Defense Manpower Data Center (DMDC)

Identity Web Services (IWS)

Business Guide

Abstract This guide is designed to help Identity Web Services customers select among the available services, and to assist in implementing those services.

Release Date January 8, 2016

Document Version 2.5

Preface

To our Customers

This Identity Web Services (IWS) Business Guide will help our customers, business analysts, and other decision makers understand the Identity Web Services available from DMDC.

In addition to this IWS Business Guide, you should also have a copy of the IWS Software Development Guide (SDG). The SDG is designed to assist your technical team in developing software, building connections, and implementing the suite of Identity Web Services.

You should also have received contact information for a designated DMDC Project Officer (PO). Your DMDC PO is the main point of contact for business and technical assistance regarding IWS.

Revision History

Revision	Release Date	Description
1.0	3-19-2004	Initial Release
1.1	4-23-2004	Edits and various corrections
1.2	6-3-2004	Edits
1.3	10-15-2004	Revised versioning and naming of the document.
1.4	11-1-2004	
1.5	1-31-2005	
1.6	5-13-2005	Clarification in terminology used throughout the document
1.7	5-27-2005	Merged TIDS and PIDS with SPDS. Merged CUS with PDS
1.8	6-3-2005	Restructured
1.9	7-19-2005	SPDS more clearly defined. Inserted Check List into Application Development section.
1.10	1-6-2006	Updated section 12
1.11	2-1-2006	Minor grammatical revisions
1.12	7-06-2006	Changes for RBS and BBS
1.13	7-17-2006	Final edit
1.14	9-13-2006	Removed sensitive information for security purposes.
2.0	3-23-2007	Edited for corrections
2.1	8-20-2008	Added documentation on the Self-Defined Population (SDP) Service
2.2	10-17-2008	Added documentation on the Policy Decision Point (PDP) Service
2.3	7-15-2010	Added TVS documentation
2.4	4-19-2012	Changed DoD EDI PN ID to DoD ID Number

2.5	01-8-2016	Updated references of SSL to TLS.

Contents

1.0 About DMDCs Identity Web Services

Identity Web Services (IWS) were developed by the Defense Manpower Data Center (DMDC) to provide identity verification services to government agencies for Department of Defense (DoD) military personnel, their dependents, retirees, DoD civilians, and contractors. These Web services allow customers to request and receive current identity data from the Defense Enrollment Eligibility Reporting System, or DEERS.

There are two categories of Identity Web Services: synchronous, where the requested information is delivered immediately to the customer, and asynchronous, where data is delivered on a regular, customer-defined schedule.

Data delivered through IWS is provided from the Authentication Data Repository (ADR) database, which is a subset of DEERS containing only current information pertaining to an individual.

1.1 Business Categories

IWS may be categorized by the following business uses:

- **Physical Security:** A Web service that qualifies a person's membership or entitlement, and may confirm an individual's identity in DEERS, issue or maintain credentials that are used to authenticate a user's identity, or make or facilitate authentication or authorization decisions.
- **Identity Integration:** A Web service that provides DEERS data that the customer integrates into its local business systems.

1.2 Technical Categories

Depending on the delivery mechanism, IWS may further be categorized as synchronous or asynchronous, as shown in the following product descriptions:

- **The Real-Time Broker Service (RBS)** is a synchronous service that returns one data record per request in real-time to the client. RBS has been bundled to include the use of token and person identifiers into a seamless synchronous Web service. The addition of these identifiers into RBS expands its former capability and simplifies client development.
- **The Batch Broker Service (BBS)** is an asynchronous service that can deliver millions of records per request. Data is not immediately returned when the client sends a request. Instead, the service returns a reference identifier, which the client uses later to retrieve the requested data. BBS is also capable of providing person and population change data.
- PIDS-Update is a way for organizations to get periodic EDI smoosh updates. Authorized customers can make PIDS-UPdate requests to DEERS on a weekly/daily basis to update any EDIs that have changed within a time period. This inquiry for EDI updates will be sent via synchronous real-time transaction. The EDI crosswalks returned in the PIDS-UPdate response from DEERS should be recorded by the receiving organization for

future inquiries. If a specific EDI smoosh case is not found within the returned PIDS-UPdate crosswalk, the receiving organization may contact DMDC with the data quality discrepancy. DMDC Customers may make the following PIDS-UPdate request to DEERS on a recurring basis (suggest nightly or weekly) to get a list of all amended DOD ID numbers since the last periodic inquiry.

- **Self-Defined Population (SDP)** is a synchronous service designed to enable specific BBS customers with the ability to track changes for specific DEERS members, or their "self-defined" population.
- **Policy Decision Point (PDP)** is a synchronous service designed to provide "red light-green light" authorization decisions based on person attributes evaluated through a defined policy.
- **Token Verification Service (TVS)** is a synchronous service designed for Physical Access Control systems that takes a single token credential and returns a standard set of results. TVS also supports the ability to return results based on a fingerprint paired with a token credential.

2.0 About this Guide

This IWS Business Guide will help customers and their business analysts make informed decisions about understanding and implementing IWS. By following this guide, you will be able to select the Web service(s) that solves your physical security or identity integration needs and to initiate a smooth development effort.

This guide describes the IWS applications, their capabilities, how they are used, rules for use, and integration steps. Detailed information about developing interfaces to IWS is covered in the *Identity Web Services Software Development Guide*.

The information in this guide is effective at the time it was written and may change without notice. Please verify accuracy and timeliness of this information prior to committing any business decisions or developing any interfaces. The latest version of this guide is available from your DMDC Project Officer (PO).

3.0 IWS Overview

3.1 General Description

The Identity Web Services (IWS) deliver current DEERS data. It is expected that customers familiarize themselves with this guide and work with their DMDC PO to determine which service best solves their data needs.

3.1.1 Defense Enrollment Eligibility Reporting System (DEERS)

The DEERS database consists of the DEERS Person Data Repository (PDR) and the DEERS Medical Satellite (MedSat). PDR provides most of the information associated with a given individual, while MedSat provides medical benefit information.

3.1.2 Authentication Data Repository (ADR)

The ADR database is the data store for physical security and identity integration data provided through IWS. ADR contains a subset of current DEERS data that is replicated on a real-time basis from both the DEERS PDR and MedSat.

Customers can access the data stored in ADR through the synchronous Real-Time Broker Service (RBS), the asynchronous Batch Broker Service (BBS), or the synchronous Self-Defined Population (SDP) service. Refer to each of the respective sections for a description of these services.

3.1.3 Interfacing with IWS

IWS provides data to client applications through Web services. To interface with IWS, the client must have the capability to send and receive Simple Object Access Protocol (SOAP)/Extensible Markup Language (XML) formatted messages.

Detailed information about developing interfaces to IWS is covered in the *IWS Software Development Guide.*

4.0 Design Considerations

Carefully consider your business and application requirements before developing interfaces to IWS. In many cases, designing your client application to retrieve data as it is needed using RBS (refer to the RBS section below) will prove to be the least expensive solution. Your DMDC PO can help you determine an effective design.

In most cases, the most expensive use of IWS is to synchronize a local data store to DEERS. Carefully consider you needs and consult with your DMDC PO before committing any analysis or design in this direction.

5.0 RBS: Synchronous Service

The Real-Time Broker Service (RBS) provides current DEERS data to customers who have a requirement to (1) qualify a person's membership or entitlement, (2) confirm an individual's identity in DEERS, (3) issue or maintain credentials that are used to authenticate identities, or (4) make or facilitate authentication or authorization decisions.

RBS is an online synchronous data delivery Web service that receives a request for an individual, queries DEERS, and returns a response to the originating system. The type of information that RBS returns for an individual is based on a customer-defined XML schema.

RBS is intended for real-time data requests for an individual, greatly reducing or eliminating the need to synchronize a local data store with DEERS. RBS is designed to return data to the

requesting system in under two seconds, although response time may vary based on network and server loads. In summary,

- RBS returns current DEERS data
- RBS provides a real-time service
- RBS accepts several different standard identifiers
- RBS is used in lieu of a local data store
- RBS establishes identity or eligibility
- RBS eliminates the need to recover from outages, errors, or application bugs
- RBS simplifies client logic required to interpret messages
- RBS provides customer-specific data elements
- RBS may return multiple sets of data elements to one customer

Current RBS customers include Army Knowledge Online (AKO), Research Development and Engineering Command (RDECOM), Military Severely Injured Joint Operations Center (MSIJSOC), Navy Education and Training Command (NETC), and Joint Personnel Adjudication System (JPAS). These customers use RBS for the following purposes:

- To obtain identifier and person/personnel information for DoD individuals
- To provide real-time updates to data records as individuals attempt access
- To propagate the common use of the DoD ID number

5.1 RBS Guidelines

Individual RBS requests may be made as often as needed within the limits of the *Memorandum of Understanding (MOU)* and the *Client Interface Specification (CIS)*, which your DMDC PO will provide. If frequent large batch updates are needed, BBS may be a more appropriate solution.

5.1.1 RBS Data Elements

RBS returns data for individuals (e.g., name, address, and date of birth) using a customer-specific XML schema. Your DMDC PO can help you determine available data elements by analyzing requested data elements provided by the customer.

RBS may be further configured to deliver multiple sets of data to the same customer by using multiple XML response schemas. Contact your DMDC PO for details.

5.1.2 RBS Processing

RBS receives the customer request, which may include any of the identifiers above, and attempts to find a match in the DEERS database. If a match is made, RBS will return all available data specified in the customer-specific RBS response schema. If a given data element is not available for an individual, that element will not be returned in the response.

If no match can be made, the RBS response will consist of the submitted request without any data elements.

5.1.3 Choosing RBS

Following are some variables to consider when determining if RBS is the solution to your data needs:

- The need for person data versus population data.
- WAN capabilities: if your WAN cannot absorb large asynchronous data feeds, then RBS may be the best solution.
- Population size: if your population size is less than one million, consider RBS.
- Anticipated growth in population size: if your population size is not expected to grow to one million or more, then RBS may be your solution.
- The primary data source is DEERS.
- The need to establish or confirm identity or eligibility.

Your DMDC PO will be available to help you decide if RBS is the right solution for your data needs.

6.0 BBS: Asynchronous Service

BBS is an asynchronous Web service that allows customers to obtain data records or changes for specific persons or populations in DEERS. BBS receives an inquiry, interrogates DEERS, and then returns a response. Data returned from BBS are for customer-specified person or population changes. Requests to BBS are handled asynchronously because large datasets are generated.

BBS returns data on all relevant changes within a given customer population for a given time period, generating a result set that is potentially very large. To ensure there is adequate time to process the result set, BBS requests should be made no more than once per hour. BBS performance is dependent on the number of records in a BBS request. To summarize:

- BBS is used to obtain person or personnel data
- BBS sends current data only (no historical data)
- BBS is used when there is a potential for "significant use" of the customer population
- BBS is used when there are large data volume needs and/or a need for fresh data
- BBS is used to run reports against locally stored but current DEERS data required more frequently than once every two weeks

Current BBS customers use this Web service to obtain identifier and demographic information for DoD populations. Some customers using BBS include the Air Force Directory Service (AFDS), Electronic Military Personnel Office (eMILPO), Army Air Force Exchange Service (AAFES), and Naval Postgraduate School (NPS).

These customers use BBS for the following purposes:

- To receive data on all Air Force personnel for the Air Force Directory Service database
- To obtain person and personnel data on all DoD Active Army and Army Reserve personnel (on active duty) sponsors
- To receive a weekly real-time file that validates and maintains the accuracy of a master database

6.1 BBS Guidelines

BBS can be used to resolve large quantities of customer inquiries in a single request for individual or multiple inquiries, for population changes, or for exception recovery. The batch update functionality provided by BBS can also be accomplished with RBS by making multiple RBS (synchronous) requests. In most cases, making multiple RBS requests is the preferred method of making these updates.

6.1.1 Request Frequency

Individual BBS requests are defined in your MOU and CIS, both or which are provided by your DMDC PO. BBS requests for the same individual should not be submitted more than once per hour.

6.1.2 Data Elements

BBS delivers data for individuals (e.g., name, address, and date of birth) or population changes, as described in a customer-specific XML response schema. The elements in the schema are listed and defined in the CIS.

6.1.3 Processing

BBS evaluates each customer inquiry to see if there is a match or a change in the defined population from the DEERS database. If a match or change is evident, BBS returns all available data in the customer-specific XML response schema. If a given data element is not available for an individual, that element will not be returned in the response.

If no match can be made, the response from BBS will consist of the original submission but no data elements.

6.1.4 Choosing BBS

Some variables to consider that help determine if BBS is the solution to your data needs may include:

- The need for batch versus real-time data
- There is a dedicated high availability network available
- There are off-line reporting requirements
- The ability to process large batch data responses

Work with your DMDC PO to help you decide if BBS is the right solution for your data delivery needs.

6.1.5 Defining Data

Before creating an application to interface with BBS, a customer needs to define the following:

1. **Population selection criteria**. Populations may include, for example, active Army members and their dependents, Navy Reserve enlisted, or Marine officers.
2. **Request frequency**. This usually ranges from hourly to daily, but can be arranged to be more or less often.

3. **Data elements**. Elements should be discussed with your DMDC PO to define a customer-specific list.

6.1.5.1 Request Frequency

The frequency of BBS requests has an impact on the number of returned records per request. The number of returned records is influenced by the following customer-defined elements:

- Customer population size
- Population selection criteria complexity
- Amount of tracked fields
- Request frequency

A typical BBS customer population may have from 5,000 to 250,000 hourly population changes. Request frequency should be designed to allow the result set from one request to be completely processed before sending the next request.

7.0 SDP: Synchronous Service

The Self-Defined Population (SDP) service is designed to enable specific BBS customers with the ability to track changes for specific DEERS members, or "self-defining" a customer population. SDP is used when a customer knows the specific people who are in their population and can provide either a DoD ID number or Person Identifier (SSN, Name, and DoB) for those people.

SDP allows customers to 1) add/remove tracked DEERS population members at any time through the SDP service and 2) request updates to their tracked population through BBS Time-based inquiry.

The benefits of providing SDP include:

- Enabling a customer to add and remove BBS-tracked population members
- Reducing transaction volumes for multi-identifier customers

8.0 PDP: Synchronous Service

The Policy Decision Point (PDP) provides a red light-green light authorization decision to a request based on the evaluation of a defined policy.

PDP is an online synchronous authorization Web service that receives a request for an individual, queries DEERS, validates the retrieved record against a defined policy, and returns an authorization response to the originating system.

In summary:

- PDP returns authorization responses
- PDP provides a real-time service
- PDP accepts several different standard identifiers (the same ones as RBS and BBS)

8.1 PDP Guidelines

Individual PDP requests may be made as often as needed within the limits of the *Memorandum of Understanding (MOU)* and the *Client Interface Specification (CIS),* which your DMDC PO will provide.

8.2 PDP Processing

PDP receives the customer request, which may include any of the identifiers above, and first attempts to find a match in the DEERS database. If a match is made, PDP will return an authorization response based on a defined policy created in cooperation with customer business needs.

8.3 Choosing PDP

Following are some variables to consider when determining if PDP is the solution to your interface needs:

· The need for authorization responses versus person data.
· The need to reduce local business processing complexity and allow DMDC to make the authorization decision.

Your DMDC PO will be available to help you decide if PDP is the right solution for your interface needs.

9.0 TVS: Synchronous Service

Token Verification Service, or TVS, is a Web service developed by DMDC to provide physical access control system (PACS) customers the ability to register users and to verify credentials against a DoD authoritative identity source. TVS provides a mechanism to verify a Common Access Card (CAC) and a way to verify fingerprints and (potentially) cards issued by the Federation for Identity and Cross-Credentialing Systems (FIXS) and or DBIDS.

9.1 TVS Guidelines

Individual TVS requests may be made as often as needed within the limits of the *Memorandum of Understanding (MOU)* and the *Client Interface Specification (CIS),* which your DMDC PO will provide.

9.2 TVS Processing

TVS receives the customer request, which may include a token and optionally a fingerprint and attempts to find a match in DEERS. If a match is made, TVS will return verification and/or additional information.

9.3 Choosing TVS

Following are some variables to consider when determining if TVS is the solution to your interface needs:

· The customer system falls under the guidance of being a DoD Physical Access Control System (PACS).

10.0 Application Development

There are several steps involved to successfully select, connect to, and use IWS. Your DMDC PO will work with you to coordinate these steps with the IWS Technical team and DMDC Systems personnel.

►Step 1: Inception

a) Receive an *IWS Getting Started* package from your DMDC PO (see Section 11).

b) Meet with your DMDC PO to determine milestones and requirements.

c) Select the Web service(s) that is capable of meeting your data needs. Use this document and work with your DMDC PO to help make this decision.

d) Establish the data elements required within your business case and work with your DMDC PO to match these elements with those available through IWS.

e) Provide a copy of your *System Notice* if you intend to store the data you receive through IWS and your *Authority to Operate (ATO)* or *Interim Authority to Operate (IATO)* to your DMDC PO.

►Step 2: Elaboration

a) Your DMDC PO will provide a draft of a *Memorandum of Understanding (MOU)*. You will work with him/her to revise and finalize the document for signature. The MOU establishes terms and conditions under which DMDC will provide data.

b) Your DMDC PO will provide a draft of your *Client Interface Specification*, which is used to communicate functional requirements to the IWS and customer's technical team.

c) Outline an implementation schedule with your DMDC PO using the IWS implementation checklist as a guide.

d) Begin the process of establishing connectivity as needed for both Contractor Test and Production. Customers with exceptional data or performance requirements may need to establish a dedicated T1 connection to DEERS. (Note: a customer signed MOU is required to initiate a VPN or TLS work order).

►Step 3: Construction

a) Refer to the *RBS/BBS Software Development Guide* (SDG) for application development information. Use this SDG to build a client application that queries for the data needed. Any programming language that supports HTTP communication across Internet socket connections, such as Java, Visual Basic, or C++, may be used.

b) Request and obtain a unique Customer System ID (CSTR_SYS_ID) from your DMDC PO. Until this Customer System ID has been configured in IWS, you will receive an error

response if you attempt to query DEERS. Customers are only allowed to use those services for which access has been requested.

c) Establish Contractor Test connectivity.

d) Implement the software client in Contractor Test.

►Step 4: Transition

a) After unit testing the client application, contact your DMDC PO to coordinate integration testing against the Contractor Test environment.

b) If a seed file is identified in the *Client Interface Specification*, arrange to have the file delivered so it can be loaded into your Production environment. Work with your DMDC PO to coordinate this request.

c) When satisfied that the client application has passed integration testing, run a final acceptance test against the Production environment. Work with your DMDC PO to coordinate the migration to Production.

d) Establish Production connectivity.

e) When migrating to the Production environment, only minor configuration changes should be needed to perform acceptance testing.

f) Deploy to Production.

11.0 Data Usage Guidelines

The DoD Identifier number is the standard DoD identifier for an individual in system-to-system electronic communication. This identifier, also embedded in the Common Access Card (CAC), is not to be displayed to a user or entered manually into any system. Systems which interface using the DoD ID number are expected to utilize their own unique identification scheme, cross-referenced to the DoD ID number. Other personal data elements available through IWS are generally protected by the Privacy Act, as specified in the *Memorandum of Understanding*, or other agreement between an IWS customer and the DMDC.

11.1 Data Currency

Identity Web Services only provide the most recent data available for a given data element. Changes are reflected on the date that they are effective in the DEERS database. If a data element is time sensitive, the value it contains will only exist for the duration of that time period. Data returned for all services is the most current at the time of processing.

11.2 Connectivity and Security

The interface to IWS uses point-to-point connections with HTTP (HyperText Transfer Protocol, port 80). The connection must be secured by a site-to-site Internet Protocol Security (IPSec) VPN or PKI-enabled TLS connection utilizing either machine certificates or a shared secret.

11.3 Availability

RBS and BBS have regularly scheduled maintenance downtime on Saturdays from 2100-2200 hours Eastern Standard Time (EST) and are available all other days 24x7. Extended maintenance windows are occasionally required and will be communicated in advance. Additional downtime is possible as needed. Requirements for rigorous high availability (greater than 97% uptime) must be negotiated in a Service Level Agreement (SLA).

12.0 Support

Development and Testing

While developing and testing the client application, your DMDC PO is the primary point of contact for general questions, technical support, or any other issues.

Production Support

Once the client application has moved to Production, application issues that require technical assistance should be sent to the IWS Production Support Group. Production Support points of contact will be provided upon migration to Production. For issues regarding individual data which is believed to be inaccurate (such as incorrect personnel rank), the member should contact the servicing installation personnel office for resolution or escalation as necessary.

During the move to production support, designate one or more contacts to be added to the production support email distribution lists for unscheduled outage notifications.

13.0 Glossary

ADR – Authentication Data Repository: ADR contains a subset of data that is replicated on a real-time basis from the DEERS Person Data Repository (PDR) and the DEERS Medical Satellite.

ADW – Access Data Warehouse: ADW provides access to person, personnel, enrollment, and eligibility data that is stored on the Authentication Data Repository (ADR).

IWS – Authentication Data Repository Web Services: Web services that provide access to current DEERS data.

BBS – Batch Broker Service: An asynchronous web services providing access to current DEERS data. BBS allows customers to obtain data records or changes for specific persons or populations in DEERS.

CAC - Common Access Card: A standard identification smart card issued by the DoD for active duty members of the Uniformed Services, Selected Reserve, DoD civilian employees, and eligible contractor personnel. The CAC is the principal card used to enable physical access to buildings and controlled spaces and for logical access to the Department's computer networks and systems. The CAC platform contains mandatory identification, physical and logical access

capabilities, Public Key Infrastructure (PKI) authentication, encryption, and digital certificates, and includes an individual's DoD ID number.

Client or Client Application – External software which interacts with IWS by making requests and retrieving responses.

Credential – A Credential is a container for tokens and can contain one or more tokens. A smartcard and a DBIDS vehicle pass are considered credentials. A credential may also be a physical device that embeds tokens.

Customer – The organization which is creating software to interface with the IWS, with the purpose of accessing data from DEERS. Note the software itself is referred to as a *client*.

DEERS – Defense Enrollment Eligibility Reporting System: A centralized DoD data repository of personnel and medical data. DEERS contains detailed personnel eligibility information for benefits and entitlements distribution to Uniformed Services members, U.S. sponsored foreign military members, DoD and Uniformed Services civilians, other personnel as directed by DoD, and their eligible family members (dependents). Additional information can be found at http://www.dmdc.osd.mil.

DMDC – Defense Manpower Data Center: A Defense Support Activity which is the most comprehensive repository of personnel, manpower, training, and financial data in the DoD. DMDC owns and manages DEERS, including IWS.

DoD (DOD) – Department of Defense: The collection of federal agencies responsible for safeguarding national security.

DoD ID Number– DoD EDI Identification number: The standard unique identifier used to represent a person within the DoD.

EDI – Electronic Data Interchange: The transfer of data between different companies using networks.

HTTP – HyperText Transport Protocol: The underlying protocol used by the Internet which defines how messages are formatted and transmitted, as well as what actions Web servers and browsers should take in response to various commands.

IPSec – Internet Protocol Security: A set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks.

MedSat – Medical Satellite: The DEERS satellite database for medical enrollment information stored under common identifiers in standardized formats.

PDR – Person Data Repository: The main DEERS database comprised of statistical information for sponsors and their dependents.

PKI – Public Key Infrastructure: Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables DoD to protect the security of their communications and business transactions. PKI integrates the Common Access Card (CAC), digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide network security architecture.

PO – Project Officer: An individual representing DMDC and assigned to a customer for the purposes of implementing IWS.

RBS – Real Time Broker Service: A synchronous web service providing access to current DEERS data. RBS allows customers to obtain data records or changes for specific persons or populations in DEERS. RBS allows the customer to (1) qualify a person's membership or entitlement, (2) confirm an individual's identity in DEERS, (3) issue or maintain credentials that are used to authenticate identities, or (4) make or facilitate authentication or authorization decisions.

SDP – Self-Defined Population: A synchronous service designed to enable specific BBS customers with the ability to track changes for specific DEERS members, or their "self-defined" population.

SOAP – Simple Object Access Protocol: A lightweight protocol for exchange of information in a decentralized, distributed environment. It is an Extensible Markup Language (XML)-based application protocol that consists of three parts:

- An envelope that is the outermost element item in a SOAP message
- A header representing the state of a transaction
- A body containing information targeted at an ultimate SOAP receiver (customer)

For more information about SOAP, refer to http://www.w3.org/TR/SOAP/

Token – A security token (or sometimes a hardware token, authentication token, or cryptographic token) may be embedded on a physical device that an authorized user of computer services is given to aid in authentication. For the purpose of this document, a token is a barcode, magnetic stripe, or CHUID that can be read from CAC.

TVS – Token Verification Service: TVS is a synchronous service designed for Physical Access Control systems that takes a single token credential and returns a standard set of results. TVS also supports the ability to return results based on a fingerprint paired with a token credential.

VPN – Virtual Private Network: A network that uses encryption and other security mechanisms to provide a secure tunnel for authorized users to send private traffic over a public network, such as the Internet.

Web Service – Any one of the IWS that provide an interface to external customers.

XML – eXtensible Markup Language: A simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety

of data on the Web and elsewhere. For more information about XML, refer to http://www.w3.org/XML/