



**Customer Interface Specifications
for
SIPRNet Enterprise Directory Query Services (EDQS)**

Between

<<Component>>

and

**DISA Enterprise Services Directorate
Enterprise Infrastructure**

2 August 2013

Version 1.2

UNCLASSIFIED

Table of Contents

1.	Overview	4
2.	Connection Specification	4
2.1.	Scope	4
2.2.	General Assumptions	6
3.	Technical Solution	6
3.1	Connection Description.....	6
3.2	External Interfaces	6
3.3	Client Requirements	7
3.4	Root Distinguished Name	7
3.5	Service Account Information	7
3.6	Business Processing Rules.....	7

Version History Tracking

Version	Date	Description of Changes	Modified By
1.0	15 APR 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. 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 Secret Internet Protocol Router Network (SIPRNet). 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 *
	●	●	<input type="checkbox"/>	1	co	Work Contact Mailing Address Country Code	CHAR(2)
●	●	●	<input type="checkbox"/>	2	company	Duty Organization Code (DISA, ARMY, etc.)	CHAR(20)
●	●	●	<input type="checkbox"/>	3	department	Administrative Organization Code (DoD, etc.)	VARCHAR2(15)
●	●	●	<input type="checkbox"/>	4	displayName	The Persona Display Name	VARCHAR2(200)
●	●	●	<input type="checkbox"/>	5	employeeID	Federal Agency Smart Credential – Number	NUMBER(16)
●	●	●	<input type="checkbox"/>	6	employeeType	The type of Persona	CHAR(3)
●	●	●	<input type="checkbox"/>	7	extensionAttribute1	Branch of Service	CHAR(1)
●	●	●	<input type="checkbox"/>	8	extensionAttribute2	Duty Organization Code (DISA, ARMY, etc.)	CHAR(20)
●	●	●	<input type="checkbox"/>	9	extensionAttribute3	Duty Building + '/' + Room Number	VARCHAR2(100) + VARCHAR2(40)
		●	<input type="checkbox"/>	10	extensionAttribute4	US Citizen	CHAR(1)
●	●	●	<input type="checkbox"/>	11	extensionAttribute7	Office Symbol Text	CHAR(30)
		●	<input type="checkbox"/>	12	extensionAttribute8	Country of Citizenship	CHAR(2)
●	●	●	<input type="checkbox"/>	13	extensionAttribute9	US Government Agency Code	CHAR(4)
	●	●	<input type="checkbox"/>	14	facsimileTelephoneNumber	Work Contact Facsimile Number	CHAR(20)
●	●	●	<input type="checkbox"/>	15	generationQualifier	The cadency name (e.g., Sr, Jr) of the person	VARCHAR2(4)
●	●	●	<input type="checkbox"/>	16	givenName	First Name	VARCHAR2(20)
●	●	●	<input type="checkbox"/>	17	Initials	Middle Name	VARCHAR2(20)
	●	●	<input type="checkbox"/>	18	l	Work Contact Mailing Address City Name	CHAR(20)
●	●	●	<input type="checkbox"/>	19	mail	Work Email address (single primary email address)	VARCHAR2(80)

Contact	Detailed	Extended	Required?		IdMI (AD LDS) Attributes	Description	Data Type *
●	●	●	<input type="checkbox"/>	20	mailNickname	The Persona User Name	VARCHAR2(64)
●	●	●	<input type="checkbox"/>	21	mobile	Work Contact Telephone Number	CHAR(20)
	●	●	<input type="checkbox"/>	22	otherTelephone	Work Contact Telephone Number	CHAR(20) **
		●	<input type="checkbox"/>	23	personalTitle	Rank Code or Civilian Grade Code	VARCHAR2(6) or VARCHAR2(10)
●	●	●	<input type="checkbox"/>	24	physicalDeliveryOfficeName	Duty Installation	CHAR(30)
	●	●	<input type="checkbox"/>	25	postalCode	Work Contact US Postal ZIP Code + Work Contact US Postal ZIP Code Extension	CHAR(5) + '-' + CHAR(4)
●	●	●	<input type="checkbox"/>	26	proxyAddressess	Work Email Address	VARCHAR2(80) ***
	●	●	<input type="checkbox"/>	27	roomNumber	Room Number	VARCHAR2(40)
●	●	●	<input type="checkbox"/>	28	sn	Last Name	VARCHAR2(26)
	●	●	<input type="checkbox"/>	29	st	Work Contact Mailing Address State Code	CHAR(2)
●	●	●	<input type="checkbox"/>	30	streetAddress	Work Contact Mailing Address Line 1 + Work Contact Mailing Address Line 2	CHAR(40) + CHAR(40)
	●	●	<input type="checkbox"/>	31	telephoneNumber	Work Contact Telephone Number + 'x' + extension number	CHAR(20) + CHAR(6)
●	●	●	<input type="checkbox"/>	32	title	Job Title Text	CHAR(80)
●	●	●	<input type="checkbox"/>	33	uid	EDIPI + Persona Type Code (1234567890.civ)	CHAR(14)
	●	●	<input type="checkbox"/>	34	userCertificate	User Encryption Certificate	BINARY

* The data type information shown is from the source location (DMDC). userCertificate is from GDS. The data type text is hyperlinked to the actual directory attribute type for AD LDS (hyperlink should resolve to the section of page for Windows Server 2008 R2).

** 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.

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.