Introduction to Identity Web Services

The Card Technology and Identity Solutions (CTIS) Division within the Defense Manpower Data Center (DMDC) provides Web services to DoD agencies needing identity verification information. Specifically, these Web services provide customers the ability to verify the identity of users accessing their applications, to confirm the eligibility of a person in DEERS, and to synchronize a local data store.

The Authentication Data Repository (ADR) is a subset of data from DEERS and is replicated on a real-time basis. It contains the same current, up-to-date information that resides in DEERS. Identity Web Services, or IWS, enable vetted customers the ability to obtain enrollment, eligibility, and demographic data, as well as Yes/No responses to identity inquiries, for military personnel and their dependents, retirees, DoD civilians, and DoD contractors.

Choosing the Web Service that Best Suits your Requirements

Customers use the Real-Time Broker Service (RBS) when:

- They need Real-time data.
- They need specific identities instead of identities that have a certain common criteria.
- Their WAN cannot absorb large asynchronous data feeds
- Their transaction volume is less than 50K per day and is not expected to grow to over 50K per day.
- The primary data source needed is DEERS.
- They need to establish or confirm identity or eligibility.
- They need to obtain a new Person ID using another DOD Person ID (SSN to DOD EDI or DOD EDI PI to SSN). Note: The latter will become a major usage in the future when SSN is taken off the ID card

Customers use Self-Defined Population (SDP) when:

- The customer knows who is in their population and wants to know about changes to that population.
- The customer would otherwise want to sweep for changes [on a similar population] using RBS or BBS, which is not allowed.

Customers use Batch Broker Service (BBS) Time-based Inquiry when:

- They can describe all of their population (current and potential) using attributes in ADR.
- The customer cannot use SDP because they don't know who is in their population ahead of time.
- Using BBS Multi-Identifier (MI) or RBS, the customer would need to periodically sweep for more than 50K user records. (Sweeping is not allowed.)
- DMDC decides that the customer's business case is strong enough to create a BBS-TBI interface, which represents a resource-intensive interface, and the customer justifies the need to store information.

Customers use BBS Multi-Identifier when:

- The customer knows who is in their population but the population varies with each request.
- They need batch data versus real-time data.
- They have a dedicated high-availability network.
- They have off-line reporting requirements.
- They have the ability to process large (over 50K) batch responses.

- They are interested in the record at the time at pull.
- VPNs should be used for BBS requests with over 10k records per trxn.

Customers use PDP when:

- They need a yes/no answer instead of data

Non-AWS Options: Customers use the DMDC Data Request System (DRS) when:

- They are unable to utilize the Web Services
- They want data elements that are not available in ADR

What is the DoD EDI Person Identifier?

The DoD EDI Person Identifier, or DOD_EDI_PN_ID, is the standard identifier within DEERS and the DoD. This identifier is used between DoD systems to uniquely identify persons without the need for privacy information, such as Social Security Number or name. The DoD EDI PN ID is a randomly-generated 10-digit number assigned to each individual affiliated with the DoD.

Implementation Steps

In the initial phase of your Web services implementation, you will be assigned a dedicated Project Officer (PO) who will guide you throughout the process. He or she will provide you with a “Getting Started with IWS” package to help you better understand the steps required for a successful Web services implementation. Your PO will then schedule a kickoff meeting to discuss requirements and determine the best solution for your particular situation. Once this meeting has taken place between the PO and the customer, the documents in the package will begin to make sense and will help guide you through the approval and implementation process.

In your “Getting Started with IWS” package, you will find an IWS Implementation Checklist. This checklist provides an overview of the steps for a customer implementation. Next, there are fact sheets for Network Certification and Accreditation and System Notices, which will assist you in providing the necessary documentation needed to gain access to DMDC and DEERS Privacy Act data. DMDC requires that any network requesting a connection be certified and accredited to DIACAP, NIACAP, or NIST standards.

A System Notice published for at least 30 days in the Federal Register is also mandatory if the receiving organization intends to store the data they get from DMDC.

Once the Network Certification and System Notice requirements are complete, DMDC requires a Memorandum of Understanding (MOU). Included in the package is an MOU Fact Sheet to explain the terms of the agreement. A signed MOU is a required document before any organization can connect to DEERS.

The Data Transmission Fact Sheet explains policy requirements for transmitting DEERS data to customers, as well as the importance of data encryption. When VPN is used for transmitting data, we require a Customer VPN template and have included a VPN Fact Sheet for further reference.

When PKI-enabled SSL is used for transmitting data, we require a completed Customer PKI-enabled SSL template that provides us with the information we need to get the SSL connection set up on our end. We have also included a PKI-enabled SSL Fact Sheet that explains the requirements and process for setting up a secure connection.

Also included in the documentation package is the Identity Web Services Software Development Guide. This document contains sample XML to help developers with their interface to DMDC and will most likely be the most helpful document in the package. There is also a document titled, "DoD EDI PN ID Explained," which discusses in detail the DEERS only unique, unambiguous identifier, the DoD EDI PN ID.

Once the customer interface is up and running in our Contractor Test environment, we move into the final phase, Transition. Here, we establish that data is successfully being sent and received in Contractor Test and the customer can begin connecting to us in Production.

These documents, as well as your DMDC PO, will assist you through a streamlined process of getting the data you need to meet your identity verification requirements.

** Following are the Federal Requirements for the Disclosure of Privacy Act Data (summarized from the Privacy Act of 1974):*

Customers may access DEERS data if they have a reason to know that is a part of their job and they can only redisclose it within DoD under the same circumstances. To make that determination, there are three tests that are used:

1. **Need to Know**. Most importantly, the requester must demonstrate that he or she has a need for the information in order to discharge his or her official duties. This is based on the "need-to-know" concept. In short, the requester must articulate in sufficient detail why such information is required so that the custodian of the information can make an informed decision as to whether the information should be disclosed.

2. **Purpose for which data is collected**. The intended use of the information by the requester generally must be related to the purpose for which the information is maintained. Ordinarily, the agency will look to the "purposes" section of the system notice as it will state for what purposes the information is being maintained. If the proposed use is unrelated to any of the articulated purposes, this would suggest that the request fails the "relational" test. But in general, this test is not difficult to meet.

3. **Minimization**. There is a minimization principle to be observed. An agency collects, maintains, uses, and disseminates only that information which is relevant and necessary to carry out an agency function prescribed by statute or executive order. Therefore, the custodian of the record is under an obligation to only disclose that information which is minimally needed to accomplish the intended purpose.