Customer Interface Specifications
for
NIPRNet Enterprise Directory Query Services (EDQS)

Between

<<Component>>

and

DISA Enterprise Services Directorate
Enterprise Infrastructure

15 September 2014

Version 1.6

Table of Contents

1. Overview 3
2. Connection Specification 3
   2.1. Scope 3
   2.2. General Assumptions 5
3. Technical Solution 5
   3.1 Connection Description 5
   3.2 External Interfaces 6
   3.3 Client Requirements 6
   3.4 Root Distinguished Name 6
   3.5 Service Account Information 6
   3.6 Business Processing Rules 6

Version History Tracking

Version	Date	Description of Changes	Modified By
1.0	28 FEB 2013	Initial version.	T. Mazzullo
1.1	23 APR 2013	Updated attribute table	T. Mazzullo
1.2	2 AUG 2013	Modified attribute description, modified verbiage in 3.5	T. Mazzullo
1.3	25 MAR 2014	Modified attribute list for IdSS release 22	T. Mazzullo
1.4	24 APR 2014	Modified attribute list per release v3.2	T. Mazzullo
1.5	27 JUL 2014	Updated attribute Description field	T. Mazzullo
1.6	15 SEP 2014	Updated attribute Description fields to align with IdMI CIS	J. Byers

1. Overview

The purpose of this document is to define the connection interface between DISA Enterprise Services Directorate, Enterprise Directory Query Services (EDQS) and the <<Component>>. This agreement defines the connection between the EDQS Lightweight Directory Access Protocol (LDAP) Servers and the <<Component>> on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet). EDQS is a solution which allows for real-time queries of DISA Enterprise Directory data using a LDAP over Secure Sockets Layer (LDAP/S) query. To prevent unwarranted proliferation, derivative use of DMDC provided identity data is subject to both DISA and DMDC oversight.

2. Connection Specification

This agreement formalizes the relationship and provides the specific authoritative detail required to operate, maintain, and update the EDQS connection in support of <<Component>>/DISA Memorandum of Agreement (MOA).

2.1. Scope

2.1.1 Data Dictionary. Please select required fields.

Contact	Detailed	Extended	Required		IdMI (AD LDS) Attributes	Description	Data Type (From DMDC)*	Data Type from IdSS
•	•	•	☐	1	**cn**	**The Persona User Name (PUN)** (e.g., thomas.e.doe47.ctr)	VARCHAR2(64)	String(64)
	•	•	☐	2	**co**	**Duty Address: Country Code** (e.g., US, CA)	CHAR(2)	String(128)
•	•	•	☐	3	**company**	The **Duty Organization Code** unless extensionAttribute2 is NULL. If extensionAttribute2 is NULL, this value is the **Administrative Organizational Code**. **NOTE:** Duty Org Code is modifiable by end-user while Admin Org Code (e.g., DoD, USARMY, etc.) is not end-user modifiable.	VARCHAR2(15)	String(64)
•	•	•	☐	4	**department**	**Duty Sub-Organization Code** (e.g., EIS)	CHAR(20)	String(64)
•	•	•	☐	5	**displayName**	**The Persona Display Name (PDN)** (e.g., Doe, Thomas E (Tom) CTR DISA EIS (US))	VARCHAR2(200)	String(256)
•	•	•	☐	6	**employeeID**	**Federal Agency Smart Credential – Number (FASC-N)** (e.g.,1234567890197005)	NUMBER(16)	String(16)
•	•	•	☐	7	**employeeType**	**Persona Type Code (PTC)** (e.g., mil, civ, ctr, etc.)	CHAR(3)	String(256)
•	•	•	☐	8	**extensionAttribute1**	**Branch of Service Code** (e.g., A, D, F, M, N, etc.)	CHAR(1)	String(1024)
•	•	•	☐	9	**extensionAttribute2**	**Duty Organization Code** (e.g. DISA, USARMY, etc.)	CHAR(20)	String(1024)
•	•	•	☐	10	**extensionAttribute3**	**Duty Address: Building + " / Rm " + Duty Address: Room** (e.g., Operations / Rm C3K50H)	VARCHAR2(100) + VARCHAR2(40)	String(1024)
		•	☐	11	**extensionAttribute4**	**US Citizen** (e.g., Y, N)	CHAR(1)	String(1024)
•	•	•	☐	12	**extensionAttribute5**	**Duty Address: Installation/Location Code** (e.g., meade)	VARCHAR2(20) ****	String(1024)
•	•	•	☐	13	**extensionAttribute7**	**Office Symbol Text** (e.g., EE212)	CHAR(30)	String(1024)
		•	☐	14	**extensionAttribute8**	**Country of Citizenship** (e.g., US, CA)	CHAR(2)	String(1024)
•	•	•	☐	15	**extensionAttribute9**	**US Government Agency Code** (e.g., DD00, AF2B, etc.)	CHAR(4)	String(1024)

Contact	Detailed	Extended	Required		IdMI (AD LDS) Attributes	Description	Data Type (From DMDC)*	Data Type from IdSS
•	•	•	☐	16	**extensionAttribute10**	**Preferred First Name**	VARCHAR2(68)	String(1024)
	•	•	☐	17	**facsimileTelephoneNumber**	**Duty Phone Number: Fax** (e.g., (425) 555-1212)	CHAR(20)	String(64)
•	•	•	☐	18	**generationQualifier**	**Generational Qualifier** (e.g., Sr, Jr)	VARCHAR2(4)	String(64)
•	•	•	☐	19	**givenName**	**First Name**	VARCHAR2(20)	String(64)
•	•	•	☐	20	**Initials**	**Middle Name**	VARCHAR2(20)	String(6)
	•	•	☐	21	**l**	**Duty Address: City**	CHAR(20)	String(128)
•	•	•	☐	22	**mail**	**Work Email address (primary email address)** (e.g., thomas.e.doe47.ctr@mail.mil)	VARCHAR2(80)	String(256)
•	•	•	☐	23	**mobile**	**Duty Phone Number: Mobile** (e.g., (425) 555-1212)	CHAR(20)	String(64)
	•	•	☐	24	**otherTelephone**	**Duty Phone Number: Other** (e.g., DSN: (425) 555-1212)	CHAR(20) **	String(64)
		•	☐	25	**personalTitle**	**Military Rank Code or Civilian Rank Code** (SES, HON, HQE only. GS-01 to GS-15 are not shown.)	VARCHAR2(6) or VARCHAR2(10)	String(64)
•	•	•	☐	26	**physicalDeliveryOfficeName**	**Duty Address: Installation/ Location Display Name** (e.g., Ft. Meade)	CHAR(50) *****	String(128)
	•	•	☐	27	**postalCode**	**Duty Address: Postal Code (ZIP Code + ZIP Code Extension)** (e.g., 20755-1212)	CHAR(5) + '-' + CHAR(4)	String(40)
•	•	•	☐	28	**proxyAddressess**	**Work Email Address** (may contain several secondary entries. Mail attribute will have the primary address). On SIPR, proxyAddress does NOT contain end-user supplied SIPR contact values (MC32 – MC34) (e.g., SMTP: thomas.e.doe@usaf.mil)	VARCHAR2(80) ***	String(1123)
	•	•	☐	29	**roomNumber**	**Duty Address: Room** (e.g., C3K50H)	VARCHAR2(40)	String
•	•	•	☐	30	**sn**	**Last Name**	VARCHAR2(26)	String(64)
	•	•	☐	31	**st**	**Duty Address: State** (e.g., MD)	CHAR(2)	String(128)
•	•	•	☐	32	**streetAddress**	**Duty Address: Street** (Address Line 1 + Address Line 2)	CHAR(40) + CHAR(40)	String(1024)
	•	•	☐	33	**telephoneNumber**	**Duty Phone Number + ' x ' + extension number**	CHAR(20) + CHAR(6)	String(64)
•	•	•	☐	34	**title**	**Job Title Text** (e.g., Branch Chief)	CHAR(80)	String(128)
•	•	•	☐	35	**uid**	**EDIPI + Persona Type Code** (1234567890.civ)	CHAR(14)	String
	•	•	☐	36	**userCertificate**	**User Encryption Certificate** For NIPR, this is the encryption certificate on the CAC while on SIPR; this is the encryption certificate on the SIPR token.	BINARY	Binary

* The data type information shown is from the source location (DMDC). userCertificate is from GDS.

** otherTelephone is a multivalued attribute and will contain up to three phone numbers from DMDC, each value will be prefixed with the following: "Work:" for type W, "Temporary:" for type T, and "DSN:" for type N.

*** proxyAddresses is a multivalued attribute that may contain more than one email address.

**** extensionAttribute5 is the DMDC code for Duty Installation. Go to IASE (http://iase.disa.mil/idam/dq) and review the "Duty Installation / Location Code" spreadsheet for valid values.

***** physicalDeliveryOfficeName is the Display Name value corresponding to the DMDC code. Go to IASE (http://iase.disa.mil/idam/dq) and review the "Duty Installation / Location Code" spreadsheet for valid values.

Attributes are provided in three groupings: Contact, Detailed and Extended. This is shown on the left hand side of the table. An attribute is included in a specific grouping when a dot (●) is present.

2.1.2 Data Terms of Use.

The registry data and contact information is provided for populating and maintaining user objects in the DOD or DOD Component level information technology (IT) systems that maintain user state (possess accounts). The data from EDQS will not be copied or maintained in other systems for other purposes, such as for local physical access authorization systems, or for attribute-based access control (ABAC) systems. Data to support ABAC systems may only be obtained directly from DMDC.

2.2. General Assumptions

- DISA will coordinate with DMDC to correct data discrepancies between DMDC provided source data and data transformed or augmented as part of the Identity Synchronization Service (IdSS) processing, which feeds EDQS. DMDC is the authoritative source for all person based data contained in EDQS.
- DISA ESD is accountable source for email addresses of migrated users of Defense Enterprise Email system
- DISA GDS is the accountable source for all encryption certificate data
- Separate Security Accreditations are required by both DISA and <<Component>>
- The connection is mission assurance category (MAC) level III and does not require a continuity of operations (COOP) capability
- DISA will maintain a list of all EDQS connections which will be made readily available to DMDC.
- <<Component>> will use this connection for real-time queries of DISA Enterprise Directory data.
- All systems receiving the data must be accredited in accordance with DoD Instruction 8500.2.
- All systems receiving EDQS data must have a valid Privacy Impact Assessment (PIA) or System of Record Notice (SORN) to ensure protection of Personally Identifiable Information (PII).

3. Technical Solution

DISA ESD has designed a solution which allows for real-time queries of Enterprise Directory data using LDAP/S queries.

3.1 Connection Description

EDQS is a solution which allows for real-time queries of DISA Enterprise Directory data using a LDAP/S query. The connection will be initiated by the customer IT system using a random TCP port and connecting to an LDAP server using the LDAP/S protocol. Authentication to the LDAP directory will require explicit credentials created for each individual customer using LDAP Simple Bind.

3.2 External Interfaces

Table below lists the required communication with external systems and specifies the ports and protocols used by each.

External System Communication Requirements				
Source Server	**Destination Server**	**Ports**	**Protocols**	**Notes**
<Customer IP>	*<DISA LDAP Server>*	TCP/636	LDAP/S	Primary Connection
<Customer IP>	*<DISA LDAP Server>*	TCP/636	LDAP/S	Secondary Connection

Table 1 - External System Communications

3.3 Client Requirements

1. <<Component>> will stand-up and maintain any necessary system they will use to interact with EDQS solution.

2. <<Component>> make necessary changes to <<Component>> firewalls to allow communication between their servers and the EDQS Primary and Secondary servers through the <<Component>> enclave boundary.

NOTE: The format of the LDAP query being sent to the EDQS solution can greatly impact the performance of the LDAP Servers – a review of the LDAP query may be requested by DISA to help reduce the LDAP directory load.

3.4 Root Distinguished Name

The baseDN used for the LDAP/S connection will be:

DC=idmi,DC=mil

3.5 Service Account Information

The service account credentials will be provided upon submission of a DD Form 2875. Users who wish to request password resets or to ask for the service account to be unlocked when they contact the service desk (DEEServiceDesk@mail.mil) must have a 2875 on file.

The service account permission level will be (Contact, Detailed, or Extended): XXXXXX

3.6 Business Processing Rules

Describe limits, constraints, and Controls necessary to protect the relationship:

3.6.1 Assessing segment cardinality and population membership.

Some segments in the IdSS schema could be populated with multiple values. The following rules govern how each segment is processed and presented.

3.6.1.1 Person Segment: Whenever data is returned, all current person elements are returned as long as the Person has a current, valid, unexpired CAC. The Person segment always returns the current, correct EDI PI.

3.6.1.2 Persona Segment: The Persona segment will be populated by at least one set of data elements because all Persons must have at least one Persona. An individual Person may have multiple Persona segments, each tied to a unique CAC, and all of the Persona segments that correspond to a valid CAC will be returned.

3.6.2 Identifying terminations from the IdSS population in EDQS

If a member no longer meets the population definition (has a valid CAC), the individual is no longer eligible for IdSS. The persona will be deleted and no longer available in EDQS 7 days after the person no longer has a valid CAC.