DISA
Enterprise Services

IdSS/IdMI Overview for Mission Partners

Document Version 1.2

02 October 2014

Defense Information Systems Agency

Enterprise Information Services

Identity Synchronization Services (IdSS)

Document Approval

Document Approved By	Date Approved

Revision History

Version	Date	Revision/Change Description	Writer	Pages Affected
1.0	March 2013	Initial version		All sections
1.1	8 August 2014	Update contents, process new format	Quang T. Huynh	All sections
1.2	03 Oct 2014	Final for Publish	ES212	All sections

Table of Contents

List of Figures

List of Tables

1 Introduction

The Identity Synchronization Service (IdSS) is a part of the DISA Enterprise Directory Services, a suite of products and services providing DoD Enterprise identity and contact attributes. Enterprise Directory Services is comprised of enterprise provisioning services, directory services, synchronization services, and DoD Enterprise White Pages in support of people discovery across the DoD community.

1.1 Identity Synchronization Service (IdSS)

IdSS connects to authoritative identity data sources including the Defense Manpower Data Center (DMDC) and the Global Directory Service (GDS) to collect and groom identity data, and to provision and maintain persona-based user objects in Lightweight Directory Access Protocol (LDAP) directories such as the Enterprise Applications Services Forest (EASF). IdSS controls all account creation, deletion, and updates into the EASF, and allows DISA mission partners to map DISA services, referred to as entitlements, to specific end-users.

1.2 IdSS Machine Interface (IdMI)

The IdSS Machine Interface (IdMI) provides a capability for machine to machine synchronization of DoD Persona data groomed by IdSS and populated in EASF. It is capable of providing a one-way data feed between IdSS and DISA mission partners for populating and maintaining DoD Component level information technology (IT) directory systems such as Global Address Lists (GALs), LDAP directories and White Pages. The IdMI feeds include person and persona identity and contact data elements for personas that have a current DoD Common Access Card (CAC). It also includes the ability to provide synchronization for Non-Person Entity (NPE) objects in support of group management and distribution.

2 IdMI

2.1 IdMI Data

IdMI data feeds provide data elements identified in the IdMI NIPRNet Customer Interface Specification (http://iase.disa.mil/idam/Pages/documentation.aspx). Note, while IdMI data provides data groomed by IdSS, ultimately DMDC is the accountable source for all data in the data dictionary, excluding email encryption certificates provided by DISA GDS, and DoD Enterprise Email (DEE) account data provided by DISA Enterprise Information Services (EIS) for DEE migrated users. 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.

DISA EIS assumes that the DoD Component receiving the IdMI feed will use this data for populating their local Active Directory and White Pages system. Options to customize the feed include frequency of synchronization, push vs. pull, and data element selection.

2.2 Enterprise Service

DISA provides the IdMI feed as an Enterprise service. The architecture of the IdMI service was scaled to accommodate an IdMI connection per Combatant Command (COCOM), service, and agency (CC/S/A) free of charge. DISA provides synchronization services on both NIPRNet and SIPRNet feeds with the expectation that each CC/S/A will distribute the data to the CC/S/A managed Active Directory and White Pages system.

2.3 Technical Implications

IdMI provides synchronization from the IdSS data to the CC/S/A synchronization service instance. To support IdMI, the CC/S/A enables a Lightweight Directory Access Protocol Secure (LDAP/S) export from the EIS server infrastructure to their server, and must open one network port for the data feed.

2.4 Network Implications

An unfiltered IdMI feed may require upwards of 25GB of storage, although, the amount of data pulled can be significantly reduced by limiting the data requested. An unfiltered initial sync with IdMI will require a full-sync using a sync engine, which will transfer approximately 20GB of data and take roughly 24-48 hours to complete. The impact to the network will be based on available bandwidth.

After the initial full-sync into the CC/S/A instance, IdMI supports periodic incremental updates. The frequency of incremental updates can be specified during IdMI setup. After the full-sync, IdMI supports 100K incremental updates for roughly 1GB of data per week. Actual network load is dependent on the synchronization tool used. Note that a full-sync may be needed approximately two to four times a year.

2.5 Synchronization Options

IdMI supports the following synchronization options:

- IdMI FIM Sync push to IdMI customer AD LDS
- Synchronization pulls from IdMI AD LDS to component synchronization service instance, using a synchronization tool of the component's choosing.

One method will be selected and agreement will only reflect the appropriate diagram:

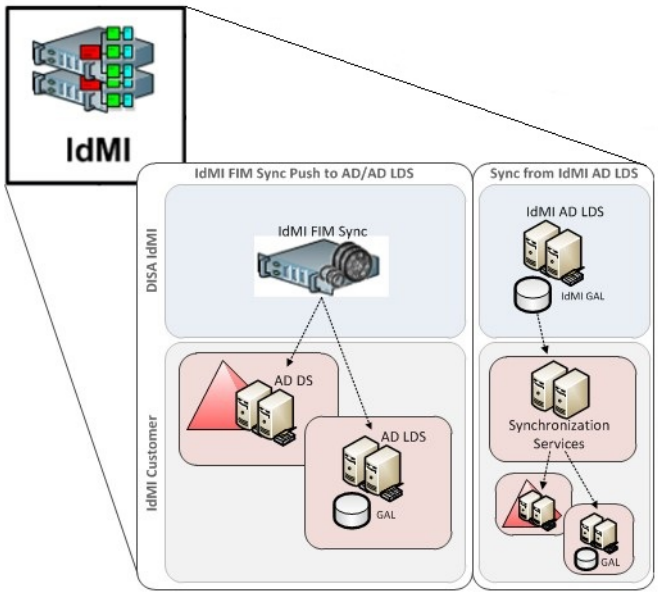


Figure 1: IdMI interfaces

3 How to get IdMI

The following requirements should be kept in mind for establishing an IdMI connection:

- **Memorandum of Agreement (MOA) Requirement**: DISA follows DoD instructions for interagency agreements. DoD instructions state an MOA is required for Reimbursable or Non-Reimbursable support agreements.

  NOTE: DISA policy allows for a delegation of signature authority for specific types of agreement to the GS-15 level. DISA signature authority has been delegated by PEO-ES to Jacqueline (Jackie) M. Huff for IdMI connections.

- **Protection of PII data**: The IdMI feed contains Personally Identifiable Information (PII) data. A Privacy Impact Assessment (PIA) and System of Record Notice (SORN) are required for the component level IT system to connect to the IdMI feed.

All systems receiving IdMI data must be accredited in accordance with DoD Instruction 8500.2.

To establish an IdMI connection, DISA EIS and the CC/S/A must work together to establish MOA, obtain security accreditations, and coordinate technical resources to implement the connection. More details below:

1. CC/S/A and DISA EIS representatives meet to review requirements and understand what is involved for an IdMI.
2. CC/S/A provides DISA with information needed to complete an MOA specifying points of contact and system information needed in the agreement.
3. CC/S/A works with DISA EIS to gather information to complete the IdMI Customer Interface Specification (CIS). This document formalizes the relationship and provides specific authoritative detail to operate, maintain, and update the connection in support of the MOA. A CIS is required for every individual NIPRNet and SIPRNet connection established.

   The CIS must include the following information:

   i. Synchronization Option (push or pull)
   ii. External Interface Communication Requirements (IP addresses, Ports/Protocols)
   iii. Frequency of synchronization (e.g., every 12 hours, daily)
   iv. Component/Client requirements
   v. Root Distinguished Name (DN) (not applicable for DISA push to Directory service)
4. CC/S/A provides a completed PIA for their directory system, needed to verify the directory system being populated has addressed privacy appropriately. PIA should comply with DoD Instruction 5400.16.
5. CC/S/A provides a copy of the Authority to Operation (ATO) for the directory system.
6. DISA completes the MOA and the IdMI CIS, and staffs the MOA for signature.
7. CC/S/A reviews the MOA and also staffs appropriately for signatures.

After the completed signed MOA is returned to DISA with all attachments, it takes a matter of days to establish the connection, depending upon how fast firewall rule changes are enacted at both DISA and the Component.

4 Points of Contact

Questions may be directed to:

DISA.EDSMemo@mail.mil

5 Appendix

5.1 Appendix A

AD	Active Directory
ATO	Approval to Operate
CAC	Common Access Card
CC/S/A	Combatant Command (COCOM), service, and agency
CIS	Customer Interface Specification
COCOM	Combatant Command
DECC	Defense Enterprise Computing Center
DEE	DoD Enterprise Email
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DN	Domain Name
DoD	Department of Defense
EASF	Enterprise Application Services Forest
ESD	Enterprise Services Directorate
GAL	Global Address List
GDS	Global Directory Service
IdAM	Identity Access Management
IdMI	IdSS Machine Interface
IdSS	Identity Synchronization Service
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement
NIPRNET	Non-Secure Internet Protocol Routing Network
NPE	Non-Person Entity
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMO	Project Management Office
SIPRNET	Secret Internet Protocol Routing Network
SORN	System of Record Notice

Table 1: Acronyms

5.2 Appendix B: IdSS architecture and Data Flow

The following diagram illustrates the flow of identity and contact data through the IdSS and EASF architecture. IdSS connects to accountable identity sources to collect and groom identity information. The Defense Manpower Data Center (DMDC) is the accountable source for identity data and Global Directory Service (GDS) is the source for encryption certificates. IdSS controls all account creation, deletion, and updates into the EASF. IdSS data is made available to DISA mission partners through IdMI.

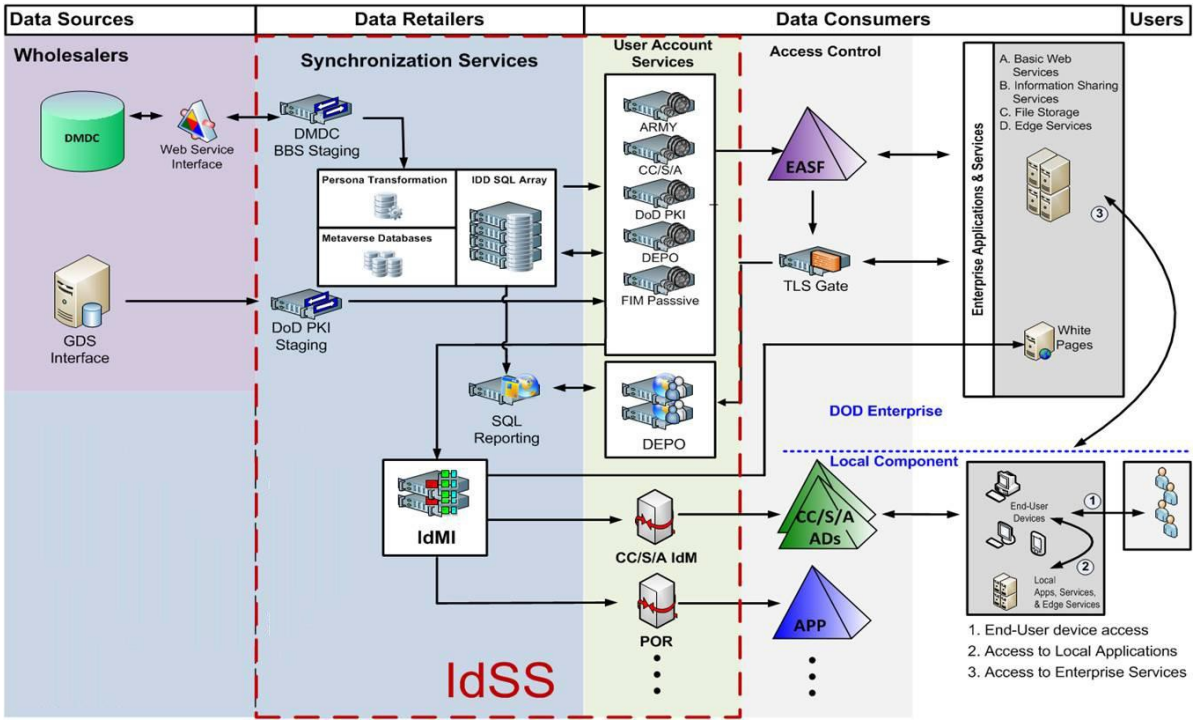
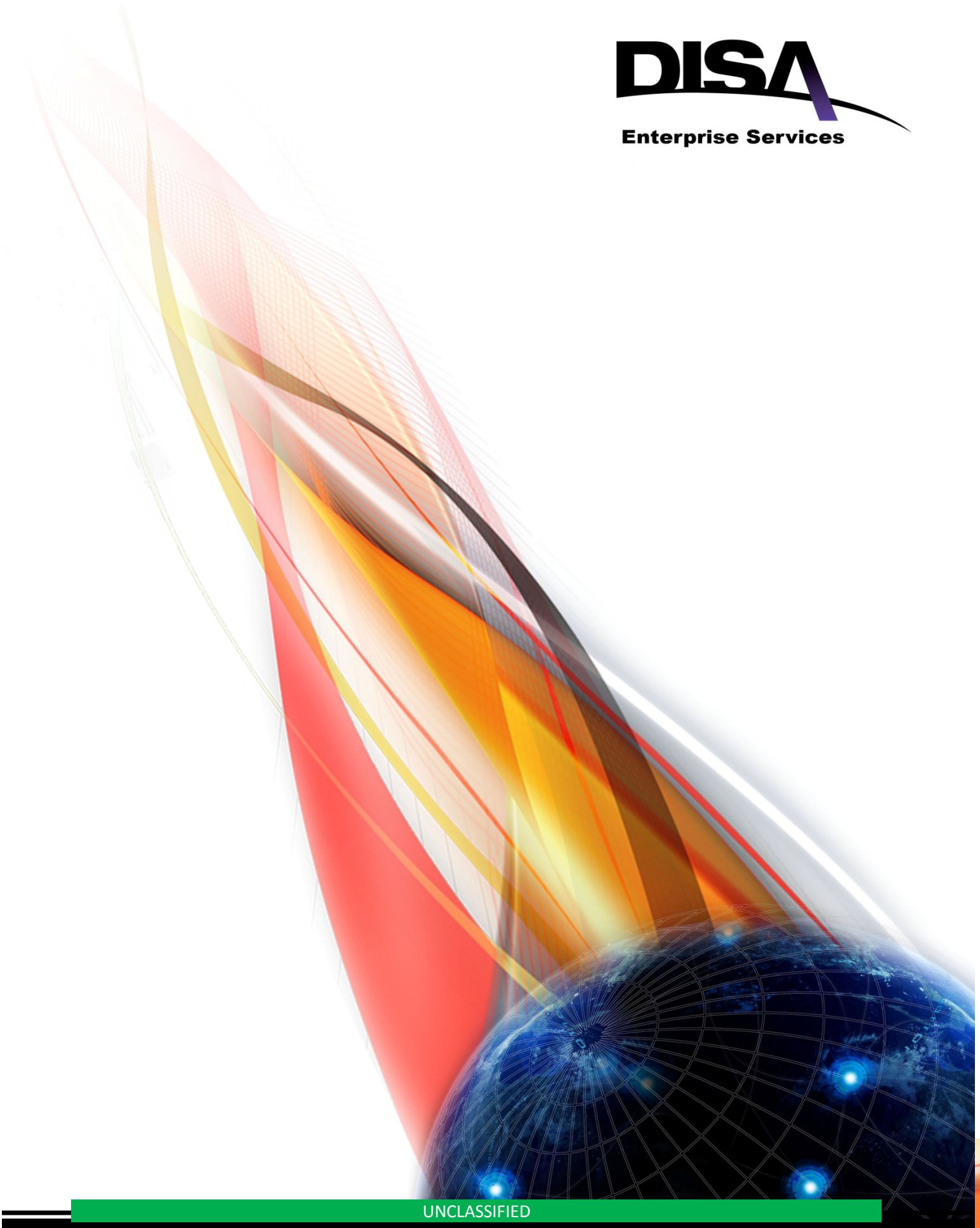


Figure 2: Data flow through the IdSS and EASF Architecture

DISA

Enterprise Services



UNCLASSIFIED

COLLABORATIVE GLOBAL SECURE