a new PIV Card.

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.

It is anticipated that more optional elements will be populated in the chain-of-trust XML record for the agency to service provider use case than the agency to agency use case. In the agency to service provider exchange, the agency is likely to indicate several optional elements that are not applicable in the agency to agency use case. Examples of these elements include those that would be printed on a card and are provided by the agency to the service provider, such as <EmployeeAffiliation>, <AgencyDepartmentOrOrganization>, <AffiliationColorCode>, and <Rank>.

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

1.3 Document Structure

The remainder of this document is divided into the following sections and appendices:

- Section 2, *Chain-of-Trust Data Requirements and Namespaces*, discusses the representation of chain-of-trust data in XML schemas.
- Section 3, *Chain-of-Trust Schema Description*, documents the detail of chain-of-trust XML schema.
- Section 4, *Chain-of-trust Record Encryption in Transit*, identifies the requirements for encrypting chain-of-trust data.
- Section 5, *Log and Historical Data*, discusses the requirement for the chain-of-trust producer to maintain records related to the cardholder.
- Appendix A contains the XML schema for the chain-of-trust.
- Appendix B contains a sample XML chain-of-trust data record.
- Appendix C identifies references used in this document.
- Appendix D provides a glossary of terms used in this document.

- Appendix E provides a list of acronyms and abbreviations used in this document.

1.4 Document Conventions

Throughout this document key words are used to identify requirements. The key words "optional", "required", "shall", "shall not", and "should" are used. These words are a subset of the IETF Request For Comments (RFC) 2119 [RFC2119] key words, and have been chosen based on convention in other normative documents. In addition to the key words, the words 'need,' 'can,' and 'may' are used in this document, but are not intended to be normative.

2 Chain-of-Trust Data Requirements and Namespaces

[FIPS201] recommends that the following data be included in the chain-of-trust:

- A log of activities that documents who took the 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.
- Any 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.

The following sections provide 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. Extending the XML schema will allow the exchange of additional elements to meet requirements for specialized exchange of chain-of-trust data. However, extending the XML schema will also result in custom exchange that is less interoperable.

2.1 Namespaces Declaration for Chain-of-Trust Schema

XML namespace prefixes are used throughout this specification to stand for their respective namespaces as follows:

Table 1: Standard Namespace

Prefix	XML Namespace	Comments
ds:	`http://www.w3.org/2000/09/xmldsig#`	This is the W3C XML Signature namespace [XMLSig].
nist:	`http://csrc.nist.gov/ns/piv/chain-of-trust/1.0`	This is the NIST's Computer Security Division's chain-of-trust namespace.
xenc:	`http://www.w3.org/2001/04/xmlenc#`	This is the W3C XML Encryption namespace [XMLEnc].
xs:	`http://www.w3.org/2001/XMLSchema`	This is the schema for XML schemas namespace [XMLSchema].

The chain of trust schema defined in this document can be downloaded at http://csrc.nist.gov/schema/piv/chain-of-trust/piv-chain-of-trust-1.0.xsd.

This specification uses the following typographical conventions in the text: <Element>, **Defined Type**, `XML and XML schema`.

3 Chain-of-Trust Schema Description

The chain-of-trust data is encoded in the XML format specified in this document. The chain-of-trust XML records are intended to be used in a direct-exchange. 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. The <PIVTrustChain> element may include the records for multiple subjects, with each <EnrollmentRecord> element containing the record for a single subject.

This section contains an overview of the elements that may appear in a chain-of-trust XML file.

3.1 Schema Header and Namespace Declarations

The following schema fragment defines the XML namespaces and other header information for the PIV chain-of-trust schema:

```
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema"
       targetNamespace="http://csrc.nist.gov/ns/piv/chain-of-trust/1.0"
       xmlns="http://csrc.nist.gov/ns/piv/chain-of-trust/1.0"
       xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
       xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
       schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
       schema.xsd"/>
<xs:import namespace="http://www.w3.org/2001/04/xmlenc#"
       schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/>
```

3.2 Element <PIVChainOfTrust>

The following schema fragment defines the <PIVChainOfTrust> element:

```
<xs:element name="PIVChainOfTrust" type="PIVChainOfTrustType"/>
```

The <PIVChainOfTrust> element is of **PIVChainOfTrustType** complex type, and carries one or more <EnrollmentRecord> elements.

3.3 Complex Type PIVChainOfTrustType

The following schema fragment defines the **PIVChainOfTrustType** complex type:

```
<xs:complexType name="PIVChainOfTrustType">
  <xs:sequence>
    <xs:choice>
      <xs:sequence>
        <xs:element ref="xenc:EncryptedData" minOccurs="1" maxOccurs="1"/>
        <xs:element ref="xenc:EncryptedKey" minOccurs="1" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:sequence>
        <xs:element name="EnrollmentRecord" type="EnrollmentRecordType" minOccurs="1"
       maxOccurs="unbounded"/>
        <xs:element ref="ds:Signature" minOccurs="1" maxOccurs="1"/>
      </xs:sequence>
    </xs:choice>
  </xs:sequence>
```

```
</xs:complexType>
```

The **PIVChainOfTrustType** complex type offers a choice to either encrypt the PIV chain-of-trust records, or to leave the record unencrypted. PIV chain-of-trust records contain personally identifiable information (PII) of actual PIV cardholders and thus shall always be encrypted when in transit. The unencrypted sequence is intended to allow a recipient of the record to validate/test XML records as required. The recipient of the record should protect the records accordingly when not in use (i.e., data at rest protection).

Each instance of the <EnrollmentRecord> element contains the enrollment information captured by the PIV issuer for a single PIV cardholder. There is a minimum of one instance of this element, and there is no limit to the maximum number of <EnrollmentRecord> elements that may be contained in the <PIVChainOfTrust> element. This allows a single instance of the <PIVChainOfTrust> element to contain several PIV cardholder records in an XML file.

Encrypted PIV chain-of-trust records are intended to include a confidentiality protection mechanism. The encrypted content and associated encryption details are defined by the XML Encryption Syntax and Processing specification [XMLEnc]. The <EncryptedData> Type attribute should be present and contain a value of http://www.w3.org/2001/04/xmlenc#Element. The encryption method algorithm for the <EncryptedData> element should be set to: http://www.w3.org/2001/04/xmlenc#aes256-cbc.

The <xenc:EncryptedKey> element is defined in the [XMLEnc] standard and used to transport encrypted symmetric keys from the originator to a known recipient(s). The symmetric key value is always encrypted to the recipient(s). A public key from a PKI certificate should be used to encrypt the symmetric key. The sender should select an encryption certificate for the recipient issued under a policy that has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level. The sender should use http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p as the key transport algorithm to encrypt the key. Each encrypted key should include a Recipient attribute that contains a hint as to which recipient the encrypted key value is intended for. An example value that could be used in the Recipient attribute is the distinguished name (DN) from the recipient's encryption certificate subject field.

A procedure for the exchange of the key encryption key is outside the scope of this document. Some example mechanisms for this exchange include the use of Secure/Multipurpose Internet Mail Extensions (S/MIME) email exchanges to share the encryption certificates, or a webpage that supports Hyper Text Transfer Protocol with Secure Sockets Layer (HTTPS) using an FPKI SSL certificate or an Extended Validation Secure Sockets Layer (EVSSL) certificate, where links to the encryption certificates for recipient federal agencies or service providers can be accessed and downloaded.

All PIV chain-of-trust records are signed using XML Signature. An XML Signature protects the integrity of the data and authenticates the issuer of the chain-of-trust. A valid

PIV Card or a private key generated under the id-fpki-common-piv-contentSigning certificate policy should be used to sign the XML record.

3.4 Complex Type EnrollmentRecordType

The following schema fragment defines the **EnrollmentRecordType** complex type:

```
<xs:complexType name="EnrollmentRecordType">
  <xs:sequence>
    <xs:element name="PersonalInformation" type="PersonalInformationType" minOccurs="1"
       maxOccurs="1"/>
    <xs:element name="AdjudicationInformation" type="AdjudicationInformationType" minOccurs="1"
       maxOccurs="1"/>
    <xs:element name="EnrollmentPackage" type="EnrollmentPackageType" minOccurs="1"
       maxOccurs="1"/>
    <xs:element name="PIVCardTopography" type="PIVCardTopographyType" minOccurs="0"
       maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

The **EnrollmentRecordType** complex type contains four elements carrying data required for the issuance of a PIV Card to the cardholder. The elements contained in the **EnrollmentRecordType** complex type are:

<PersonalInformation>:
: This element is an instance of the **PersonalInformationType** complex type and contains personally identifying information on the subject of the chain-of-trust enrollment record. The <PersonalInformation> element is a required element that appears once in the **EnrollmentRecordType** complex type.

<AdjudicationInformation>:
: This element is an instance of the **AdjudicationInformationType** complex type and contains information on the status of the background investigation into the subject of the chain-of-trust enrollment record. The <AdjudicationInformation> element is a required element that appears once in the **EnrollmentRecordType** complex type.

<EnrollmentPackage>:
: This element is an instance of the **EnrollmentPackageType** complex type and contains biographic and biometric information on the subject of the chain-of-trust enrollment record. The <EnrollmentPackage> element is a required element that appears once in the **EnrollmentPackageType** complex type.

<PIVCardTopography>:
: This element is an instance of the **PIVCardTopographyType** complex type and contains information used for the physical printing of PIV Cards. The <PIVCardTopography> element is an optional element. If used, it would appear once in the **EnrollmentRecordType** complex type.

The **EnrollmentRecordType** for an agency to agency record exchange use case would typically include the following types:

- **PersonalInformationType**
- **AdjudicationInformationType**
- **EnrollmentPackageType**

The **EnrollmentRecordType** for an agency to service provider record exchange use case would typically include the following types:

- **PersonalInformationType**
- **AdjudicationInformationType**
- **EnrollmentPackageType**
- **PIVCardTopographyType**

As indicated above, the PIVCardTopographyType data element is more likely to be included in the service provider record exchange use case rather than the agency to agency record exchange use case. This is because a client agency needs to provide information about its agency and its new employees/contractors to be printed on the surface of each card. For the agency to agency record exchange, topographic information may not be needed as the receiving agency will use its own topographic elements when printing on the PIV Card.

3.5 Complex Type PersonalInformationType

The following schema fragment defines the **PersonalInformationType** complex type:

```
<xs:complexType name="PersonalInformationType">
  <xs:sequence>
    <xs:element name="PrimaryIdentifier" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SecondaryIdentifier" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PrintedName" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SSN" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="IsUSCitizen" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CitizenshipCountryCode" type="xs:string" minOccurs="1"
       maxOccurs="unbounded"/>
    <xs:element name="CardHolderUUID" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CardUUID" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CHUID" type="xs:string" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

The CardUUID and CHUID type data element generally is not included in the agency to agency record exchange use case as the new agency will generate these values. For the agency to servicer provider record exchange, however, the client agency may wish to specify the CardUUID and CHUID for each PIV cardholder.

The **PersonalInformationType** complex type contains eight elements that describe the subject of the chain-of-trust enrollment record. Those elements are:

<PrimaryIdentifier>:

This element contains the Primary Identifier of the subject of the chain-of-trust enrollment record. The Primary Identifier is defined in [FIPS201] as the surnames or family names of the PIV cardholder. The <PrimaryIdentifier> element is always included in the **PersonalInformationType** complex type

and appears only once. The data is provided in an xs:string format.

<SecondaryIdentifier>:
This element contains the Secondary Identifier of the subject of the chain-of-trust enrollment record. The Secondary Identifier is defined in [FIPS201] as pre-names or given names of the PIV Cardholder. The <SecondaryIdentifier> element is always included in the **PersonalInformationType** complex type and occurs only once. The data is provided in an xs:string format.

<PrintedName>:
This element contains the Printed Name of the subject of the chain-of-trust enrollment record. The Printed Name is a combination of the card holder's primary and secondary identifiers, as it is to be printed on the PIV Card according to [FIPS201]. The <PrintedName> element is always included in the **PersonalInformationType** complex type and only occurs once. The data is provided in an xs:string format.

<SSN>:
This element may contain the Social Security Number of the subject of the chain-of-trust enrollment record.[1] The <SSN> element is optional, and may occur only once if included in the **PersonalInformationType** complex type. The data is provided in an xs:string format.

<IsUSCitizen>:
This element is required, occurs once in the **PersonalInformationType** complex type and contains a boolean value. If the subject of the chain-of-trust enrollment record is a U.S. Citizen, then the value is set to true. If the subject of the chain-of-trust enrollment record is not a U.S. Citizen, then the value is set to false. The data is provided in an xs:boolean format. If the <IsUSCitizen> element is false, then at least one country is specified in <CitizenshipCountryCode>.

<CitizenshipCountryCode>:
This element is required if <IsUSCitizen> is set to false and optional if <IsUSCitizen> is set to true. The element contains the countries of citizenship of the subject of the chain-of-trust enrollment record. The country code is formatted in an abbreviation (alpha-3 format), as documented in [ISO3166]. The <CitizenshipCountryCode> element may occur once for each citizenship the applicant possesses. The data is provided in an xs:string format.

[1] To eliminate unnecessary use of the SSN, whenever possible, departments and agencies should avoid using the <SSN> element. See the attachment to OMB M-07-16 [M-07-16], Section 2: "Reduce the Use of Social Security Numbers."

<CardHolderUUID>:

The <CardHolderUUID > element is optional, and occurs once when included in the **PersonalInformationType** complex type. The Cardholder UUID is is a persistent identifier for the cardholder. The data is provided in an xs:string format. <CardHolderUUID> can be used by Agency B to request record from Agency A. The user then re-connects with the record via a biometric match.

<CardUUID>:

The <CardUUID > element is optional, and occurs once when included in the **PersonalInformationType** complex type. It is envisioned that the <CardUUID> will be used only in the agency to service provider record exchange use case to transfer the Card UUID to be stored on the PIV Card. The data is provided in an xs:string format. <CardUUID> can be used by Agency B to request a record from Agency A. The user then re-connects with the record via a biometric match.

<CHUID>:

This element is optional and if used should occur once when included in the **PersonalInformationType** complex type. It is envisioned that the <CHUID> will be used only in the agency to service provider use case to transfer the CHUID-specific details to be stored on the PIV Card. The data is provided in an xs:string format. <CHUID>'s FASC-N can be used by Agency B to request a record from Agency A. The user then re-connects with the record via a biometric match.

3.6 Complex Type AdjudicationInformationType

The following schema fragment defines the **AdjudicationInformationType** complex type:

```
<xs:complexType name="AdjudicationInformationType">
  <xs:sequence>
    <xs:element name="NACIAdjudicationValue" minOccurs="1" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Approved"/>
          <xs:enumeration value="Pending"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="NACIAdjudicationEffDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

The **AdjudicationInformationType** complex type contains two elements that describe the status of the PIV background investigation of the subject of the chain-of-trust enrollment record. Those elements are:

<NACIAdjudicationValue>:

This element is required, and occurs once in the **AdjudicationInformationType** complex type. The element indicates the status of the National Agency Check with Inquiries (NACI) (or equivalent or

higher) or Tier 1 or higher federal background investigation the PIV cardholder underwent. There are two permitted values based on the progress of the background investigation. The element is set to 'Approved' or 'Pending.' 'Approved' indicates a NACI (or equivalent or higher) or Tier 1 or higher federal background investigation has been completed. 'Pending' status indicates the Federal Bureau of Investigation (FBI) National Criminal History Check (NCHC) portion of the background investigation is completed and that NACI background check is in process, but has not yet received final adjudication. The data is provided in an xs:string format.

<NACIAdjudicationEffDate>:

This element is optional, and occurs once when included in the **AdjudicationInformationType** complex type. The element indicates the date the current status of the <NACIAdjudicationValue> element went into effect. The data is provided in an xs:date format.

3.7 Complex Type EnrollmentPackageType

The following schema fragment defines the **EnrollmentPackageType** complex type:

```
<xs:complexType name="EnrollmentPackageType">
  <xs:sequence>
    <xs:element name="EPBiographic" type="EPBiographicType" minOccurs="0" maxOccurs="1"/>
    <xs:element name="EPBiometrics" type="EPBiometricsType" minOccurs="1" maxOccurs="1"/>
    <xs:element name="EPDocument" type="EPDocumentType" minOccurs="2" maxOccurs="2"/>
  </xs:sequence>
</xs:complexType>
```

The **EnrollmentPackageType** complex type contains three elements that identify the biographic and biometric properties of a PIV cardholder. The elements contained in the **EnrollmentPackageType** complex type are:

<EPBiographic>:

This element is an instance of the **EPBiographicType** complex type, containing biographic information on the subject of the chain-of-trust enrollment record as described in Section 3.8. The <EPBiographic> element is an optional element and if present, appears once in the **EnrollmentPackageType** complex type.

<EPBiometrics>:

This element is an instance of the **EPBiometricsType** complex type, containing biometric information on the subject of the chain-of-trust enrollment record as described in Section 3.9. The < EPBiometrics> element is a required element that appears once in the **EnrollmentPackageType** complex type.

<EPDocument>:

This element is an instance of the **EPDocumentType** complex type as described in Section 3.10. The <EPDocument > element is a mandatory element and appears twice in the **EnrollmentPackageType** complex type.

One instance of the <EPDocument> element contains the primary identity source document as defined in [FIPS201]. The second instance of the <EPDocument> element complex type contains the secondary identity source document as defined in [FIPS201].

3.8 Complex Type EPBiographicType

The following schema fragment defines the **EPBiographicType** complex type:

```
<xs:complexType name="EPBiographicType">
  <xs:sequence>
    <xs:element name="GenderCode" minOccurs="0" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Female"/>
          <xs:enumeration value="Male"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="EyeColorCode" minOccurs="0" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Blue"/>
          <xs:enumeration value="Brown"/>
          <xs:enumeration value="Gray"/>
          <xs:enumeration value="Green"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="HairColorCode" minOccurs="0" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Bald"/>
          <xs:enumeration value="Black"/>
          <xs:enumeration value="Blonde"/>
          <xs:enumeration value="Brown"/>
          <xs:enumeration value="Gray or Partially Gray"/>
          <xs:enumeration value="Red or Auburn"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="Height" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Weight" type="xs:integer" minOccurs="0" maxOccurs="1"/>
    <xs:element name="EthnicityCode" minOccurs="0" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="A"/>
          <xs:enumeration value="B"/>
          <xs:enumeration value="I"/>
          <xs:enumeration value="U"/>
          <xs:enumeration value="W"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="EnrollmentDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

The **EPBiographicType** complex type contains six optional elements that describe the biographical data of the subject of the chain-of-trust enrollment record. Values for EPBiographicType complex type are based on the FBI's Electronic Biometric Transmission specification [EBTS]. Those elements are:

<GenderCode>:

This element contains the gender of the subject of the chain-of-trust enrollment record. The <GenderCode> element is optional and occurs once when included in the **EPBioGraphicType** complex type. The <GenderCode> element is set to Female or Male. The data is provided in an xs:string format.

<EyeColorCode>:

This element contains the eye color of the subject of the chain-of-trust enrollment record. The <EyeColorCode> element is optional and occurs once when included in the **EPBioGraphicType** complex type. The <EyeColorCode> element is selected from the following values: Blue, Brown, Gray or Green. The data is provided in an xs:string format.

<HairColorCode>:

This element contains the hair color of the subject of the chain-of-trust enrollment record. The <HairColorCode> element is optional and occurs once when included in the **EPBioGraphicType** complex type. The <HairColorCode> element is selected from the following values: Bald, Black, Blonde, Brown, Gray or Partially Gray, Red or Auburn. The data is provided in an xs:string format.

<Height>:

This element contains the physical height of the subject of the chain-of-trust enrollment record. If reported in feet and inches, the first (leftmost) digit is used to show feet while the two rightmost digits are used to show the inches between 00 and 11. If reported in inches, then the leftmost character is 'N' followed by two digits. The <Height> element is optional and occurs once when included in the **EPBioGraphicType** complex type. The data is provided in an xs:string format.

<Weight:>:

This element contains the physical weight of the subject of the chain-of-trust enrollment record. The subject's weight in pounds is entered. All weights in excess of 499 pounds will be set to 499. The <Weight> element is optional and occurs once when included in the **EPBioGraphicType** complex type. The data is provided in an xs:string format.

<EthnicityCode>:

This element contains the ethnicity of the subject of the chain-of-trust enrollment record. The <EthnicityCode> element is optional and occurs once when included in the **EPBioGraphicType** complex type. The <EthnicityCode> element is selected from the following values: A, B, I, U, or W.

Table 2: Ethnicity Codes

If Subject Is	Enter Code
Chinese, Japanese, Filipino, Korean, Polynesian, Indian, Indonesian, Asian Indian, Samoan, or any other Pacific Islander	A
A person having origins in any of the black racial groups of Africa	B
American Indian, Eskimo, or Alaskan native, or a person having origins in any of the 48 contiguous states of the United States or Alaska who maintains cultural identification through tribal affiliation or community recognition	I
Of indeterminable race	U
Caucasian, Mexican, Puerto Rican, Cuban, Central or South American, or other Spanish culture or origin, Regardless of race	W

<EnrollmentDate>:

This element contains the date the subject of the chain-of-trust enrollment record enrolled for a PIV Card. The <EnrollmentDate> element is optional and occurs once when included in the **EPBioGraphicType** complex type. The data is provided in an xs:date format.

3.9 Complex Type EPBiometricsType

The following schema fragment defines the **EPBiometricsType** complex type:

```
<xs:complexType name="EPBiometricsType">
  <xs:sequence>
    <xs:element name="Photo" type="xs:base64Binary" minOccurs="1" maxOccurs="1"/>
    <xs:element name="FingerprintOffCardComparisonRepresentation" type="xs:base64Binary"
       minOccurs="1" maxOccurs="1" />
    <xs:element name="FingerprintOnCardComparisonRepresentation" type="xs:base64Binary"
       minOccurs="0" maxOccurs="1"/>
    <xs:element name="IrisRepresentation" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

The **EPBiometrics** complex type contains information related to the biometric data of the subject of the chain-of-trust enrollment record, as captured during PIV enrollment including the primary and secondary fingerprint representation. The four elements supported in the **EPBiometrics** complex type are:

<Photo>:

This element is required. The <Photo> element contains the facial image collected during the enrollment process, as documented in [SP800-76] Biometric Specifications for Personal Identity Verification. The <Photo> element includes the CBEFF Header, the INCITS 385 profile for PIV facial images, and the CBEFF signature. The facial image is used to both print the image on the card and as the digital representation stored in the PIV Card. The data is provided in an xs:base64Binary format.

<FingerprintsOffCardComparisonRepresentation>:

This element is mandatory and occurs only once. The <FingerprintsOffCardComparisonRepresentation> element contains the fingerprint data collected during the enrollment process and is used for off-card comparison, as documented in [SP800-76]. The <FingerprintsOffCardComparisonRepresentation> element includes the CBEFF Header, the INCITS 378 Minutiae, and the CBEFF signature. The data is provided in an xs:base64Binary format.

<FingerprintsOnCardComparisonRepresentation>:

This element is optional and if used occurs once. <FingerprintsOnCardComparisonRepresentation> element is only used if the <FingerprintsOnCardComparisonRepresentation> element uses different fingers representation than in <FingerprintsOffCardComparisonRepresentation> element. If the fingers for on-card and off-card comparison representation are identical, on-card comparison minutia templates representation can be created using the data stored in the <FingerprintsOffCardComparsionRepresentation> element. If used, the <FingerprintsOnCardComparisonRepresentation> includes the CBEFF Header, the ISO/IEC 19794-2:2011 minutiae, and the CBEFF signature, as documented in [SP800-76]. The data is provided in an xs:base64Binary format.

<IrisRepresentation>:

This element is optional and if used occurs once. The <IrisRepresentation> element contains the iris image representation collected during the enrollment process, as documented in [SP800-76]. The <IrisRepresentation> element includes the CBEFF Header, ISO 19794-6 iris, and the CBEFF signature. The data is provided in an xs:base64Binary format.

3.10 Complex Type EPDocumentType

The following schema fragment defines the **EPDocumentType** complex type:

```
<xs:complexType name="EPDocumentType">
  <xs:sequence>
    <xs:element name="DocumentTypeIdentifier" minOccurs="1" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Primary identity source"/>
          <xs:enumeration value="Secondary identity source"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="DocumentTypeCode" minOccurs="1" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="U.S. Passport or a U.S. Passport Card"/>
          <xs:enumeration value="Permanent Resident Card or an Alien Registration Receipt Card
       (Form I-551)"/>
          <xs:enumeration value="Foreign Passport"/>
          <xs:enumeration value="Employment Authorization Document that contains a photograph
       (Form I-766)"/>
          <xs:enumeration value="Driver's license or an ID card issued by a state or possession of
```

```
      the United States provided it contains a photograph"/>
         <xs:enumeration value="U.S. Military ID card"/>
         <xs:enumeration value="U.S. Military dependent's ID card"/>
         <xs:enumeration value="PIV Card"/>
         <xs:enumeration value="U.S. Social Security Card issued by the Social Security
      Administration"/>
         <xs:enumeration value="Original or certified copy of a birth certificate issued by a
      state, county, municipal authority, possession, or outlying possession of the United States
      bearing an official seal"/>
         <xs:enumeration value="ID card issued by a federal, state, or local government agency or
      entity, provided it contains a photograph"/>
         <xs:enumeration value="Voter's registration card"/>
         <xs:enumeration value="U.S. Coast Guard Merchant Mariner Card"/>
         <xs:enumeration value="Certificate of U.S. Citizenship (Form N-560 or N-561)"/>
         <xs:enumeration value="Certificate of Naturalization (Form N-550 or N-570)"/>
         <xs:enumeration value="U.S. Citizen ID Card (Form I-197)"/>
         <xs:enumeration value="Identification Card for Use of Resident Citizen in the United
      States (Form I-179)"/>
         <xs:enumeration value=" Certification of Birth Abroad or Certification of Report of
      Birth issued by the Department of State (Form FS-545 or Form DS-1350)"/>
         <xs:enumeration value="Temporary Resident Card (Form I-688)"/>
         <xs:enumeration value="Employment Authorization Card (Form I-688A)"/>
         <xs:enumeration value="Reentry Permit (Form I-327)"/>
         <xs:enumeration value="Refugee Travel Document (Form I-571)"/>
         <xs:enumeration value="Employment authorization document issued by DHS"/>
         <xs:enumeration value="Employment Authorization Document issued by DHS with photograph
      (Form I-688B)"/>
         <xs:enumeration value="Driver's license issued by a Canadian government entity"/>
         <xs:enumeration value="Native American tribal document"/>
       </xs:restriction>
     </xs:simpleType>
   </xs:element>
   <xs:element name="DocumentNumber" type="xs:string" minOccurs="0" maxOccurs="1"/>
   <xs:element name="SequenceNumber" type="xs:string" minOccurs="0" maxOccurs="1"/>
   <xs:element name="CountryCode" type="xs:string" minOccurs="0" maxOccurs="1"/>
   <xs:element name="StateCode" type="xs:string" minOccurs="0" maxOccurs="1"/>
   <xs:element name="ExpiryDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
   <xs:element name="DocumentImageFront" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
   <xs:element name="DocumentImageBack" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
   <xs:element name="CollectionDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

The **EPDocumentType** complex type contains information related to the identity source document presented by the subject of the PIV chain-of-trust enrollment record during the enrollment process. There are two instances of the type to specify primary and secondary identity source documents. The ten elements supported in each **EPDocumentType** complex type are:

<DocumentTypeIdentifier>:

This element is required and occurs once. The element represents the identity source document presented during the [FIPS201] identity proofing process. The <DocumentTypeIdentifier> element indicates either: the Primary identity source document or the Secondary identity source document as the value. The data is provided in an xs:string format.

<DocumentTypeCode>:

This element is required and occurs once. The <DocumentTypeCode> element indicates the type of document verified during the enrollment of the PIV cardholder. The data is provided in an xs:string format. The

<DocumentTypeCode> element is selected from the following two bulleted lists of permitted values, as documented in [FIPS201]:

For one of the **EPDocumentType** instances, the identity source document is a primary identity source document and one of the following values should be used:

- U.S. Passport or a U.S. Passport Card;
- Driver's license or an ID card issued by a state or possession of the United States provided it contains a photograph;
- Permanent Resident Card or an Alien Registration Receipt Card (Form I-551);
- Foreign passport;
- Employment Authorization Document that contains a photograph (Form I-766);
- U.S. Military ID card;
- U.S. Military dependent's ID card; or
- PIV Card.

For the other **EPDocumentType** instance, the secondary identity source document is indicated and the following values should be used:

- U.S. Social Security Card issued by the Social Security Administration;
- Original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal;
- ID card issued by a federal, state, or local government agency or entity, provided it contains a photograph;
- Voter's registration card;
- U.S. Coast Guard Merchant Mariner Card;
- Certificate of U.S. Citizenship (Form N-560 or N-561);
- Certificate of Naturalization (Form N-550 or N-570);
- U.S. Citizen ID Card (Form I-197);
- Identification Card for Use of Resident Citizen in the United States (Form I-179);
- Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350);
- Temporary Resident Card (Form I-688);
- Employment Authorization Card (Form I-688A);
- Reentry Permit (Form I-327);
- Refugee Travel Document (Form I-571);
- Employment authorization document issued by DHS;
- Employment Authorization Document issued by DHS with photograph (Form I-688B);
- Driver's license issued by a Canadian government entity; or

- Native American tribal document.

<DocumentNumber>:
This element is optional, and if used occurs once. The element indicates the document number from the identity source document verified during enrollment. The data is provided in an xs:string format.

<SequenceNumber>:
This element is optional, and if used occurs once. The element indicates the sequence number from the identity source document verified during enrollment. The data is provided in an xs:string format.

<CountryCode>:
This element is optional and if used occurs once. The element indicates the country that issued the identity source document verified during the PIV enrollment process. The country code is formatted in an abbreviation (alpha-3 format), as documented in [ISO3166]. The data is provided in an xs:string format.

<StateCode>:
This element is optional and if used occurs once. The element indicates the US state that provided the identity source document verified during enrollment. The state name is formatted as a two letter abbreviation, as documented by the United States Postal Service [USPS-Appendix B]. The data is provided in an xs:string format.

<ExpiryDate>:
This element is optional and if used occurs only once. The element indicates the date the identity source document verified during enrollment is set to expire. The data is provided in an xs:date format.

<DocumentImageFront>:
This element is optional and if used occurs only once. The <DocumentImageFront> element contains a scanned JPEG or PDF image of the front of the identity source document verified during enrollment. The data is provided in an xs:base64Binary format.

<DocumentImageBack>:
This element is optional and if used occurs only once. The <DocumentImageBack> element contains a scanned JPEG or PDF image of the back of the identity source document verified during enrollment. The data is provided in an xs:base64Binary format.

<CollectionDate>:
This element is optional and if used occurs only once. The element indicates the date the identity source document was collected and verified by an enrollment official. The data is provided in an xs:date format.

3.11 Complex Type PIVCardTopographyType

The following schema fragment defines the **PIVCardTopographyType** complex type:

```
<xs:complexType name="PIVCardTopographyType">
  <xs:sequence>
    <xs:element name="EmployeeAffiliation" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="AgencyDepartmentOrOrganization" type="xs:string" minOccurs="0"
       maxOccurs="1"/>
    <xs:element name="CardExpirationDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
    <xs:element name="AffiliationColorCode" minOccurs="0" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="B"/>
          <xs:enumeration value="G"/>
          <xs:enumeration value="W"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="AgencyCardSerialNumber" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="IssuerIdentificationNumber" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Signature" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="AgencySpecificText4F" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Rank" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="PDFBarCode" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Header" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="AgencySeal" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Footer" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="PhotoBorder" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="AgencySpecificData" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="OrganizationalAffiliationAbbreviation" type="xs:string" minOccurs="0"
       maxOccurs="1"/>
    <xs:element name="RidgingOrNotchedTactileMarker" minOccurs="0" maxOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Ridging"/>
          <xs:enumeration value="Notched Corner"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="LaserEngraving" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ReturnAddress" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="AdditionalLanguageForEmergencyResponseOfficials" type="xs:string"
       minOccurs="0" maxOccurs="1"/>
    <xs:element name="StandardSection499Title18" type="xs:string" minOccurs="0" maxOccurs="1"
       fixed="This credential is the property of the U.S. Government. Counterfeiting, altering, or
       misusing violates Section 499, Title 18 of the U.S. Code."/>
    <xs:element name="AgencySpecificText9B" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="AgencySpecificText10B" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CardFrontImage" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CardBackImage" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

The **PIVCardTopography** complex type contains information used for printing the front and back of the PIV Card as described in [FIPS201][2]. The twenty-three elements supported in the **PIVCardTopography** complex type are:

[2] <PrintedName> in the PersonalInformationType can be used to print the name of the subject on the front of the card.

<EmployeeAffiliation>:

This element is optional and if used occurs only once. The element contains the employee affiliation to be printed on the card. Some examples of employee affiliation are “Employee,” “Contractor,” “Active Duty,” and “Civilian.” The <EmployeeAffiliation> element is the value for Zone 8F on the front of the PIV Card. The data is provided in an xs:string format.

<AgencyDepartmentOrOrganization>:

This element is optional and if used occurs only once. The element contains the organizational affiliation of the cardholder. The <AgencyDepartmentOrOrganization> element is the value for Zone 10F on the front of the PIV Card. The data is provided in an xs:string format.

<CardExpirationDate>:

This element optional and if used occurs only once. The element contains the date the PIV Card is set to expire. The <CardExpirationDate> element is the value for Zone 14F on the front of the PIV Card. The data is provided in an xs:date format.

<AffiliationColorCode>:

This element is optional and if used occurs only once. The <AffiliationColorCode> element is the value for Zone 18F on the front of the PIV Card. This value also indicates the color that is to be used in Zone 15F and as a background color for Zone 2F (name). The <AffiliationColorCode> element is selected from the following values: B, G, or W. B indicates Blue for Foreign National, G indicates Green for Contractors, and W indicates White for Government Employee. The data is provided in an xs:string format.

<AgencyCardSerialNumber>:

This element is optional and if used occurs only once. The element contains the unique serial number from the issuing department or agency. The format shall be at the discretion of the issuing department or agency. The <AgencyCardSerialNumber> element is the value for Zone 1B on the back of the PIV Card. The data is provided in an xs:string format.

<IssuerIdentificationNumber>:

This element is optional and if used occurs only once. The element consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency. The <IssuerIdentificationNumber> element is the value for Zone 2B on the back of the PIV Card. The data is provided in an xs:string format.

<Signature>:

This element is optional and if used occurs only once. The element contains a JPEG image of the cardholder’s signature. The <Signature> element is the

value for Zone 3F on the front of the PIV Card. The data is provided in an xs:base64Binary format.

<AgencySpecificText4F>:
This element is optional and if used occurs only once. The element contains text for printing agency specific requirements on the PIV Card, such as employee status. The <AgencySpecificText4F> element is the value for Zone 4F on the front of the PIV Card. The data is provided in an xs:string format.

<Rank>:
This element is optional and if used occurs only once. The element contains text for the cardholder's rank. The format of the text is at the department or agency's discretion. The <Rank> element is the value for Zone 5F on the front of the PIV Card. The data is provided in an xs:string format.

<PDFBarCode>:
This element is optional and if used occurs only once. The element contains a Portable Data File (PDF) Two-Dimensional Bar Code JPEG image. The <PDFBarCode > element is the value for Zone 6F on the front of the PIV Card. The data is provided in an xs:base64Binary format.

<Header>:
This element is optional and if used occurs only once. If used the element should contain either the text "United States Government", or departments and agencies may also choose to use this text for other department or agency-specific information, such as identifying a federal emergency responder role. The <Header> element is the value for Zone 9F on the front of the PIV Card. The data is provided in an xs:string format.

<AgencySeal>:
This element is optional and if used occurs only once. The element contains a JPEG image of the seal selected by the issuing department, agency, or organization for printing on the PIV Card. The <AgencySeal> element is the value for Zone 11F on the front of the PIV Card. The data is provided in an xs:base64Binary format.

<Footer>:
This element is optional and if used occurs only once. If used the element should contain the location label for the Federal Emergency Response Official (FERO) identification. A department or agency may print "Federal Emergency Response Official", preferably in white lettering on a red background on the PIV Card. Departments and agencies may also use the <Footer> element to further identify the federal emergency respondent's official role. Some examples of official roles are "Law Enforcement," "Fire Fighter," and "Emergency Response Team (ERT)." When Zone 15F indicates foreign national affiliation and the department or agency does not need to

highlight emergency response official status, the <Footer> element may be used to denote the country or countries of citizenship. If so used, the department or agency shall print the country name or the three-letter country abbreviation (alpha-3 format) in accordance with ISO 3166-1, Country Codes [ISO3166]. The <Footer> element is the value for Zone 12F on the front of the PIV Card. The data is provided in an xs:string format.

<PhotoBorderPattern>:

This element is optional and if used occurs only once. The element contains a JPEG image of the photo border. A border may be used with the photo to further identify employee affiliation. This border may be used in conjunction with Zone 15F to enable departments and agencies to develop various employee categories. The photo border shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red shall be reserved for emergency response officials, blue for foreign nationals, and green for contractors. All other colors may be used at the department or agency's discretion. The <PhotoBorderPattern> element is the value for Zone 16F on the front of the PIV Card. The data is provided in an xs:base64Binary format.

<AgencySpecificData>:

This element is optional and if used occurs only once. In cases in which other defined optional elements are not used, the <AgencySpecificData> element may be used for other department or agency-specific information and is set to the value of Zone 17F on the front of the PIV Card. The data is provided in an xs:string format.

<OrganizationalAffiliationAbbreviation>:

This element is optional and if used occurs only once. The element contains the organizational affiliation abbreviation for printing on the PIV Card. The <OrganizationalAffiliationAbbreviation> element is the value for Zone 20F on the front of the PIV Card. The data is provided in an xs:string format.

<RidgingOrNotchedTactileMarker>:

This element is optional and if used occurs only once. The element indicates if the PIV Card should incorporate edge ridging or a notched corner to indicate card orientation. The <RidgingOrNotchedTactileMarker> element is selected from the following values: "Ridging" or Notched Corner". The <RidgingOrNotchedTactileMarker> element is the value for Zone 21F on the front of the PIV Card. The data is provided in an xs:string format.

<LaserEngraving>:

This element is optional and if used occurs only once. The element indicates if the PIV Card should include tactilely discernible marks created using laser engraving to indicate card orientation. The <LaserEngraving> element is set to true if laser engraving should be applied to the PIV Card and set to false if

laser engraving should not be applied to the PIV Card. The <LaserEngraving> element is the value for Zone 22F on the front of the PIV Card. The data is provided in an xs:boolean format.

<ReturnAddress>:

This element is optional and if used occurs only once. The element contains the "return if lost" language placed on the back of the PIV Card. The <ReturnAddress> element is the value for Zone 4B on the back of the PIV Card. The data is provided in an xs:string format.

<AdditionalLanguageForEmergencyResponseOfficials>:

This element is optional and if used occurs only once. The element contains text if the departments and agencies choose to provide additional information to identify emergency response officials or to better identify the cardholder's authorized access. The <AdditionalLanguageForEmergencyResponseOfficials> element is the value for Zone 6B on the back of the PIV Card. The data is provided in an xs:string format.

<StandardSection499Title18>:

This element is optional and if used occurs only once. The element contains the fixed text for the standard Section 499, Title 18, language warning against counterfeiting, altering, or misusing the PIV Card. The <StandardSection499Title18> element is the value for Zone 7B on the back of the PIV Card. The data is provided in an xs:string format.

<AgencySpecificText9B>:

This element is optional and if used occurs only once. The element contains text for printing agency specific requirements on the PIV Card. Departments and agencies are encouraged to use this area prudently and minimize printed text to that which is absolutely necessary. The <AgencySpecificText9B> element is the value for Zone 9B on the back of the PIV Card. The data is provided in an xs:string format.

<AgencySpecificText10B>:

This element is optional and if used occurs only once. The element contains text for printing agency specific requirements on the PIV Card. Departments and agencies are encouraged to use this area prudently and minimize printed text to that which is absolutely necessary. The <AgencySpecificText10B> element is the value for Zone 10B on the back of the PIV Card. The data is provided in an xs:string format.

<CardFrontImage>:

This element is optional and if used occurs only once. The element contains a JPEG image of how the front of the PIV Card should appears when printed. The data is provided in an xs:base64Binary format.

<CardBackImage>:

This element is optional and if used occurs only once. The element contains a JPEG image of how the back of the PIV Card should appears when printed. The data is provided in an xs:base64Binary format.

4 Chain-of-trust Record Encryption in Transit

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, as documented in Section 3.3 for PIVChainOfTrustType, 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 [FIPS140] standard.

5 Log and Historical Data

Logs and historical data are 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 re-issuance, loss of card and subsequent reissuance.

Appendix A—XML Schema

This appendix contains the chain of trust XML schema, which can also be download at http://csrc.nist.gov/schema/piv/chain-of-trust/piv-chain-of-trust-1.0.xsd.

```
<?xml version="1.0" encoding="utf-8"?>

<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://csrc.nist.gov/ns/piv/chain-of-trust/1.0" xmlns="http://csrc.nist.gov/ns/piv/chain-of-trust/1.0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/>
<xs:import namespace="http://www.w3.org/2001/04/xmlenc#" schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/>

        <xs:element name="PIVChainOfTrust" type="PIVChainOfTrustType"/>

        <xs:complexType name="PIVChainOfTrustType">
                <xs:sequence>
                        <xs:choice>
                                <xs:sequence>
                                        <xs:element ref="xenc:EncryptedData" minOccurs="1" maxOccurs="1"/>
                                        <xs:element ref="xenc:EncryptedKey" minOccurs="1" maxOccurs="unbounded"/>
                                </xs:sequence>
                                <xs:sequence>
                                        <xs:element name="EnrollmentRecord" type="EnrollmentRecordType" minOccurs="1"
maxOccurs="unbounded"/>
                                        <xs:element ref="ds:Signature" minOccurs="1" maxOccurs="1"/>
                                </xs:sequence>
                        </xs:choice>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="EnrollmentRecordType">
                <xs:sequence>
                        <xs:element name="PersonalInformation" type="PersonalInformationType" minOccurs="1" maxOccurs="1"/>
                        <xs:element name="AdjudicationInformation" type="AdjudicationInformationType" minOccurs="1" maxOccurs="1"/>
                        <xs:element name="EnrollmentPackage" type="EnrollmentPackageType" minOccurs="1" maxOccurs="1"/>
                        <xs:element name="PIVCardTopography" type="PIVCardTopographyType" minOccurs="0" maxOccurs="1"/>
                </xs:sequence>
        </xs:complexType>
        <xs:complexType name="PersonalInformationType">
                <xs:sequence>
                        <xs:element name="PrimaryIdentifier" type="xs:string" minOccurs="1" maxOccurs="1"/>
                        <xs:element name="SecondaryIdentifier" type="xs:string" minOccurs="1" maxOccurs="1"/>
```

```
                <xs:element name="PrintedName" type="xs:string" minOccurs="1" maxOccurs="1"/>
                <xs:element name="SSN" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="IsUSCitizen" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
                <xs:element name="CitizenshipCountryCode" type="xs:string" minOccurs="1" maxOccurs="unbounded"/>
                <xs:element name="CardHolderUUID" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="CardUUID" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="CHUID" type="xs:string" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
</xs:complexType>
<xs:complexType name="AdjudicationInformationType">
        <xs:sequence>
                <xs:element name="NACIAdjudicationValue" minOccurs="1" maxOccurs="1">
                        <xs:simpleType>
                                <xs:restriction base="xs:string">
                                        <xs:enumeration value="Approved"/>
                                        <xs:enumeration value="Pending"/>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:element>
                <xs:element name="NACIAdjudicationEffDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
</xs:complexType>
<xs:complexType name="EnrollmentPackageType">
        <xs:sequence>
                <xs:element name="EPBiographic" type="EPBiographicType" minOccurs="0" maxOccurs="1"/>
                <xs:element name="EPBiometrics" type="EPBiometricsType" minOccurs="1" maxOccurs="1"/>
                <xs:element name="EPDocument" type="EPDocumentType" minOccurs="2" maxOccurs="2"/>
        </xs:sequence>
</xs:complexType>
<xs:complexType name="EPBiographicType">
        <xs:sequence>
                <xs:element name="GenderCode" minOccurs="0" maxOccurs="1">
                        <xs:simpleType>
                                <xs:restriction base="xs:string">
                                        <xs:enumeration value="Female"/>
                                        <xs:enumeration value="Male"/>

                                </xs:restriction>
                        </xs:simpleType>
                </xs:element>
                <xs:element name="EyeColorCode" minOccurs="0" maxOccurs="1">
                        <xs:simpleType>
                                <xs:restriction base="xs:string">

                                        <xs:enumeration value="Blue"/>
                                        <xs:enumeration value="Brown"/>
                                        <xs:enumeration value="Gray"/>
```

```
                                        <xs:enumeration value="Green"/>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:element>
                <xs:element name="HairColorCode" minOccurs="0" maxOccurs="1">
                        <xs:simpleType>
                                <xs:restriction base="xs:string">
                                        <xs:enumeration value="Bald"/>
                                        <xs:enumeration value="Black"/>
                                        <xs:enumeration value="Blonde"/>

                                        <xs:enumeration value="Brown"/>
                                        <xs:enumeration value="Gray or Partially Gray"/>
                                        <xs:enumeration value="Red or Auburn"/>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:element>
                <xs:element name="Height" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="Weight" type="xs:integer" minOccurs="0" maxOccurs="1"/>
                <xs:element name="EthnicityCode" minOccurs="0" maxOccurs="1">
                        <xs:simpleType>
                                <xs:restriction base="xs:string">
                                        <xs:enumeration value="A"/>
                                        <xs:enumeration value="B"/>
                                        <xs:enumeration value="I"/>
                                        <xs:enumeration value="U"/>
                                        <xs:enumeration value="W"/>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:element>
                <xs:element name="EnrollmentDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
</xs:complexType>
<xs:complexType name="EPBiometricsType">
        <xs:sequence>
                <xs:element name="Photo" type="xs:base64Binary" minOccurs="1" maxOccurs="1"/>
                <xs:element name="FingerprintsOffCardComparisonRepresentation" type="xs:base64Binary" minOccurs="1"
maxOccurs="1"/>
                <xs:element name="FingerprintOnCardComparisonRepresentation" type="xs:base64Binary" minOccurs="0"
maxOccurs="1"/>
                <xs:element name="IrisRepresentation" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
</xs:complexType>
<xs:complexType name="EPDocumentType">
        <xs:sequence>
                <xs:element name="DocumentTypeIdentifier" minOccurs="1" maxOccurs="1">
                        <xs:simpleType>
```

```
                                        <xs:restriction base="xs:string">
                                                <xs:enumeration value="Primary identity source"/>
                                                <xs:enumeration value="Secondary identity source"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:element>
                        <xs:element name="DocumentTypeCode" minOccurs="1" maxOccurs="1">
                                <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                                <xs:enumeration value="U.S. Passport or a U.S. Passport Card"/>
                                                <xs:enumeration value="Permanent Resident Card or an Alien Registration Receipt Card
(Form I-551)"/>
                                                <xs:enumeration value="Foreign Passport"/>
                                                <xs:enumeration value="Employment Authorization Document that contains a photograph (Form
I-766)"/>
                                                <xs:enumeration value="Driver's license or an ID card issued by a state or possession of
the United States provided it contains a photograph"/>
                                                <xs:enumeration value="U.S. Military ID card"/>
                                                <xs:enumeration value="U.S. Military dependent's ID card"/>
                                                <xs:enumeration value="PIV Card"/>
                                                <xs:enumeration value="U.S. Social Security Card issued by the Social Security
Administration"/>
                                                <xs:enumeration value="Original or certified copy of a birth certificate issued by a
state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal"/>
                                                <xs:enumeration value="ID card issued by a federal, state, or local government agency or
entity, provided it contains a photograph"/>
                                                <xs:enumeration value="Voter's registration card"/>
                                                <xs:enumeration value="U.S. Coast Guard Merchant Mariner Card"/>
                                                <xs:enumeration value="Certificate of U.S. Citizenship (Form N-560 or N-561)"/>
                                                <xs:enumeration value="Certificate of Naturalization (Form N-550 or N-570)"/>
                                                <xs:enumeration value="U.S. Citizen ID Card (Form I-197)"/>
                                                <xs:enumeration value="Identification Card for Use of Resident Citizen in the United
States (Form I-179)"/>
                                                <xs:enumeration value=" Certification of Birth Abroad or Certification of Report of Birth
issued by the Department of State (Form FS-545 or Form DS-1350)"/>
                                                <xs:enumeration value="Temporary Resident Card (Form I-688)"/>
                                                <xs:enumeration value="Employment Authorization Card (Form I-688A)"/>
                                                <xs:enumeration value="Reentry Permit (Form I-327)"/>
                                                <xs:enumeration value="Refugee Travel Document (Form I-571)"/>
                                                <xs:enumeration value="Employment authorization document issued by DHS"/>
                                                <xs:enumeration value="Employment Authorization Document issued by DHS with photograph
(Form I-688B)"/>
                                                <xs:enumeration value="Driver's license issued by a Canadian government entity"/>
                                                <xs:enumeration value="Native American tribal document"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:element>
```

```
                <xs:element name="DocumentNumber" type="xs:string" minOccurs="1" maxOccurs="1"/>
                <xs:element name="SequenceNumber" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="CountryCode" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="StateCode" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="ExpiryDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
                <xs:element name="DocumentImageFront" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                <xs:element name="DocumentImageBack" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                <xs:element name="CollectionDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
</xs:complexType>
<xs:complexType name="PIVCardTopographyType">
        <xs:sequence>
                <xs:element name="EmployeeAffiliation" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="AgencyDepartmentOrOrganization" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="CardExpirationDate" type="xs:date" minOccurs="0" maxOccurs="1"/>
                <xs:element name="AffiliationColorCode" minOccurs="0" maxOccurs="1">
                        <xs:simpleType>
                                <xs:restriction base="xs:string">
                                        <xs:enumeration value="B"/>
                                        <xs:enumeration value="G"/>
                                        <xs:enumeration value="W"/>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:element>
                <xs:element name="AgencyCardSerialNumber" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="IssuerIdentificationNumber" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="Signature" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                <xs:element name="AgencySpecificText4F" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="Rank" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="PDFBarCode" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                <xs:element name="Header" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="AgencySeal" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                <xs:element name="Footer" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="PhotoBorder" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                <xs:element name="AgencySpecificData" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="OrganizationalAffiliationAbbreviation" type="xs:string" minOccurs="0" maxOccurs="1"/>
                <xs:element name="RidgingOrNotchedTactileMarker" minOccurs="0" maxOccurs="1">
                        <xs:simpleType>
                                <xs:restriction base="xs:string">
                                        <xs:enumeration value="Ridging"/>
                                        <xs:enumeration value="Notched Corner"/>
                                </xs:restriction>
                        </xs:simpleType>
                </xs:element>
                <xs:element name="LaserEngraving" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
                <xs:element name="ReturnAddress" type="xs:string" minOccurs="0" maxOccurs="1"/>
```

```
                        <xs:element name="AdditionalLanguageForEmergencyResponseOfficials" type="xs:string" minOccurs="0"
maxOccurs="1"/>
                        <xs:element name="StandardSection499Title18" type="xs:string" minOccurs="0" maxOccurs="1" fixed="This credential
is the property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code."/>
                        <xs:element name="AgencySpecificText9B" type="xs:string" minOccurs="0" maxOccurs="1"/>
                        <xs:element name="AgencySpecificText10B" type="xs:string" minOccurs="0" maxOccurs="1"/>
                        <xs:element name="CardFrontImage" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                        <xs:element name="CardBackImage" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                </xs:sequence>
        </xs:complexType>
</xs:schema>
```

Appendix B—XML Sample PIVChainOfTrust Record

```
<?xml version="1.0" encoding="utf-8"?>
<nist:PIVChainOfTrust xmlns:nist="http://csrc.nist.gov/ns/piv/chain-of-trust/1.0">
        <nist:EnrollmentRecord>
                <nist:PersonalInformation>
                        <nist:PrimaryIdentifier>Doe</nist:PrimaryIdentifier>
                        <nist:SecondaryIdentifier>Jane</nist:SecondaryIdentifier>
                        <nist:PrintedName>Jane Doe</nist:PrintedName>
                        <nist:IsUSCitizen>true</nist:IsUSCitizen>
                        <nist:CitizenshipCountryCode>US</nist:CitizenshipCountryCode>
                        <nist:CardUUID>bb3618a0-4d26-11e5-885d-feff819cdc9f</nist:CardUUID>

        <nist:CHUID>538206493019D4F81oD901156010020285836oDRB4BC32D14F8184388E13FC341830303038303030383030303030383030353832303131 3B333
B343E82068D308206890609298648 86F7BD8187829082SFR308205F68201033189300786052BBEB3021938890608638648816503060190828423308284 1F3882038890
03020102020219E13000068929864886F7BDo10105050030503103388906035584861302555331183816860355048913oF552E532E28476F7665726E6D656E74318038
09860355048B1303446F44318C380906035504oB1383584849311738158683550403 13oE444F44204R4954432843412D3133381E17BD3B373B31323231393238343459
17BD31323031323131393238343459306231BB380986835504861382555331183816860355848913BF552E532E23476F7665726E6D656E74318C388906835504881383
446F44313C338906B35584BB13B3534B49311D381306035584331314446F44284361726420497373756572205438303738819F3ooDo68929864886F780010101050003
818Do830818902818 18oD4C2B97DD4F37C1RBD573094286B2058DE9B2667DDE1924981140673DB3BC8ED285663E8563475ECC3EE1100809028DDGE88BFBSR9B8964CBB
4BESF81E1ERSB342992298F557F44905C6709B37326B47D66DSC313D1965BRE33FZBQFD34FEo571FDDB1BBl43DEB8EDSDI4B297C83EEF2CB8771E8E6403429C7F74f1E
D982D69050203010801f138201E8308201E4301Fo603551D23B41830168014DB88CB96584EFQCD4D107E994EZB4FC173D37917301Do603551DBEB416B414773988D289
E69D889D4EIC7F28C99DS9129769793813868 3551D2584BC3889060868864801658386873BBE8683551DBFBlBlFFB4848302860038160683551D2884oF3BBD38038609
6886480165823183093081DF8683551D1F8481D73881D4383898399037863568747478392F2F63726C2E6764732E6E69742E646973612E6D696C2F67657463726C3F44
4F44253238494954432532304341203133308194988191908 18E86818B6C646170392F2F63726C2E6764732E6E69742E646973612E6D696C2F636E253364444F442532
3049495443253230434120313325326 36F752533645048492532636F75253364446F442532636F253364552E532E253230476F7665726E6D656E742532636325336455
533F6365727469666963617465726 6F636174696F6E6C6973743B62696E617279338182060828868105058731 01@476307438420688230601058507388286366874
7478392F2F63726E2E6764732E6E69742E646973612E6D696C2F6765747369676E3F444F442532304f1495443253238434 12D3133382E860823068185058730818622 6
8747470392F2F6F6373782E6E736E382E726376732E6E69742E646973612E6D696CBBBD868929864886F7BD8181858508838188B631481DF3DD550297829919FB464
R75063387378203BF3E7DFCICSSERD91F104E562893996CRFD8613EC3B991592904529371oD3B4CDQBB4DFBS478oF867Q61918433922259CEOE37BR944504145C258E5
837089942418CE382215028nCB3EC4BFF26B372D5F340754DE6787CR3953SF509FE854CZBC9CBF8814269170785903182 01B13082019002010130623 05C31083809060
35504B6130255533118381686035504 8913oF552E532E28476F7665726E6D656E7431003889860355048B1303446F44318C3009060355040313035043493117381586 8
355040313oE444F44284R4954432843412D3133028219E13BB7B6BSZBBEB3821998819938118683672908318986886086488165838681382306892986 4886F78Do109B
431168414EDDBB7R710158C6689F66828D73421FCSZB4608430780688608648816583868531643062 31BB380906835584861302555331183316868355843913BF552E5
32E20476F7665726E6D656E7431oC3BBRB6035584BBI383446F44310€3089060355 04BB1303504349311D3018068355048313144 6F44204361726428497373756572 2
05430383738oB868929864886F7BDo1010584818980162C29697DF641EE7E141C2BC29B41689SF96FB77R79959E69C4438DFDC7BBE9128E8D05BDDSRFF8194RB3C4E61
37EB9354B8F3773DC142F7F57E9E1E244BCBFRR3E949D9724B1BFCR49F9E1C2B1CB821B3BD1f1ECD9RF636SCD2BE95CF5C64808879D67942CF4B18624F4763F9BBD713
Do4CDD899FE480629F4235BCEB3884FEBB</nist:CHUID>
                </nist:PersonalInformation>
                <nist:AdjudicationInformation>
                        <nist:NACIAdjudicationValue>Approved</nist:NACIAdjudicationValue>
                        <nist:NACIAdjudicationEffDate>2014-12-13</nist:NACIAdjudicationEffDate>
                </nist:AdjudicationInformation>
                <nist:EnrollmentPackage>
                        <nist:EPBiographic>
                                <nist:GenderCode>Female</nist:GenderCode>
```

```
                        <nist:EyeColorCode>Brown</nist:EyeColorCode>
                        <nist:HairColorCode>Brown</nist:HairColorCode>
                        <nist:Height>508</nist:Height>
                        <nist:Weight>150</nist:Weight>
                        <nist:EthnicityCode>W</nist:EthnicityCode>
                        <nist:EnrollmentDate>2015-11-13</nist:EnrollmentDate>
                </nist:EPBiographic>
                <nist:EPBiometrics>
                        <nist:Photo>Base64EncodedData...</nist:Photo>

        <nist:FingerprintsOffCardComparisonRepresentation>Base64EncodedData...</nist:FingerprintsOffCardComparisonRepresentation>

        <nist:FingerprintOnCardComparisonRepresentation>Base64EncodedData...</nist:FingerprintOnCardComparisonRepresentation>
        <nist:IrisRepresentation>Base64EncodedData...</nist:RepresentationIris>
                </nist:EPBiometrics>
                <nist:EPDocument>
                        <nist:DocumentTypeIdentifier>Primary identity source</nist:DocumentTypeIdentifier>
                        <nist:DocumentTypeCode>Driver's license or an ID card issued by a state or possession of the United
States provided it contains a photograph</nist:DocumentTypeCode>
                        <nist:DocumentNumber>T12345678</nist:DocumentNumber>
                        <nist:SequenceNumber>00001</nist:SequenceNumber>
                        <nist:CountryCode>USA</nist:CountryCode>
                        <nist:StateCode>VA</nist:StateCode>
                        <nist:ExpiryDate>2018-12-18</nist:ExpiryDate>
                        <nist:DocumentImageFront>Base64EncodedData...</nist:DocumentImageFront>
                        <nist:DocumentImageBack>Base64EncodedData...</nist:DocumentImageBack>
                        <nist:CollectionDate>2012-12-13</nist:CollectionDate>
                </nist:EPDocument>
                <nist:EPDocument>
                        <nist:DocumentTypeIdentifier>Secondary identity source</nist:DocumentTypeIdentifier>
                        <nist:DocumentTypeCode>U.S. Social Security Card issued by the Social Security
Administration</nist:DocumentTypeCode>
                        <nist:SequenceNumber>123-12-1234</nist:SequenceNumber>
                        <nist:CountryCode>USA</nist:CountryCode>
                        <nist:DocumentImageFront>Base64EncodedData...</nist:DocumentImageFront>
                        <nist:DocumentImageBack>Base64EncodedData...</nist:DocumentImageBack>
                        <nist:CollectionDate>2012-12-13</nist:CollectionDate>
                </nist:EPDocument>
        </nist:EnrollmentPackage>
        <nist:PIVCardTopography>
                <nist:EmployeeAffiliation>Employee</nist:EmployeeAffiliation>
                <nist:AgencyDepartmentOrOrganization>DHS</nist:AgencyDepartmentOrOrganization>
                <nist:CardExpirationDate>2016-12-13</nist:CardExpirationDate>
                <nist:AffiliationColorCode>W</nist:AffiliationColorCode>
                <nist:AgencyCardSerialNumber>987654321</nist:AgencyCardSerialNumber>
                <nist:IssuerIdentificationNumber>123456123412345</nist:IssuerIdentificationNumber>
                <nist:Signature>Base64EncodedData...</nist:Signature>
```

```
                        <nist:AgencySpecificText4F>Zone 2 Approved</nist:AgencySpecificText4F>
                        <nist:Rank>SES</nist:Rank>
                        <nist:PDFBarCode>Base64EncodedData...</nist:PDFBarCode>
                        <nist:Header>United States Government</nist:Header>
                        <nist:AgencySeal>Base64EncodedData...</nist:AgencySeal>
                        <nist:Footer>Federal Emergency Response Official</nist:Footer>
                        <nist:PhotoBorder>Base64EncodedData...</nist:PhotoBorder>
                        <nist:AgencySpecificData>str1234</nist:AgencySpecificData>
                        <nist:OrganizationalAffiliationAbbreviation>DHS</nist:OrganizationalAffiliationAbbreviation>
                        <nist:RidgingOrNotchedTactileMarker>Ridging</nist:RidgingOrNotchedTactileMarker>
                        <nist:LaserEngraving>true</nist:LaserEngraving>
                        <nist:ReturnAddress>Return to: Washington Navy Yard, Building 410, 245 Murray Lane SW Washington, DC
20528</nist:ReturnAddress>
                        <nist:AdditionalLanguageForEmergencyResponseOfficials>Priority
1</nist:AdditionalLanguageForEmergencyResponseOfficials>
                        <nist:StandardSection499Title18>This credential is the property of the U.S. Government. Counterfeiting,
altering, or misusing violates Section 499, Title 18 of the U.S. Code.</nist:StandardSection499Title18>
                </nist:PIVCardTopography>
        </nist:EnrollmentRecord>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
                <ds:Reference URI="#_65c217dd-6589-4830-a277-2083fe4a6183">
                        <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                        <ds:DigestValue>BaCypVvGnmkJvmHImOfavpbrq1f4bL9HasRWGmm7HW0=</ds:DigestValue>
                </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>
        dmbTWZKUYFquHclxtaGOoPYt6Y/J7aFSwj5kfaWIQRG6StlVUk/2OBl7iIDuvRKOYSjwRTpGOXFikjh+iXuA1M+fRKpdTTHPQx/jyLuZDUhcKLWmK/4Sf1DWC39pRLu
Rue5ZSA6zMut+CFEO/x75BQVI2+qwBxCBGLkWV7Bw00JVkYTAV9ILAfP4PNQopnvYA25XAn7XjLX+a/0cC5/l9HB8G1TCKbEmTIBok3oW/j4YaofUhz+zp0Q7YZMMAXZDW3P3B
S2Jy6C90xnihvqBhrQaSCI+acQ1EvLPq8843IUMjSu6Fxr0NOeBBx9sqa837eMlUZZ2UVooOa83q2CHww==</ds:SignatureValue>
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>

        <X509Certificate>MIIFPzCCBCegAwIBAgIHKySIQq+lZDANBgkqhkiG9w0BAQUFADCByjELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTCl
Njb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHkuY29tLCBJbmMuMTMwMQYDVQQLEypodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkxMDAuBgNVBAMT
J0dvIERhZGR5IFNlY3VyZSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTERMA8GA1UEBRMIMDc5NjkyODcwHhcNMTQwODE5MTg1NjAxWhcNMTUwODE5MTg1NjAxWjA7MSEwHwYDVQ
QLExhEb21haW4gQ29udHJvbCBWYWxpZGF0ZWQxFjAUBgNVBAMMDSoudHNjcGxhYi5vcmcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3begiEJktcO17B3DdNGYJ
+KFC4E9sgh0VgkzYas4DVcT9CFAvWaeZCC8Gqp/ywfA4fjIE9U5Toe+t/o9CMReqmnKX52Zd8iGhCawgsdZOLEq5E5Zxe5OJG1IKH+KNH2q1lJPpSd2LShqmqHawqnGplF5Dz9
vSMEcBxXePO/vWInTIkpUCdaKM0DGW34wWZsuk0fpFSjABGxVBsVoy7R40gnDvCBLDDHs7NydorpBrD5hp194feqNTWpda6TgLrsYkh1Ln0AD4y9509u4bHzIsgzac/FFGAJzW
ZZ8+9VbsMpB02GlbjFK4NRAiZHTPlAiJwH6xHQxQzSl1acnq65udAgMBAAGjggG2MIIBsjAMBgNVHRMBAf8EAjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAOBg
NVHQ8BAf8EBAMCBaAwNAYDVR0fBC0wKzApoCegJYYjaHR0cDovL2NybC5nb2RhZGR5LmNvbS9nZHMxLTExMi5jcmwwUwYDVR0gBEwwSjBIBgtghkgBhv1tAQcXATA5MDcGCCsG
```

AQUFBzIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMIGABggrBgEFBQcBAQR0MHIwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmdvZGFkZH
kuY29tLzBKBggrBgEFBQcwAoY+aHR0cDovL2NlcnRpZmljYXRlcy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5L2dkX2ludGVybWVkaWF0ZS5jcnQwHwYDVR0jBBgwFoAU/axhMpNs
Rdbi7oVfmrrndplozOcwJQYDVR0RBB4wHIINKi50c2NwbGFiLm9yZ4ILdHNjcGxhYi5vcmcwHQYDVR0OBBYEFP0E9r1Mgzp48Kd74+fbhZjUvzZQMA0GCSqGSIb3DQEBBQUAA4
IBAQAxl/u3Nb8mG5Bm4tWV+j+NW2PqwvLVL2qTafk+fNwlI46Rjxmb4+QR2xZbYytO0zPPa9rszVQy43SA2+sOD5OAWoUv+P7lOX87d26Nzi/gAJCgfbLj6YMaeOKfut5KIVih
h2x/CJbV12w3Gn0Jf6TUYi/6HayKrDVAw1MFNzTS0oFCWOZj9I1KIyhe99+s+h5rIVjT75ETyPn3jfjmiWr4sXwswjdGhuxOrgq0tonKI6NdzQnC1OAgvFcAiMzJT+RmN8Ltat
SwESv5YBND8PYJ/1rD2nGVI27S/LkAMeWCQxGf+9wFtzuqzYtbX1nxv5ksvimzJ+cOaa/BcAYkGC10</X509Certificate>
</X509Data>
</KeyInfo>
</ds:Signature>
</nist:PIVChainOfTrust>

Appendix C—References

[EBTS] Criminal Justice Information Services. Electronic Biometric Transmission Specification (EBTS) 10.0, July 2, 2013, https://www.fbibiospecs.cjis.gov/Document/Get?fileName=Master%20EBTS%20v10%20-%20FINAL%2020130702.pdf [accessed 5/10/16].

[FIPS140] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-2, May 2001 (including change notices through 12/3/02), 61 pp. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [accessed 5/10/16].

[FIPS201] National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Federal Information Processing Standards (FIPS) Publication 201-2, August 2013, 87pp. http://dx.doi.org/10.6028/NIST.FIPS.201-2.

[HSPD12] Homeland Security Presidential Directive-12, *Policies for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. http://www.dhs.gov/homeland-security-presidential-directive-12 [accessed 5/10/16].

[ISO3166] International Organization for Standardization, *Codes for the representation of names of countries and their subdivisions*, https://www.iso.org/obp/ui/#search [accessed 5/10/16].

[M-07-16] Office of Management and Budget (OMB), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf [accessed 5/11/16]

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2119, March 1997 https://dx.doi.org/10.17487/rfc2119.

[SP800-73-4] National Institute of Standards and Technology, *Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation*, NIST Special Publication (SP) 800-73-4, May 2015 (updated 2/8/16), http://dx.doi.org/10.6028/NIST.SP.800-73-4.

[SP800-76] National Institute of Standards and Technology, *Biometric*

Specifications for Personal Identity Verification, NIST Special Publication (SP) 800-76-2, July 2013, http://dx.doi.org/10.6028/NIST.SP.800-76-2.

[SP800-79-2] National Institute of Standards and Technology, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)* , NIST Special Publication (SP) 800-79-2, July 2015, http://dx.doi.org/10.6028/NIST.SP.800-79-2.

[USPS-Appendix B] United States Postal Service, *Appendix B: Two-Letter State and Possession Abbreviations*, in Publication 28, *Postal Addressing Standards*, PSN 7610-03-000-3688, May 2015, http://pe.usps.gov/text/pub28/28apb.htm [accessed 5/10/16].

[XMLEnc] World Wide Web Consortium, *XML Encryption Syntax and Processing Version 1.1*, W3C Recommendation 11 April 2013, http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/ [accessed 5/10/16].

[XMLSchema] World Wide Web Consortium, *XML Schema*, October 15, 2014, http://www.w3.org/2001/XMLSchema [accessed 5/10/16].

[XMLSig] World Wide Web Consortium, *XML Signature Syntax and Processing (Second Edition)*, W3C Recommendation 10 June 2008, http://www.w3.org/TR/xmldsig-core/#sec-Versions [accessed 5/10/16].

Appendix D—Glossary of Terms

Biometric	The stored electronic information pertaining to a biometric. This information can be in terms of compressed pixels or in terms of some characteristic (e.g., patterns).
Cardholder	An individual possessing an issued PIV Card.
Chain-of-trust	The chain-of-trust is a sequence of related enrollment data sets that is created and maintained by PIV Card issuers
FASC-N	Federal Agency Smart Credential Number (FASC-N): As required by [FIPS201], one of the primary identifiers on the PIV Card. The FASC-N is a fixed length (25-byte) data object, specified in [SP800-73-4], and included in several data objects on a PIV Card.
Issuer	An agency or service provider that issues PIV credentials in accordance with [FIPS201] and NIST [SP 800-79-2].
Off-Card	A cardholder's biometric reference data stored on the PIV Card that is matched against the cardholder's life-scan biometrics Off-Card during authentication.
On-Card	A cardholder's biometric reference data stored on the PIV Card that is matched against the cardholder's life-scan biometrics On-Card during authentication.

Appendix E—Acronyms

CHUID	Card Holder Unique Identifier
DN	Distinguished Name
EVSSL	Extended Validation Secure Sockets Layer
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certificate Authority
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FTPS	File Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HSPD	Homeland Security Presidential Directive
ITL	Information Technology Laboratory
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OCC	On-Card Comparison
OMB	Office of Management and Budget
PDF	Portable Data File
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RFC	Request for Comment
S/MIME	Secure/Multipurpose Internet Mail Extensions
USPS	United States Postal Service
UUID	Universally Unique Identifier

W3C	World Wide Web Consortium
XML	Extensible Markup Language