



**Identity Synchronization Service Machine Interface (IdMI)  
SIPRNet Customer Interface Specification  
Between**

**<<Component>>**

**and**

**DISA Enterprise Services Directorate  
Enterprise Infrastructure Division**

**27 December 2013**

Version 1.9

**UNCLASSIFIED**

## 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 .....	7
3.6	Business Processing Rules.....	7

### Version History Tracking

Version	Date	Description of Changes	Modified By
1.7	12 JUN 2013	Modified 2.1.1 Data Dictionary	T. Mazzullo
1.8	2 AUG 2013	Modified attribute description, modified verbiage in 3.5	T. Mazzullo
1.9	27 DEC 2013	Modified attributes based on IdSS Release 22	T. Mazzullo

## 1. Overview

The purpose of this document is to define the connection interface between DISA Enterprise Services Directorate, Identity Synchronization Service (IdSS) Machine Interface (IdMI) and the <<Component>>. This agreement defines the connection allowing the flow of IdSS Contact Data into the <<Specific Component Directory System>> on the Secret Internet Protocol Router Network (SIPRNet). IdMI is a suite of synchronization interface capabilities for machine to machine synchronization of DoD Persona data. 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 connection in support of <<Component>>/DISA Memorandum of Agreement.

### 2.1. Scope

#### 2.1.1 Data Dictionary.

Data fed via IdMI connection to <<Component>> includes data for <<all DoD personas with a known SIPRNet email address or migrated users of DoD Enterprise Email system only and/or contact objects>> and will consist of those data elements identified in the below table. DMDC is the accountable source for all data in the table below, excluding email encryption certificates provided by DISA GDS, and DEE email account data provided by DISA ESD for DEE migrated users.

Contact	Detailed	Extended		IdMI (AD LDS) Attributes	Description	Data Type (from DMDC)*	Data Type (from IdMI)
●	●	●	1	cn	The Persona User Name (PUN)	VARCHAR2(64)	String(64)
	●	●	2	co	Work Contact Mailing Address Country Code	CHAR(2)	String(128)
●	●	●	3	company	Administrative Organizational Code (DoD, etc.)	VARCHAR2(15)	String(64)
●	●	●	4	department	Duty Organization Subdivision Code	CHAR(20)	String(64)
●	●	●	5	displayName	The Persona Display Name	VARCHAR2(200)	String(256)
●	●	●	6	employeeID	Federal Agency Smart Credential – Number	NUMBER(16)	String(16)
●	●	●	7	employeeType	Persona Type Code (PTC) such as MIL, CIV, CTR, etc.	CHAR(3)	String(256)
●	●	●	8	extensionAttribute1	Branch of Service	CHAR(1)	String(1024)
●	●	●	9	extensionAttribute2	Duty Organization Code (DISA, ARMY, etc.)	CHAR(20)	String(1024)
●	●	●	10	extensionAttribute3	Duty Building + ‘/ Rm ’ + Room Number	VARCHAR2(100) + VARCHAR2(40)	String(1024)
		●	11	extensionAttribute4	US Citizen	CHAR(1)	String(1024)
●	●	●	12	extensionAttribute7	Office Symbol Text	CHAR(30)	String(1024)
		●	13	extensionAttribute8	Country of Citizenship	CHAR(2)	String(1024)
●	●	●	14	extensionAttribute9	US Government Agency Code	CHAR(4)	String(1024)

Contact	Detailed	Extended		IdMI ( <a href="#">AD LDS</a> ) Attributes	Description	Data Type (from DMDC)*	Data Type (from IdMI)
			15	extensionAttribute10	Preferred First Name	VARCHAR2(68)	<a href="#">String(1024)</a>
	●	●	16	facsimileTelephoneNumber	Work Contact Facsimile Number	CHAR(20)	<a href="#">String(64)</a>
●	●	●	17	generationQualifier	The cadency name (e.g., Sr, Jr) of the person	VARCHAR2(4)	<a href="#">String(64)</a>
●	●	●	18	givenName	First name	VARCHAR2(20)	<a href="#">String(64)</a>
●	●	●	19	Initials	Middle Name	VARCHAR2(20)	<a href="#">String(6)</a>
	●	●	20	1	Work Contact Mailing Address City Name	CHAR(20)	<a href="#">String(128)</a>
●	●	●	21	mail	Work Email address (single primary email address)	VARCHAR2(80)	<a href="#">String(256)</a>
●	●	●	22	mobile	Mobile Contact Telephone Number	CHAR(20)	<a href="#">String(64)</a>
	●	●	23	otherTelephone	Other Contact Telephone Number	CHAR(20) **	<a href="#">String(64)</a> **
		●	24	personalTitle	Rank Code or Civilian Grade Code (SES, HON, HQE only)	VARCHAR2(6) or VARCHAR2(10)	<a href="#">String(64)</a>
●	●	●	25	physicalDeliveryOfficeName	Duty Installation	CHAR(20)	<a href="#">String(128)</a>
	●	●	26	postalCode	Work Contact US Postal ZIP Code + Work Contact US Postal ZIP Code Extension	CHAR(5) + '-' + CHAR(4)	<a href="#">String(40)</a>
●	●	●	27	proxyAddresses	Work Email Address	VARCHAR2(80) ***	<a href="#">String(1123)</a> ***
	●	●	28	roomNumber	Room Number	VARCHAR2(40)	<a href="#">String</a>
●	●	●	29	sn	Last Name	VARCHAR2(26)	<a href="#">String(64)</a>
	●	●	30	st	Work Contact Mailing Address State Code	CHAR(2)	<a href="#">String(128)</a>
●	●	●	31	streetAddress	Work Contact Mailing Address Line 1 + Work Contact Mailing Address Line 2	CHAR(40) + CHAR(40)	<a href="#">String(1024)</a>
	●	●	32	telephoneNumber	Work Contact Telephone Number + ' x ' + extension number	CHAR(20) + CHAR(6)	<a href="#">String(64)</a>
●	●	●	33	title	Job Title Text	CHAR(80)	<a href="#">String(128)</a>
●	●	●	34	uid	EDIPI + Persona Type Code (1234567890.civ)	CHAR(14)	<a href="#">String</a>
	●	●	35	userCertificate	User Encryption Certificate	BINARY	<a href="#">Binary</a>

\* 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 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 should obtain at run time 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 IdMI processing. DMDC is the authoritative source for all person based data contained in IdSS excluding email addresses of migrated users of DOD Enterprise Email system
- 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 IdMI connections which will be made readily available to DMDC.
- <<Component>> will use this data for populating their local Active Directory and White pages.
- All systems receiving the data must be accredited in accordance with DoD Instruction 8500.2.

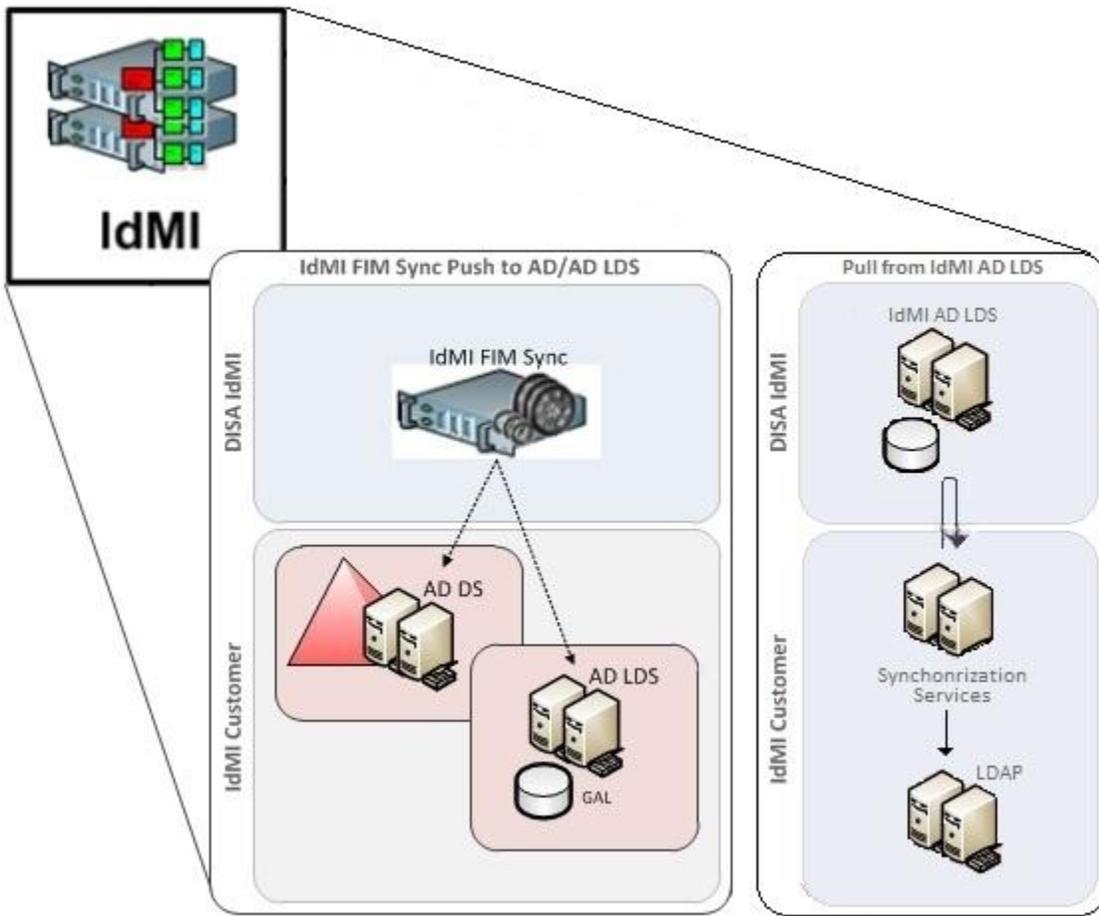
## 3. Technical Solution

### 3.1 Connection Description

IdMI will provide synchronization from the IdMI Active Directory Lightweight directory service (AD LDS) to <<Specific Component Directory System>> synchronization service instance.

Synchronization options: (one method will be selected and agreement will only reflect the appropriate diagram)

1. IdMI FIM Sync push to IdMI customer AD LDS
2. Component synchronization service pull from from IdMI AD LDS  
(Insert correct diagram below)



### 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
x.x.x.x	x.x.x.x	636	LDAP/S	
x.x.x.x	x.x.x.x	636	LDAP/S	

### 3.3 Client Requirements

1. <<Component>> will stand up and maintain a directory service instance within the <<component>> enclave boundary.
2. <<Component>> make necessary changes to <<component>> firewalls to allow synchronization traffic to flow through the <<Component>> enclave boundary.
3. Describe the frequency of the synchronization data flow (push or pull)

### 3.4 Root Distinguished Name

(Enter required Distinguished Name or N/A for DISA push to component Directory Service)

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](mailto: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 IdMI

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 IdMI 7 days after the person no longer has a valid CAC.