Framework for Inter-Agency Authentication of Federal Personal Identity Verification (PIV) Cards

Prepared by: Backend Authentication Work Group
Prepared For: Federal Smart Card Interagency Advisory Board (IAB)

Version 1.0

14 August 2006

About the Federal Smart Card Interagency Advisory Board (IAB)

The IAB is a Federal forum that focuses on sharing implementation lessons learned and developing implementation guidance on identity management initiatives. The IAB provides recommendations on smart card and identity management standards across the government with the intent to unify the Federal community in common operating practices and to maximize interoperability. Representatives are from Federal agencies, state and local governments, industry associations, and the vendor community.

About this document

This report was developed by the Backend Authentication Work Group (BAS WG), an organization under the IAB, and will be published by the IAB. It focuses on defining implementation options for authenticating the validity of Federal Personal Identity Verification (PIV) credentials and exchanging additional attributes about a particular PIV cardholder. It is intended to be a framework for backend transactions through gateways. We have purposely omitted finite information needed to actually implement a solution. The Homeland Presidential Directive 12 Executive Steering Committee's (ESC) Architecture Work Group (AWG) will create an interface specification utilizing this framework. The interface specification is expected to contain details associated with transport protocols, authentication schemes, operating rules, file sizes, and such.

This document is informative and elective in nature.

Table of Contents

1. Overview

Back-end (issuer) authentication and validation of credentials and tokens is an essential element in secure access. The Federal Smart Card Interagency Advisory Board (IAB) established a working level group to examine the needs and potential guidelines to better enable back-end transactions to:

- Authenticate the validity of Personal Identity Verification (PIV) certificates
- Authenticate the validity of PIV credentials
- Share NAC-with written inquiries (NAC-I)[1] status information
- Provide information on revoked, expired, suspended or lost/stolen credentials
- Utilize web-based transactions
- Provision PIV credential and credential-holder to local access registry store for continued access
- Enable additional functionality like:
    - Authenticating credentials that do not contain PKI material
    - Provide other attributes (e.g. picture and biometrics data) for further validation
    - Provide for visit request process and security clearance validation

The Backend Authentication Scheme Work Group (BAS WG) proposed a series of recommendations that included methods and technologies for the delivery of back-end information requested by reliant parties. Two general methods were described: 1) the use of certificate revocation lists (CRL) in conjunction with on-line certificate status protocol (OCSP); 2) the use of a secured backend gateway infrastructure.

Reliant parties are to use certificate revocation lists (CRL) in conjunction with on-line certificate status protocol (OCSP) to check the revocation status of PIV certificates. The primary focus is logic access (operating web-applications/networks). Whereas, the gateway approach's primary focus is physical security/installation management community. The gateway approach is also recommended for enabling the other capabilities listed above for both physical and virtual environments. Those reliant parties and card issuers that need to share information, either of a privacy nature (e.g. personal\personnel information for local credential registry) or information whose update by the issuer does not require a certificate revocation (e.g. clearance or NAC-I), are encouraged to fully understand the capabilities of the gateway scheme.

This document is a framework for backend transactions through gateways. We have purposely omitted finite information needed to actually implement a solution. The Homeland Presidential Directive 12 Executive Steering Committee's (ESC) Architecture Work Group (AWG) will create an interface specification utilizing this framework. The

[1] There are several investigations which are greater in scope than the NAC-I. These investigations are conducted on Federal employees and support contractors upon hiring, and also meet the requirements of HSPD-12

interface specification is expected to contain details associated with transport protocols, authentication schemes, operating rules, file sizes, and such.

This document is informative and elective.

1.1. Backend Authentication via a Gateway Approach

The Visa credit card model is often cited as an example of establishing backend transactions. A Visa card is not used by commercial relying parties, even for the smallest purchase, without being validated by a backend system. This is not just to check the account balance but it is also to ensure that:

- The card is valid
- The account has not been terminated
- The card has not been reported lost or stolen

What is not done by this backend process, as most credit cards today, is the verification of the cardholder. This is done locally either by using another credential (with a photograph) or by a signature comparison. With the Federal PIV credential technology, as currently defined, both verification of card and cardholder can be performed. The cardholder can be verified locally using the PIN or the on card biometrics (including fingerprint and photograph). However the card itself, even if determined authentic locally, is only as valid as it was when it was issued. This means that, like the credit card, any change in status of the person holding the card or of the card itself will not be found with a local check for validity.

A backend authentication service can do both card and cardholder validation while its primary value (given that the onboard PIN and biometrics are secure and can be used by the relying party) is in making sure that what is being declared on the credential has not changed. For example, it can confirm the following information has not changed:

- The affiliation of the person to the Federal government
- The basic role that the person performs within it (i.e. employee, contractor) or
- The trustworthiness of the cardholder and the credential (based on conditions that may have changed since issuance).

However, there are conditions in which it is difficult for an agency to physically get the card back when the person carrying it terminates employment. Card Expiration dates are never precise as to when a person will terminate their employment and thus the card will appear valid for a period of time after it is no longer valid. Further, lost or stolen cards will in most cases never be found and returned/destroyed. This means that while a card may look valid and may check out valid using local validation technologies, the person may no longer be authorized to carry the card or the card may have been centrally invalidated.

High assurance usage of a credential therefore requires a check for validity and authenticity to the credential issuer or maintainer of backend system. This backend authentication and validation within the Federal PIV initiative may take three general forms:

1. Simple validation of the credential, returning only a yes or no as to authenticity and validity. An example of this is the Certificate Revocation List (CRL) employed by PKI which returns only revoked/ not revoked as a response.
2. Validation along with some credential holder authentication information. For example, returning a photograph or providing a fingerprint match.
3. Return conditions or restrictions placed on the credential (e.g. the current PIV condition of “interim” for cards issued before NAC-I completion)

It is assumed that all backend transaction will require communications to successfully execute the web-based transactions. This document does not address offline capabilities.

2. Capabilities

There are four primary capabilities a backend check could fulfill:

1. Obtain Status changes such as terminations or lost or stolen status of a PIV card
2. Obtaining information that may have changed since issuance (as with "interim" status based on the NAC-I for PIV being changed to completed)
3. Provide centrally stored authentication information to validate the cardholder (server-based fingerprint match or photograph for visual examination)
4. Obtain additional information for registry on local access systems (e.g. the reference biometrics and the demographics)

The following is a list of capabilities that need to be met in order for secure and reliable inter-agency and intra-agency backend authentication of the PIV card:

- Any change in the status of a PIV card holder as represented in the Cardholder Unique ID (CHUID) or, more specifically, the Federal Agency Smart Credential Number (FASC-N) will cause a PIV credential issuance/maintenance system to terminate the token. Similar organizational and association data (i.e. FASC-N) stored in the PIV authentication certificate also requires revocation on change.

- It must be assumed that on authentication of a PIV card the following information about the cardholder is also being confirmed
  - the cardholder’s agency (e.g. the Organization Identifier in the FASC-N of the CHUID and in the PIV PKI authentication certificate)
  - the cardholder’s role within that organization (e.g. contractor, civilian employee) as represented in the Person /Organization Association Category in the FASC-N for the CHUID and in the PIV authentication certificate

- A common set of information that needs to be stored by the agency from the agencies issuance and personnel registry/maintenance process will need to be specified. This may include:
  - FASC-N (from either the CHUID or certificate)_
  - Fingerprints in Federal Information Processing Standard (FIPS) 201 standard format (both image and minutia)
  - Photograph in FIPS 201 standard format
  - An agency employee ID (as represented by the Person ID on the FASC-N)
  - Person ID (used only for local registry transactions)
  - Person ID type Code (SSN, Foreign National ID etc.,)
  - Person Last Name
  - Person First Name
  - Person Middle Name
  - Person Cadency
  - Person Sex Code
  - Person Date of Birth
  - Card issuance and card expiration
  - NAC-I status information (open/closed)

- A means for returning the status of the credential with a reason for termination if applicable (lost or stolen, personnel termination, data change, suspension)

- While it is anticipated that the certificates can be validated via the CRL/OCSP option stated in the overview there may be situations where these may not be network accessible between specific agencies, therefore if the X509 PIV authentication certificate is included in the message the gateway could be used for this purpose as well.

- A standard set of messages for inquiry and response containing the above information must be proposed
  - Messages should be in real-time mode between connected systems
  - When systems are not connected the message requirements depend on the relying party's agency policy.
  - When systems connectivity again becomes available, all messages made in non-connected mode will be processed and all new messages proceed in connected mode.

- A secure means of transporting these messages must be devised

- An infrastructure schema to route these messages to and from the appropriate agencies must be created

- A standard interface for each agency to connect to this infrastructure must be proposed

- Authentication should be performable on PIV cards both inside an agency (intra-agency) and outside an agency (inter-agency) from relying client applications

- An audit trail should be kept by each backend system containing basic information on the PIV inquiry (i.e. when it took place and from what system/user)

- Redundancy and fail-over capability should be provided within the systems

This guide outlines ways in which all of the above capabilities can be implemented.

3. Authentication Methods using the Gateway Approach

In addition to the PIN and certificate validation services (e.g. CRL and OCSP), there are other ways PIV cards can be authenticated. They are as follows:

3.1 Validate of the PIV card via the FASC-N from the Authentication Certificate or the CHUID

The FASC-N may be transmitted to the issuing agency to check if it is valid. At a minimum, the issuing agency will reply with a valid/not valid response and additional information as applicable (e.g. terminated due to lost or stolen, suspended). Also, the agency may return a cardholder facial image for visual verification; perform a server-side comparison of a captured fingerprint with the reference prints, and\or return demographic information for local registry of the cardholder.

The FASC-N, obtained from the contact or contactless chip's CHUID or from the authentication certificate, will represent a key in finding the cardholder and card related information from the agencies central issuance system or IDMS. In addition, once it is stored in a local registry data store, the FASC-N can provide a means to periodically verify the continued validity of the PIV card and PIV cardholder that is registered for access against the backend system.

3.2 Cardholder Validation with Biometrics

There are three methods available for fingerprint verification.

1. The cardholder gives a live sample at a biometric reader followed by Match on Card (MOC).
2. The live capture along with the FASC-N can be transmitted to the issuing agency for match on server verification.
3. The cardholder gives a live sample that is compared to the biometric retrieved from the PIV and match within the biometric reader or workstation.

Above method #2 involves the gateway. Additionally, a facial image, while not always tailored for biometric facial recognition, should also be available either on the card or from the issuing agency.

3.3 Backend Authentication Use cases for the Gateway

Assume the following usage capabilities:

1. Backend authentication for validation of PIV card. This gives a relying party the ability to check that the card itself is valid and current according to the issuer of the card.

   - Pass FASC-N from the CHUID or authentication certificate to Issuer.
   - Response verifying the validity of the card

2. Backend authentication for validation of a PIV certificate on the card. This gives a relying party the ability to check that the certificate on the card is still valid if the CRL or OCSP of the target agency is not accessible.

   - Pass FASC-N and the x509 certificate from authentication certificate to Issuer.
   - Response verifying the validity of the credential

3. Backend authentication for validation of non-PIV cards. This gives a relying party the ability to check that the card itself is valid and current according to the issuer of the card.
   - Pass common FASC-N or other unique information from barcodes/magnetic stripe or select issuing organization from list for authentication and enter an employee id to send to Issuer.
   - Response verifying the validity of the card

4. Backend authentication for validation of PIV card and card holder. This gives a relying party the ability to check that the card and the cardholder are valid and current according to the issuer of the card

   - Pass FASC-N from the CHUID or authentication certificate and fingerprint to Issuer
   - Response verifying the validity of the card and cardholder
   - Pass FASC-N from the CHUID or authentication certificate with a photo request to the issuer
   - Response verifying the validity of the card which contains the Photograph for visual verification

5. Backend transactions for local registration. This provides required issuer stored personal information regarding the person requesting local registration.

- Pass FASC-N from the CHUID or authentication certificate) and request information about the card holder and receive current information from the issuer in the response.

4. A Backend Authentication Reference Architecture

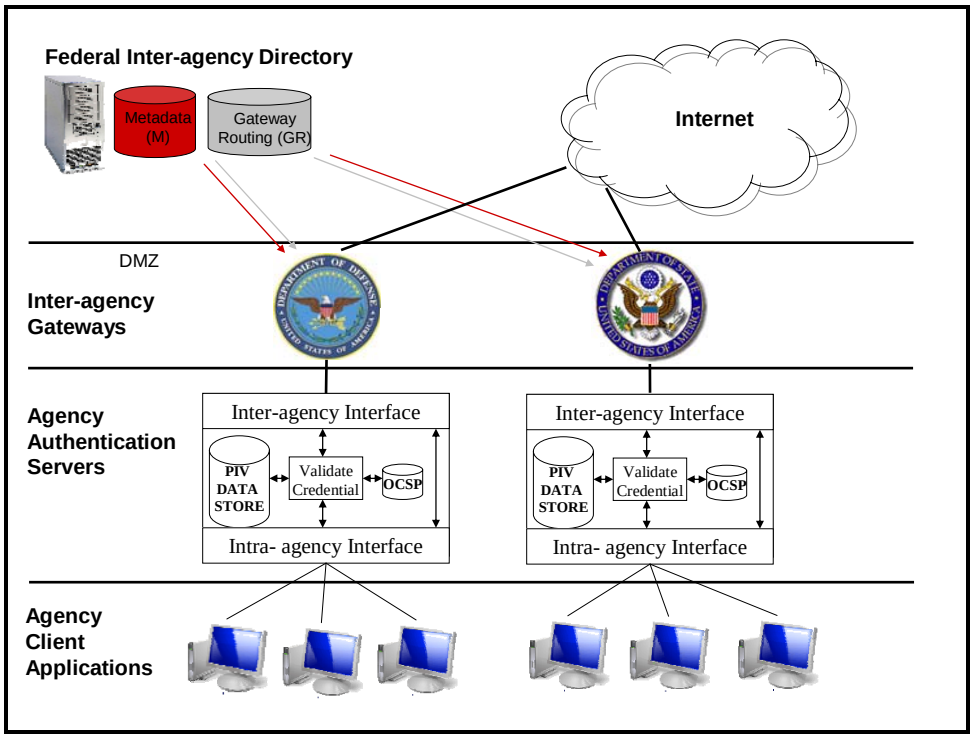

Figure 1- Reference Architecture

The basic operational components of the above diagram are:

- **Federal Interagency Directory:** centrally available to obtain metadata and routing data applicable to interagency communications and security
- **Interagency Gateways:** secure message routing and internal network security (these may be optional depending on interagency connectivity)
- **Agency Authentication Servers:** physical entities that contain information to authenticate agency issued PIV cards. They contain the following components
  - **PIV Data Store:** a repository of authentication information generated from the registry maintenance and card issuance systems within the agency
  - **Inter-agency Interface:** creates authentication inquiries and receives authentication results from other agencies
  - **Validate Credential:** the internal service that uses both the agency PIV data store or an OCSP responder to authenticates agency PIV credentials
  - **OCSP:** responder to validate agency X.509 credentials when OCSP or CRL is not available outside agency
  - **Intra-agency Interface:** connects with the internal clients to process intra and inter-agency PIV validation. This can be browser based or operate as an Extensible Markup Language (XML) or Security Assertion Markup Language (SAML) service interface

- **Agency Client Applications -** simple web browsers or host systems for authorizing physical or logical access.

Messages
- As processed by the Inter-Agency Interface to pass via the **Inter-agency Gateway** to the internet – source agency signed and destination agency encrypted SAML messages.
- As processed by the **Intra-Agency Interface** to the Agency Client applications - browser based HTTPS or SAML messages.

Connections
- The connections between the Interagency Gateways can be secured in a variety of ways (mutually authenticated SSL, VPN, etc.,)
- The most important aspect of this security (since the message payload will already be encrypted) is that a gateway can trust that the message was sent by another trusted gateway

4.1 Federal Agreement for Use of Federated Interagency Directory

All Federal agencies and/or entities using the Federated Inter-agency Directory, attached to the backend authentication architecture for the Federal PIV System (outlined within this document and above), MUST notify their PIV applicants and cardholders that the information (as outlined in this document—section 4.4.2 table 1—and obtained in the enrollment and issuance of their PIV cards) can be shared with other government organizations. This information may be shared to assist in authenticating the validity of their PIV cards and/or processing applications and validating eligibility for other Federal credentialing programs.

Participating federal agencies and/or entities are expected to codify the information sharing agreement associated with the use of the Federal Inter-agency Directory in the proper Privacy Act Statements, Privacy Act System of Records Notices (SORNs), and/or Privacy Impact Assessments.

4.2 Components

The sections below provide additional information on the different components of the reference architecture. It is worth noting that there is only one component that is required to successfully hold up the architecture. This component is the **Federal Interagency Directory**. This must be implemented. At this time, it remains unclear who will be responsible for operating this portion of the architecture for the long term; however, the Department of Defense (i.e. Defense Manpower Datacenter (DMDC)) has offered to host it until a permanent home agency can be found

4.2.1 Interagency Gateways

For each agency or group of agencies, interagency gateways represent:

- Platforms to connect to outside organizations and networks securely.

- Routers to send messages to and from the appropriate Interagency Gateway.

These platforms would be used for all communications to external entities for backend authentication to and from any other Federal agency. It would be common point of inter-agency connectivity and communication within this reference architecture. The platforms would be web servers\routers within the organizations Demilitarized Zone (DMZ), which would reside between an agency's internal trusted network and the internet (as a non-trusted external network). Additionally, the component may not be necessary if the agency determines that they wish to communicate directly from their Inter-Agency Interface which may also be as simply as a router for supporting Virtual Private Networks (VPN) between the agencies.

4.2.2. Federal Interagency Directory

The primary directory components for a flexible backend authentication of credentials are:

- A standard organizational identifier to identify the credential issuer/authority
- A way to use the organizational identifier to find a destination (address) on the internet where the backend authentication system for that organization can be found
- A means of securing the authentication request message between the sender and receiver

As indicated above, this is the sole required component.

4.2.2.1 Metadata Directory

The metadata purpose is to direct and secure traffic between the agencies. It consists of:

- The ORGANIZATION CATEGORY and IDENTIFIER as defined by PIV in the FASC-N of the credentials CHUID or authentication certificate to discover the agency that issued the credential
- Unique Identifiers for the INTERAGENCY GATEWAY server that are associated to that ORGANIZATION CATEGORY and IDENTIFIER to use in routing the messages
- A public key from an asymmetric key pair created by each ORGANIZATION that can be used for securing the message by:
    - Verifying the signature of the sending agency
    - Encrypting the payload to the receiving agency

4.2.2.1.1 Organizational Category and Organizational Identifier

The portion of the CHUID or authentication certificate on a PIV that can be used for backend authentication is called FASC-N. It is flexible, extensible, and can be used not only for Federal agencies but eventually, if required, for State, Commercial, and Foreign countries.

Table I-Organizational Information

Field Name	Abbreviation	Length (BCD digits)
Organizational Category	OC	1
Organization Identifier	OI	4

The above portion of the FASC-N can be parsed by a relying party to identify the

- Category of organization (for Federal agencies "1")
- The Special Publication (SP) 800-87 based Organizational code of the Federal agency whose employees and contractors were issued the PIV card

This information, parsed from the CHUID on the PIV card, can be passed against the metadata directory by the Interagency Interface component to:

- Find the correct Interagency Gateway id (for routing)
- Obtain the agencies public key for encrypting the message payload

4.2.2.1.2 Inter-Agency Gateway Identifier

The inter-agency gateway identifier is:

1. Placed in the header area of the SAML message by the inter-agency interface
2. Used by the senders Interagency Gateway against the Routing Directory to locate the network address of the authenticators Inter-agency Gateway

This construct allows for the payload of the message (other than the header information) to be signed and encrypted before being sent to the Inter-agency Gateway in the DMZ by the Inter-agency Interface (within the trusted network). In this way, all that needs to be exposed, both in the DMZ and to the internet, is the Gateway ID (to and from) and address information.

4.2.2.1.3 Agency Public Key

In order to secure the messages, it is proposed that some form of standard asymmetric cryptography be used. Each agency will be asked to generate a key pair and to supply the public key to the Inter-agency Directory for use in verifying a signed message and in encrypting the message payload so that only the intended agency can see the message content

4.2.2.2 Routing Directory

Routing the message traffic is a matter of using the Routing Directory that holds the address (IP or URL) for each Inter-agency Gateway ID within the Inter-agency Federation.

4.2.3 Agency Authentication Servers

These are platforms where the authentication and validation of the credentials are performed against the PIV data store or the agency OCSP responder, which both hold an agency's credential authentication information.

4.2.3.1 Inter-agency Interface

This is primarily a protocol conversion service that provides two basic capabilities:

- Create SAML inquiries to send to other agencies. It is also here that the payload of the outgoing SAML messages are signed and encrypted before being passed to the Gateway
- Parse SAML inquires and responses from other agencies. Here the incoming message is decrypted (using the agencies private key) and signatures are verified (using the public key from the Metadata)

4.2.3.2 Intra-agency Interface

This is a service layer to the Agency Application Clients to accept authentication requests that are both inter and intra- agency. This service may take two forms:

- As a web server application that provides a browser interface to clients that request authentication of a provided PIV card (e.g. a security check point application)
- As an interface that accepts messages from an internal host system or application (e.g. a physical or logical access system requesting authentication)

4.2.3.3 Validate Credential

This is a service that processes PIV credentials (FASC-N or X509 certificate) and matches biometric images against the stored reference prints by accessing internal agency resources (e.g. PIV Data Store, OCSP Responder and a biometrics match service). This service accepts requests originating from both:

- The Intra-agency Interface (for requests on cardholders within the current agency)
- The Inter-agency Interface (for authentication inquires from other agencies)

4.2.3.4 PIV Authentication Data Store

This data store is created from two business systems within the agency as defined in PIV 1; the personnel registry system and the issuance system. These systems supply information to the data store:

- On PIV Issuance - the registry system can provide the basic personnel and demographic information along with the biometrics. The issuance system can provide the created CHUID and the certificate information

- On Personnel Action – the registry system can perform maintenance activity on the data store that may result in credential termination.
- On PIV credential maintenance or security events – the issuance system can perform credential terminations due to re-issuance, card loss or stolen cards

Reference Model for basic PIV Data Store

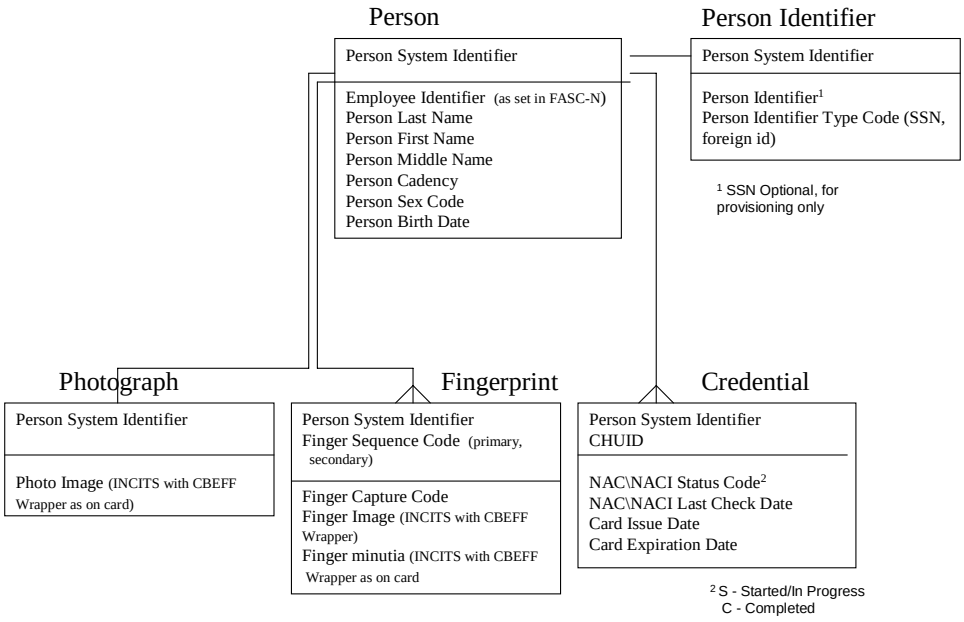

Figure 2- PIV Data Store

4.2.3.5 OCSP Responder

This is a data store that is used to capture certificate revocation lists issued by the agencies Certificate Authority (CA) directory. It could also be a simple flat CRL, if required. OCSP responder will respond to an inquiry of the revocation status of the X.509 certificate being sent. The answer will detail whether the credential is on the CRL list and is therefore revoked.

Revocations on this are based on maintenance to the certificates from the:

- The issuance system
- The registry system
- Manually by persons designated as Registration Authority (RA)

It is essential that the certificate is revoked if the person, or card they carry, are terminated or compromised. Larger agencies, based on volume, will need to develop

some form of connection between their issuance system, registry system and CA in order to send revocations when PIV cards are terminated due to personnel action, or lost or stolen cards. For smaller agencies, this may be done manually by the RA.

4.2.4 Agency Desktop/Client Applications

These are the applications that represent relying parties that:

1. Require PIV card authentication and validation so that the credentials can be used for logical or physical access.
2. Require central registry information in order to locally register a PIV card holder for continued access.
3. Required continued confirmation of validity of locally registered PIV card information based on possible changes in personnel or credential status.

4.2.4.1 Example 1 - Browser based Application at Security desk or checkpoint

A Browser-based web application operated by a security officer checking visitors PIV credentials. In this case the contact or contactless portion of the card could be used to obtain the CHUID. The FASC-N from the CHUID is, in turn, sent to the Inter-Agency Interface (a web service application in this case) for validation of the PIV card. This inquiry is sent by Intra-Agency Interface to the Inter-Agency Interface (if it is a PIV card outside the applications agency) or is processed within the Agency's server (if it is within the agency). A basic successful/ not successful answer can be returned to the operator. In addition, biometric information could be employed to centrally authenticate the card holder as well. This could take the form of a photograph being sent down with the response and/or the fingerprint being extracted and then sent and matched against the reference print on the agency's PIV data store.

An application following this basic schema (the Defense National Visitor Center (DNVC)) was developed by the DoD some years ago for authentication of their ID cards (including the Common Access Card or CAC) and that software could be made available as a reference other Federal agencies

4.2.4.2 Example 2 - Host to Host - Real-time authentication and provisioning

This can be an XML or SAML-based web service in the Intra-Agency Interface. This service will respond to requests from another system to authenticate a PIV credential and provide data for local registry from the PIV Data store. The client system could be a physical or logical access system requiring some local registration information in order to build an authorization entry in its local store.

An application following this schema was developed by the DoD (Defense Personnel Registry Service (DRPS)) for use by local and regional physical access systems including the Defense Biometric Identity System (DBIDS) and the Navy's Central Access System (ENABLER). This interface provides authentication of the DoD ID cards (including the CAC) and provisions central registry information to the local store so that

registry data such as fingerprint and photograph are consistent across the DoD enterprise. This application could be used as a reference by other PIV agencies.

4.2.4.3 Example 3 - Host to Host - Continued Validation of a locally registered PIV credential

This could also be an XML or SAML based web service in the Intra-Agency Interface responding to requests from or actually pushing updates to local registry systems from the PIV Data store about:

- Personnel actions - credential terminations based on employee termination, retirement or death
- Card re-issuance - credential termination and re-instatement of the new credential
- Security issues - like lost or stole credentials

The clients system could be a physical or logical access system that has already locally registered and stored the PIV credential employing the Example 2 Host to Host application.

An application that is based on request/response was developed by the DoD (Defense Token Revocation Service (TRS)) for use by local and regional physical access systems including the Defense Biometric Identity System (DBIDS) and the Navy's Central Access System (ENABLER). This interface provides continued validity confirmation, security alerts for lost or stolen cards and re-issuance information about DoD ID cards (including the CAC). This web service could be used as a reference by other PIV agencies.

4.3 Process Flow

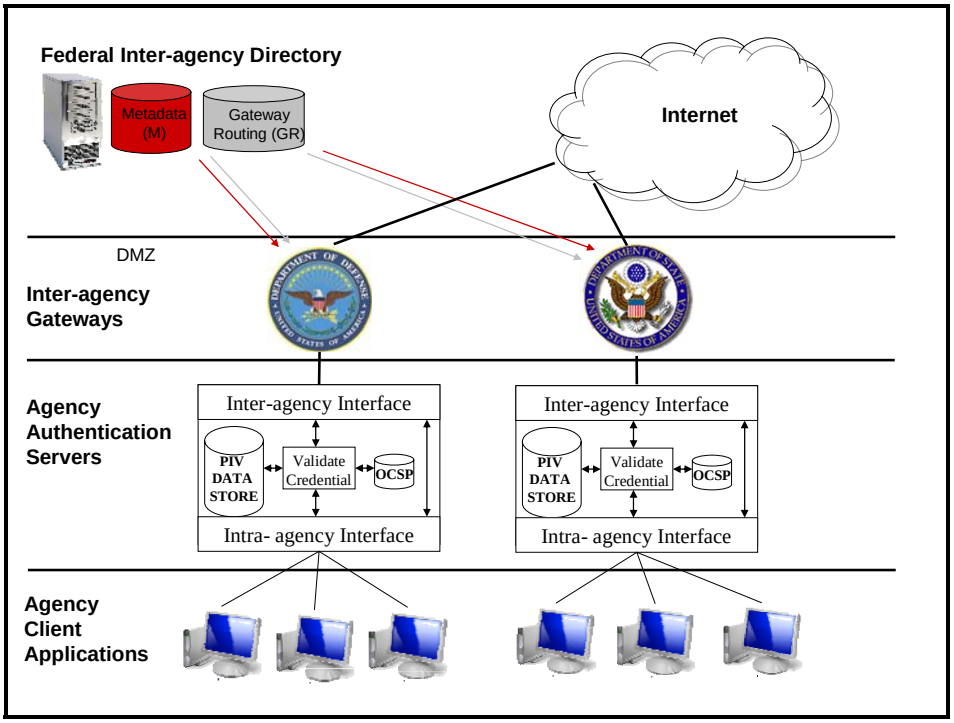

Figure 3- Figure 1 Repeated

4.3.1 Intra-Agency Authentication Traffic

Starting with the Agency Client Application inquiry that carries the PIV credential

1. Once the Intra-agency Interface receives the CHUID or the X509 certificate from the Agency Application Client it will examine it to obtain the Organization Category and ID
2. Based on a discovery that the Organization ID is an internal agency the interface calls the Validate Credential Service which either uses the PIV data store or the OCSP responder.
3. The response is then returned to the Intra-agency interface and then displayed or sent to the client

4.3.2 Inter-Agency Authentication Traffic

Starting with the Agency Client Application inquiry that carries the PIV credential

1. Once the Intra-agency Interface receives the CHUID or the authentication certificate from the Agency Application Client, it will examine it to obtain the Organization Category and ID from the FASC-N

2. Based on a discovery that the Organization ID it is NOT the internal agency, the interface passes it to the Inter-agency Interface with some type of session ID that will follow the message until it is returned in order to match up the request from the client to the response coming back. This session ID may (in the Inter-Agency Interface) be incorporated into or cross referenced to a SAML message session specific ID.
3. The Inter-agency Interface will then use the metadata directory information obtained from the Inter-agency directory to find the correct Interagency Gateway ID
4. A message will now be created for transmission through the Gateway as follows:
    a. A message header is created that contains both the Inter-agency Gateway ID (from the metadata) of the destination and the Senders Gateway ID (for use in the returned response)
    b. The payload is now created with the inquiry information (FASC-N and possibly the X509 certificate or captured biometric image)
    c. A hash of the payload is now signed using the sending agencies private key
    d. Then the payload is encrypted with the destination agencies public key (obtained from the metadata)
5. The message is now given to the senders Interagency Gateway where, using the destination Interagency Gateway ID, it looks up the address in the routing director and sends the message
6. On receipt of the message by the destinations Interagency Gateway, it ensures that the sender is an authentic and trusted inter-agency gateway.
7. The message is then sent to the Inter-Agency Interface service which:
    a. Decrypts the message payload using its private key
    b. Obtains the public key of the sender (using the senders Gateway ID in the header and the metadata directory) to confirm the signature
    c. Parses the message and sends the credential to the Validate Credential service
8. The Validate Credential service either uses the PIV data store or the OCSP responder depending on the credential sent. It will then, based on the request and the result, return whatever information is required back to the Inter-Agency Interface.
9. A message will now be created for transmission back through the Gateway as follows
    a. A message header is created that contains both originating Interagency Gateway ID (from the original senders message header) and this agency's Gateway ID along with whatever session persistence information that was originally sent
    b. The payload is now created with the information being returned
    c. A hash of the payload is now signed using this agency's private key
    d. Then the payload is encrypted with the destination agency's public key (from the metadata)
10. The message is now given to the senders Interagency Gateway where, using the new destination Interagency Gateway ID, it looks up the return address in the routing directory
11. On receipt of the message by the destination Interagency Gateway, it ensures that the sender is an authentic and trusted inter-agency gateway
12. The message is then sent to the Inter-Agency Interface service which:

a. Decrypts the message using its agency private key
b. Obtains the public key of the sender (using the senders ID in the header) to confirm the signature
c. Parses the message and sends the information with the original session ID back to the intra-agency Interface for return to the client

4.4 Message Transactions Format and content

4.4.1 Application of SAML for the PIV

The basic requirements for the PIV make SAML a logical design choice for exchanging security information between Federal agencies. SAML provides a standard request/response framework for communicating identity and affiliation of persons carrying Federal ID cards. It also uses standard security technologies to protect this communication. Given these standards, the implementation of SAML for the PIV will still require the publication of a standard for using it among the Federal agencies. The following points require such coordination:

- **Implementation guidelines** - for integrating the SAML interface into an agency's identity management infrastructure. This infrastructure might include a Federal ID card issuance center, an authentication server, and/or an authorization server. These systems might also be linked to systems controlling physical access to Federal agency facilities.
- **Security** - Common solution for security, including web services security and PKI infrastructure.
- **XML schema** – The format of the schema must be defined. The identifiers or tags for a subject (such as Person Last Name) and his valid identity credentials (such as a digital certificate) and many other tags must be defined.

4.4.2 Transaction Pair Format

The request/response transactions between agencies shall be formatted as standard SAML requests and assertions. The SAML requests will be of the Subject Query and Attribute Query types. See appendix A for SAML examples of a request and response for each transaction use case.

The information transmitted in these transactions shall include a STANDARD set of attributes. These attributes must be maintained by each agency that issues cards. The following are examples of standard attributes that can be used in request/response transactions.

Table 2- Personal Information Attributes

Attribute Names	Attribute Description	Format
FASC-N (required)	card, organization, role and person identifier.	String, Length Variable
PN_ID	Person Identifier	0x05 30 Var T
PN_ID_TYP_CD	Person Identifier Type Code (S - SSN F - foreign national ID)	0x08 2 F A
PN_1ST_NM	Person first name	String, Length variable
PN_LST_NM	Person last name	String, Length variable
PN_MID_NM	Person middle name	String, Length variable
PN_CD_NM	Person Cadency Name	0x04 8 Var A
PN_SEX_CD	Person sex category code	String, Length 1 M, F
PN_BRTH_DT	Person birth date	YYYY/MM/DD
PN_CITIZENSHIP_COUNTRY CODE	FIPS Country Code	String: length 2
PHT_IMG	Person photo image	INCITS wrapped in CBEFF header
FNGR_CPTR_DT	Person fingerprint capture date	YYYY/MM/DD
FNGR_CPTR_CD	Person fingerprint capture code (indicates which finger)	String: Length 1
FNGR_IMG	Person fingerprint image	500 dpi bitmap file
FNGR_MTA_IMG	The image of the minutiae (finer details) of a person's fingerprint.	340 dpi (256x255) .min file INCITS wrapped in CBEFF header
CRD_ISS_DT	Identification Card Issue Date	0x62 8 F N
CRD_EXP_DT	Identification Card Expiration Date	0x63 8 F N
CRD_TERM_DT	Identification Card Termination Date (if applicable)	0x63 8 F N
CRD_TERM_RSN_CD	Identification Card Expiration Reason	String length 1 Blank if not applicable L - lost or stolen P - personnel action (separation, death etc.,) C- Credential information change S – credential

Attribute Names	Attribute Description	Format
		suspension
NACI_STAT_CD	NAC-I Status Code	String length 1 F - Fingerprint results returned from FBI O - NACI opened C - NACI Completed
X509_CERT	Attribute containing the properties of the digital certificate as XML. (only if cert is being checked)	String, Length variable

Reference NIST Special Publication 800-73-1

4.4.3 Transaction Example Use Cases

4.4.3.1 Validation Transactions

1. Request Issuer to validate by passing a FASC-N from the CHUID or X.509 certificate from the card.

2. Request Issuer to validate by passing a FASC-N from the CHUID or X.509 certificate and a fingerprint from the card.

3. Request Issuer to validate by passing a FASC-N from the CHUID or X.509 certificate and receiving back a photo of the cardholder.

4.4.3.2 User Provisioning Transaction

This standard set of personal information shall be used for provisioning a user at the time of local registration.

1. Request Issuer to pass current person information about the PIV cardholder for a registration process

Appendix A - Examples of Transaction Use Cases Using SAML

A1. Request Issuer to validate a PIV card by passing a FASC-N from the card.

Request

```
<SAMLQuery xsi:type=”samlp:SubjectQueryAbstractType""">
        <Subject>
                <NameIdentifier>
                        <SecurityDomain>www.agency1.gov</SecurityDomain>

                        <FASCN>11111222333333456666666666667888890000</FASCN>
                </NameIdentifier>
        </Subject>
</SAMLQuery>
```

Response

```
<SAMLResponse ResponseID=“{HR90GJFF-3452-4ebe-84D3-4D372C892A5D}”
InResponseTo= “{EE52CAF4-3768-4ebe-84D3-4D372C892A5D}”
Version=“0100”
StatusCode=“Success”>
        <Assertion xsi:type=“saml:SubjectAssertionType”
        version=”http://www.oasis.org/tbs/1066-12-25/”
        AssertionID=”{EE52CAF4-3452-4ebe-84D3-4D372C892A5D}”
        Issuer="www.agency1.gov"
        IssueInstant="2004-02-26T11:10:17.795Z">
                <Conditions NotBefore="2004-02-26T11:05:17.795Z"
                NotOnOrAfter="2004-02-26T11:15:17.795Z"/>
                <Subject>
                        <NameIdentifier
                                <SecurityDomain>www.example.com</SecurityDomain>
                                <CHUID>11111222333333456666666666667888890000</CHUID
                                >
                        </saml:NameIdentifier>
                <Subject>
</saml:Assertion>
```

A2. Request Issuer to validate a X509 certificate by passing a FASC-N from the certificate and the certificate.

Request

```
<SAMLQuery xsi:type=”samlp:SubjectQueryAbstractType""">
        <Subject>
                <NameIdentifier>
                        <SecurityDomain>www.agency1.gov</SecurityDomain>

                        <FASCN>11111222333333456666666666667888890000</FASCN>
                        <X509_CERT>===</X509_CERT>
                </NameIdentifier>
        </Subject>
```

```
</SAMLQuery>
```

Response

```
<SAMLResponse ResponseID=“{HR90GJFF-3452-4ebe-84D3-4D372C892A5D}”
InResponseTo= “{EE52CAF4-3768-4ebe-84D3-4D372C892A5D}”
Version=“0100”
StatusCode=“Success”>
        <Assertion xsi:type=“saml:SubjectAssertionType”
        version=”http://www.oasis.org/tbs/1066-12-25/”
        AssertionID=”{EE52CAF4-3452-4ebe-84D3-4D372C892A5D}”
        Issuer="www.agency1.gov"
        IssueInstant="2004-02-26T11:10:17.795Z">
                <Conditions NotBefore="2004-02-26T11:05:17.795Z"
                NotOnOrAfter="2004-02-26T11:15:17.795Z"/>
                <Subject>
                        <NameIdentifier
                                <SecurityDomain>www.example.com</SecurityDomain>
                                <CHUID>111122223333334566666666667888890000</CHUID
                                >
                                <X509_CERT>===</X509_CERT>
                        </saml:NameIdentifier>
                <Subject>
</saml:Assertion>
```

A3. Request Issuer to validate a PIV card by passing a FASC-N and a captured fingerprint.

Request

```
<SAMLQuery xsi:type=”samlp:SubjectQueryAbstractType””>
        <Subject>
                <NameIdentifier>
                        <SecurityDomain>www.agency1.gov</SecurityDomain>
                        <FASCN>111122223333334566666666667888890000</FASCN>
                        <FNGR_IMG>===</FNGR_IMG>
                </NameIdentifier>
        </Subject>
</SAMLQuery>
```

Response

```
<SAMLResponse ResponseID=“{HR90GJFF-3452-4ebe-84D3-4D372C892A5D}”
InResponseTo= “{EE52CAF4-3768-4ebe-84D3-4D372C892A5D}”
Version=“0100”
StatusCode=“Success”>
        <Assertion xsi:type=“saml:SubjectAssertionType”
        version=”http://www.oasis.org/tbs/1066-12-25/”
        AssertionID=”{EE52CAF4-3452-4ebe-84D3-4D372C892A5D}”
        Issuer="www.agency1.gov"
        IssueInstant="2004-02-26T11:10:17.795Z">
                <Conditions NotBefore="2004-02-26T11:05:17.795Z"
                NotOnOrAfter="2004-02-26T11:15:17.795Z"/>
                <Subject>
                        <NameIdentifier
                                <SecurityDomain>www.example.com</SecurityDomain>
```

```
                    <FASCN>1111222233333345666666666667888890000</FASC
                    N>
                </saml:NameIdentifier>
            <Subject>
</saml:Assertion>
```

A4. Request Issuer to validate a PIV card by passing a FASC-N and receiving back a Photo of the Cardholder.

Request

```
<SAMLQuery xsi:type=”samlp:AttributeQueryType”>
    <Subject>
        <NameIdentifier>
            <SecurityDomain>www.agency1.gov</SecurityDomain>
            <FASCN>1111222233333345666666666667888890000</FASCN>
        </NameIdentifier>
    </Subject>
    <CompletenessSpecifier>ANY</CompletenessSpecifier>
    <Attribute>
        <AttributeName>PHT_IMG</AttributeName>
        <AttributeNamespace> http://example.gov</AttributeNamespace>
    </Attribute>
</SAMLQuery>
```

Response

```
<SAMLResponse ResponseID=“{HR90GJFF-3452-4ebe-84D3-4D372C892A5D}”
InResponseTo= “{EE52CAF4-3768-4ebe-84D3-4D372C892A5D}”
Version=“0100”
StatusCode=“Success”>
    <Assertion xsi:type=“saml:AttributeAssertionType”
    version=”http://www.oasis.org/tbs/1066-12-25/”
    AssertionID=”{EE52CAF4-3452-4ebe-84D3-4D372C892A5D}”
    Issuer="www.agency1.gov"
    IssueInstant="2004-02-26T11:10:17.795Z">
        <Conditions NotBefore="2004-02-26T11:05:17.795Z"
        NotOnOrAfter="2004-02-26T11:15:17.795Z"/>
        <Subject>
            <NameIdentifier
                <SecurityDomain>www.example.com</SecurityDomain>
                <FASCN>1111222233333345666666666667888890000</FASC
                N>
            </saml:NameIdentifier>
        <Subject>
        <Attribute>
            <AttributeName>PHT_IMG</AttributeName>
            <AttributeNamespace> http://example.gov</AttributeNamespace>
            <AttributeValue>===</AttributeValue>
        </Attribute>
    </Assertion>
</SAMLResponse>
```

A5. Request Issuer to pass current person information about the PIV Cardholder for a Registration Process.

Request

```
<SAMLQuery xsi:type=”samlp:AttributeQueryType”>
        <Subject>
                <NameIdentifier>
                        <SecurityDomain>www.agency1.gov</SecurityDomain>
                        <FASCN>11112222333333456666666666667888890000</FASCN>

                </NameIdentifier>
                <CompletenessSpecifier>ANY</CompletenessSpecifier>
                        <Attribute>
                                <AttributeName>Person_Data</AttributeName>
                                <AttributeNamespace>
                                http://example.gov</AttributeNamespace>
                        </Attribute>
        </Subject>
</SAMLQuery>
```

Response

```
<SAMLResponse ResponseID=“{HR90GJFF-3452-4ebe-84D3-4D372C892A5D}”
InResponseTo= “{EE52CAF4-3768-4ebe-84D3-4D372C892A5D}”
Version=“0100”
StatusCode=“Success”>
        <Assertion xsi:type=“saml:AttributeAssertionType”
        version=”http://www.oasis.org/tbs/1066-12-25/”
        AssertionID=”{EE52CAF4-3452-4ebe-84D3-4D372C892A5D}”
        Issuer="www.agency1.gov"
        IssueInstant="2004-02-26T11:10:17.795Z">
                <Conditions NotBefore="2004-02-26T11:05:17.795Z"
                NotOnOrAfter="2004-02-26T11:15:17.795Z"/>
                <Subject>
                        <NameIdentifier
                                <SecurityDomain>www.example.com</SecurityDomain>
                                <FASCN>11112222333333456666666666667888890000</FASC
                                N>

                        </saml:NameIdentifier>
                <Subject>
                <Attribute>

                        <AttributeName>Person_Data</AttributeName>

                        <AttributeNamespace> http://example.gov</AttributeNamespace>

                        <AttributeValue>

                                <PN_ID>126231523</PN_ID>
                                < PN_ID_TYP_CD>S</PN_ID_TYP_CD>
                                <PN_LST_NM>Last</PN_LST_NM>
                                <PN_1ST_NM>First</PN_1ST_NM>
                                <PN_MID_NM>Middle</PN_MID_NM>
                                < PN_CD_NM>Jr</PN_CD_NM>
```

```
                                    <PN_SEX_CD>M</PN_SEX_CD>
                                    <PN_BRTH_DT>19791206</PN_BRTH_DT>
                                    <PN_CITIZENSHIP_COUNTRY_CD>US</PN_CITIZENSHIP_C
                                    OUNTRY_CD>
                                    <NACI_STAT_CD>O</NACI_STAT_CD>
                                    <CRD_ISS_DT>20030205</CRD_ISS_DT>
                                    <CRD_EXP_DT>20061005</CRD_EXP_DT>
                                    <CRD_TRM__DT>20060603</CRD_TRMDT>
                                    <CRD_TRM_RSN_CDT>L</CRD_TRMRSN_CDT>
                            </AttributeValue>

                    </Attribute>

            </Assertion>

</SAMLResponse
```

Appendix B: Terms and Definitions

Application Identifier: A globally unique identifier of a card application as defined in ISO/IEC 7816-4.

Application Session: The period of time within a card session between when a card application is selected and a different card application is selected or the card session ends.

Authenticatable Entity: An entity that can successfully participate in an authentication protocol with a card application.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator or a means of verifying an individual's authorization to receive specific categories of information.

Authorization: Approval or denial of access to an information system or facility in order to perform or assist in a function.

BER-TLV Data Object: A data object coded according to ISO/IEC 8825-2.

Biometric: Measurable physiological and behavioral characteristics that can be used to establish and verify the identity of an individual.

Biometric file: A digital file that consists of an individual's biometric signature(s) and associated information.

Biometric identity: A distinct, non-refutable set of physical and behavioral characteristics that remains constant.

Biometric samples: Data that represents a biometric characteristic of a user as captured by a biometric system.

Card: An integrated circuit card.

Card Application: A set of data objects and card commands that can be selected using an application identifier.

Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.

Cardholder Unique ID (CHUID): is defined to provide the basis for interoperable identification of individuals and to extend capabilities over magnetic stripe technology for Physical Access Control System applications. It contains a series of mandatory and optional tagged objects. Some of these include the Federal Agency Smart Credential Number (FASC-N), the Global Unique ID (GUID), and the asymmetric signature.

Card Interface Device: An electronic device that connects an integrated circuit card and the card applications therein to a client application.

Card Reader: A synonym for card interface device.

Client Application: A computer program running on a computer in communication with a card interface device.

Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally signed by a Certification Authority. [RFC 3280]

Data Object: An item of information seen at the card command interface for which are specified a name, a description of logical content, a format and a coding.

Defense Biometric Identity System (DBIDS): is a fully configurable security and identification system that enhances safety. It provides a force protection tool for the law enforcement community, utilizing a centralized "rules-based" identity management and access verification system. Additionally, DBIDS uses the DEERS/RAPIDS ID card or produces a DBIDS ID card, DoD standard ID, to non-DoD ID cardholders for installation access authorization. It is installed at military sites around the world.

Defense National Visitor Center (DNVC): is a web-based system that allows DoD organizations to authenticate credentials and credential holders using photograph, text and fingerprint data stored in centralized databases

Extensible Markup Language (XML): Specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

Federal Agency Smart Credential Number (FASC-N): a number required on all Federal PIVs that consist of a “System Code || Credential Number” to establish a credential number space of 9,999,999,999 credentials. The FASC-N is a part of the CHUID.

Individual: A specific person.

Interagency: Within the context of Department of Defense involvement, elements of the Department of Defense, US Government agencies, State and Local governments, and nongovernmental organizations.

Interface Device: Synonym for card interface device.

Key Reference: A 6-bit identifier of cryptographic material used in a cryptographic protocol such as an authentication or a signing protocol.

Logical access: Process of granting access to information system resources to authorized users, programs, processes, or other systems. The controls and protection mechanisms that limit users' access to information and restrict their forms of access to only what is appropriate

Match: The process of accurately identifying or verifying the identity of an individual by comparing a standardized, usable biometric file to an existing source and scoring the level of similarity.

Object Identifier: A globally unique identifier of a data object as defined in ISO/IEC 8824-2. Reference Data Cryptographic material used in the performance a cryptographic protocol such as an authentication or a signing protocol.

On-line Certificate Revocation Protocol (OCSP): An online protocol used to determine the status of a public key certificate

Personal Identification Number (PIN): A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Physical Access: The process of granting access to installations and facilities

Privacy Act System of Records Notices (SORN): notification of system changes or enhancements requirement by the 1974 Privacy Act.

Privacy Impact Assessment (PIA): is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Public Key Infrastructure (PKI): A support service to the system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

Revocation Checking: The process of ensuring a credential is valid at a given point in time.

Security Assertions Markup Language (SAML): an XML standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. **SAML** is a product of the Organization for the Advancement of Structured Information Standards (OASIS) Security Service.

Status Word: Two bytes returned by an integrated circuit card after processing any command that signify the success of or errors encountered during said processing.

Special Publication 800-73-1: Interfaces for Personal Identity Verification

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification: The one-to-one process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed

Appendix C: References

This listing is provided for reader reference and convenience. Unless otherwise specified in this document, these documents should be used for information only.

Government References

- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004
- National Institute of Standards and Technology (NIST)– Technology Administration U.S. Department of Commerce, Government Smart Card Interoperability Specification. Version 2.1, July 12, 2003, http://smartcard.nist.gov
- NIST Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, February 2005, http://csrc.nist.gov/piv-project
- NIST Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, May 2001, http://csrc.nist.gov/publications/fips/
- NIST Special Publication 73, Interfaces for Personal Identity Verification, April 2005, http://csrc.nist.gov/piv-project
- NIST Special Publication 78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, April 2005, http://csrc.nist.gov/piv-project
- NIST Special Publication 800-85, PIV middleware and PIV Card Application Conformance Test Guidelines, October 2005, http://csrc.nist.gov/piv-project

Industry References

- Organization for Advancement of Structured Information Sciences (OASIS), Security Assertions Markup Language (SAML) version 2.0

Appendix D: Acknowledgements

The “Framework for Inter-Agency Authentication of Federal PIV Cards” is the product of extensive efforts by the co-chairs, Industry, and members of the IAB’s Backend Authentication Scheme Work Group (BAS WG).

Representatives of the following departments and agencies participated in the development of the framework and made multiple technical and editorial contributions to the content of this document:

Department of Agriculture
Department of Justice
Department of Defense
Department of Homeland Security
Department of Interior
Department of State
Department of Transportation
General Service Administration
National Aeronautics and Space Administration
National Institute of Standards and Technology